Modicon M580

Redundant Communication Adapter Module (PRP) for X80 RIO Drops

Installation and Configuration Guide

Original instructions

11/2024

EIO0000004532.01

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.
- Only those operational adjustments required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

About the Book

Document Scope

This document describes the X80 RIO drop redundant communication adapter on Parallel Redundancy Protocol (PRP) network technology modules (BMECRA31310 and BMECRA31310H).

NOTE: The specific configuration settings contained in this guide are for instructional purposes only. The settings required for your specific application can be different from the examples presented in this guide.

Validity Note

This document has been updated for the release of EcoStruxure™ Control Expert V16.1.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Related Documents

Title of documentation	Reference number
Modicon M580, Hardware, Reference Manual	EIO0000001578 (ENG) EIO0000001583 (CHS) EIO0000001579 (FRE) EIO0000001580 (GER) EIO0000001582 (ITA) EIO0000001581 (SPA)
Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	EIO0000002726 (ENG) EIO0000002731 (CHS) EIO0000002727 (FRE) EIO0000002728 (GER) EIO0000002730 (ITA) EIO0000002729 (SPA)
Modicon M580 Hot Standby, System Planning Guide for Frequently Used Architectures	NHA58880 (ENG) NHA58885 (CHS) NHA58881 (FRE) NHA58882 (GER) NHA58883 (ITA) NHA58884 (SPA)
Modicon M580, Change Configuration on the Fly, User Guide	EIO0000001590 (ENG) EIO0000001595 (CHS) EIO0000001591 (FRE) EIO0000001592 (GER) EIO0000001594 (ITA) EIO0000001593 (SPA)
Modicon M580, RIO Modules, Installation and Configuration Guide	EIO0000001584 (ENG) EIO0000001589 (CHS) EIO0000001585 (FRE) EIO0000001586 (GER) EIO0000001587 (ITA) EIO0000001588 (SPA)
Modicon X80, BMXNRP0200/0201 Fiber Converter Modules, User Guide	EIO0000001108 (ENG) EIO0000001113 (CHS) EIO0000001109 (FRE) EIO0000001110 (GER) EIO0000001112 (ITA) EIO0000001111 (SPA)

Title of documentation	Reference number
EcoStruxure™ Control Expert, Topology Manager, User Manual	EIO0000002756 (ENG) EIO0000004373 (CHS) EIO0000004371 (FRE) EIO0000004372 (GER) EIO0000004370 (ITA) EIO0000004369 (SPA)
EcoStruxure™ Control Expert, Program Languages and Structure, Reference Manual	35006144K01000 (ENG) 35013362K01000 (CHS) 35006145K01000 (FRE) 35006146K01000 (GER) 35013361K01000 (ITA) 35006147K01000 (SPA)
EcoStruxure™ Control Expert, System, Block Library	33002539 (ENG) 33003689K01000 (CHS) 33002540K01000 (FRE) 33002541K01000 (GER) 33003688K01000 (ITA) 33002542K01000 (SPA)
Modicon Controllers Platform Cyber Security, Reference Manual	EIO0000001999 (ENG) EIO0000002004 (CHS) EIO0000002001 (FRE) EIO0000002000 (GER) EIO0000002002 (ITA) EIO0000002003 (SPA)
EcoStruxure Automation Device Maintenance, Firmware Upgrade Tool, Online Help	EIO0000004033 (ENG) EIO0000004050 (CHS) EIO0000004048 (FRE) EIO0000004046 (GER) EIO0000004049 (ITA) EIO0000005090 (POR-BRA) EIO0000004047 (SPA) EIO0000005089 (TUR)
Modicon X80 Racks and Power Supplies, Hardware, Reference Manual	EIO0000002626 (ENG) EIO0000002631 (CHS) EIO0000002627 (FRE) EIO0000002628 (GER) EIO0000002630 (ITA) EIO0000002629 (SPA)
System Time Stamping, User Guide	EIO0000001217 (ENG) EIO0000001711 (CHS) EIO0000001707 (FRE) EIO0000001708 (GER) EIO0000001710 (ITA) EIO0000001709 (SPA)
Electrical installation guide	EIGED306001EN (ENG)
Control Panel Technical Guide, How to protect a machine from malfunctions due to electromagnetic disturbance	CPTG003_EN (ENG) CPTG003_FR (FRE)

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Product Related Information

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables, or wires except under the specific conditions specified in the appropriate hardware guide for this equipment.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to the unit.
- Use only the specified voltage when operating this equipment and any associated products.

Failure to follow these instructions will result in death or serious injury.

⚠DANGER

POTENTIAL FOR EXPLOSION

- Only use this equipment in non-hazardous locations, or in locations that comply with Class I, Division 2, Groups A, B, C and D.
- Do not substitute components which would impair compliance to Class I Division 2.
- Do not connect or disconnect equipment unless power has been removed or the location is known to be non-hazardous.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

LOSS OF CONTROL

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.[1]
- Test each implementation of a system for proper operation before placing it into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* and to NEMA ICS 7.1 (latest edition), *Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems* or their equivalent governing your particular location.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in the information contained herein, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2020	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2021	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2021	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term *zone of operation* may be used in conjunction with the description of specific hazards, and is defined as it is for a *hazard zone* or *danger zone* in the *Machinery Directive* (*2006/42/EC*) and *ISO 12100:2010*.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Modicon M580 Redundant RIO Network

What's in This Part

PRP Network – Design Principles

What's in This Chapter

This chapter provides a description of the PRP network and how to implement it in M580 architectures using the X80 RIO drop redundant communication adapter BMECRA31310(H) module.

Introduction

In a typical M580 Ethernet RIO (EIO) architecture, BMXCRA31200, BMXCRA31210, or BMECRA31210 adapter modules are used to manage Modicon X80 I/O drops. The M580 system uses RSTP protocol and redundant physical paths along its device network (daisy chain loop topologies) for providing automatic network recovery of less than 50 ms and deterministic RIO performance.

When using BMECRA31310(H) adapter modules to manage Modicon X80 I/O drops, the device network rely on PRP for network recovery. The PRP technology, described in the IEC 62439-3 standard, provides redundancy by duplicating the network infrastructure and by monitoring the simultaneous data transmitted in both independent network. The PRP network recovery is 0 ms.

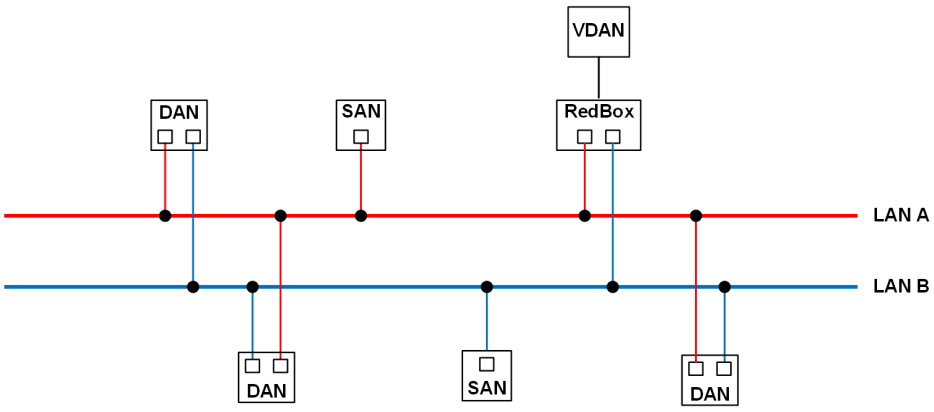
PRP Network Terminology

The PRP network infrastructure is based on two independent Local Area Networks (LAN A and LAN B). The incoming and outgoing traffics on the PRP network are duplicated on both LANs.

If a communication disruption is detected on one of the LANs, traffic continues to flow over the other LAN uninterruptedly and re-configuring the LAN(s) (for example, unblocking the port) is not required. The dual cabling of the PRP network infrastructure and its technology provides a 0 ms recovery time.

NOTE: After reconnecting a cable, it can take up to 3 seconds for the port to re-establish connections and synchronize with the PRP network.

The following figure shows the LANs with various nodes:



Terminology for PRP network nodes:

- **DAN** (Dual Attached Node / Dual Access Node): It is a redundant node in the network as it sends two packets simultaneously through its two network interfaces to the destination node. A DAN have redundant paths to other DANs in the network.
- **SAN** (Single Attached Node / Single Access Node): It is a non-redundant node in the network as it is connected to either LAN A or LAN B. If there is an interruption, a device connected as a SAN cannot be reached through the redundant network.
- **RedBox** (Redundancy Box): It is an industrial switch with PRP technology that connects non-PRP devices or non-PRP part of the network to both LAN A and LAN B. The RedBox itself is a DAN and acts as a proxy on behalf of its VDANs.
- **VDAN** (Virtual Dual Attached Node / Virtual Dual Access Node): It is connected behind a RedBox. As it appears for the other nodes like a DAN in the PRP network, it is called a virtual DAN.

A redundancy control trailer (RCT), which includes a sequence number, is added to each frame to help the destination node to distinguish between duplicate packets. When the destination DAN receives the first packet successfully, it removes the RCT and consumes the packet. If the second packet arrives successfully, it is discarded.

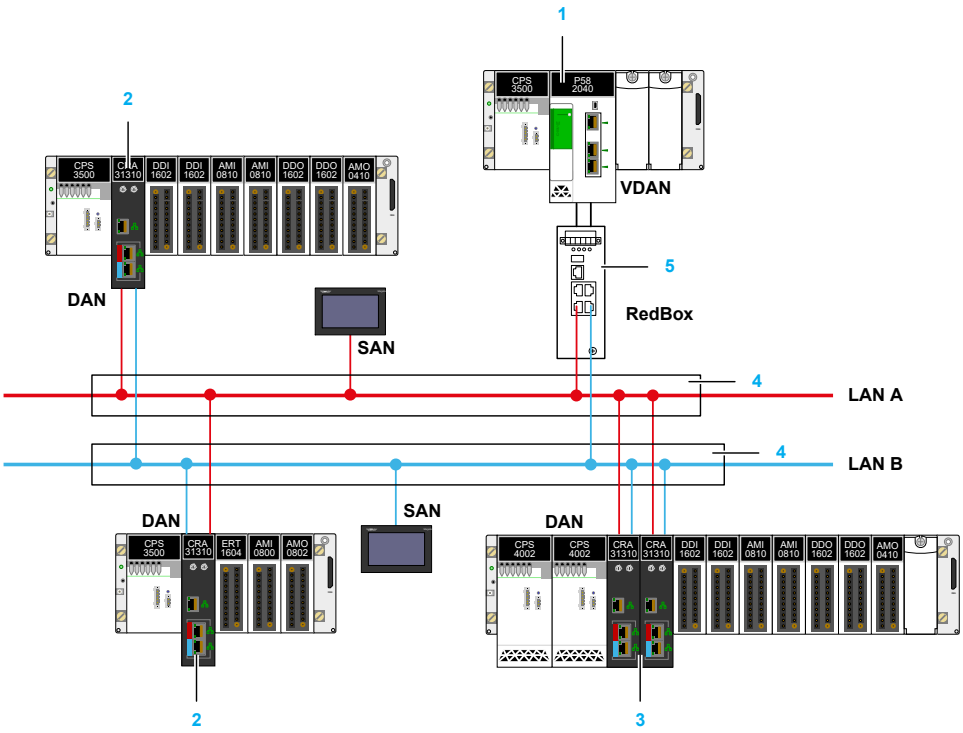
NOTE: The connection between both LANs operates at a node level (DAN, RedBox).

PRP Network Components

Overview

Designing a Modicon M580 architecture with a redundant I/O Network on PRP network technology requires as a minimum:

- A Modicon M580 controller
- RIO drop(s) managed by X80 RIO drop redundant communication adapter PRP module(s)
- Modicon Redundancy switch(es) (RedBox)
- Managed Ethernet switch(es) (Modicon or ConneXium)



1 Modicon M580 controller
2 BMECRA31310(H) adapter module
3 Two BMECRA31310(H) adapter modules allowing module redundancy (only used with hot standby controller) in an architecture including a Modicon Redundancy switch
4 Ethernet switches allowing connections to LAN A and LAN B

5 Modicon Redundancy switch

BMECRA31310(H) Module

In a network management perspective, the X80 RIO drop redundant communication adapter PRP module BMECRA31310(H) is a DAN.

The PRP technology enables communication with the RIO scanner. The device network ports of the redundant adapter module operate in dual attached node to duplicate independent network infrastructure (LAN A and LAN B).

Both networks sustain the exchange of packets between the controller and the I/O drops, through either network independently. During normal network operation, the device simultaneously sends and receives duplicate Ethernet frames through both ports. The receiving node accepts whichever frame arrives first on one of the two LANs and discards the copy form the other LAN. Even if a communication interruption is detected on one of the LANs, the traffic continues to flow through the other uninterrupted LAN with no recovery time.

The BMECRA31310(H) adapter module manages an RIO drop composed of I/O modules, expert modules and communication modules, and exchanges data with the RIO scanner of the Modicon M580 controllers.

With M580 controller for high-availability architectures, configuring two BMECRA31310(H) adapter modules in an RIO drop provides redundancy of the adapter module.

Modicon Redundancy Switch – MCSESR043F2•••(C)

The Modicon Redundancy switch is an industrial switch that allows you to implement redundancy on an end node without PRP network ports.

The Modicon Redundancy switch connects the RIO scanner of the M580 controller on one side to the PRP network on the other side. In a high-availability architecture the primary and standby M580 controllers are respectively connected to two different Modicon Redundancy switches.

The Modicon Redundancy switch connects the non-PRP devices or part of the RIO network to the redundant PRP network.

Ethernet Switch

On the LAN, conventional Ethernet switches are required for the transit of the frames in the PRP network. The Ethernet switch does not require any PRP support.

As Modicon M580 system requires to prioritize the traffic on the network between controller and X80 drop with VLAN and QoS (DSCP) specific configuration, only managed switches can be used.

The following switches are supported:

- Modicon managed switches MCSESM•••
- Modicon PoE managed switches MCSESP•••
- ConneXium managed switches TCSESM163•••, TCSESM243•••
- ConneXium extended managed switches TCSESM063•••, TCSESM083•••

M580 Controller

In a network management perspective, the M580 controller is a VDAN and is connected to the PRP network through a Modicon Redundancy switch.

The following Modicon M580 controllers with an RIO scanner support I/O network relying on PRP:

- BMEP58•040 for standalone architectures
- BMEH58•040 for high-availability architectures

  NOTE: These Modicon M580 controllers require a firmware version SV4.30 or any subsequent supporting version(s).

Operating two BMECRA31310(H) adapter modules in an RIO drop (redundant mode) is only compatible with BMEH58•040 controllers (Modicon M580 redundant controllers).

Modicon M580 Redundant RIO Network Architectures Relying on PRP

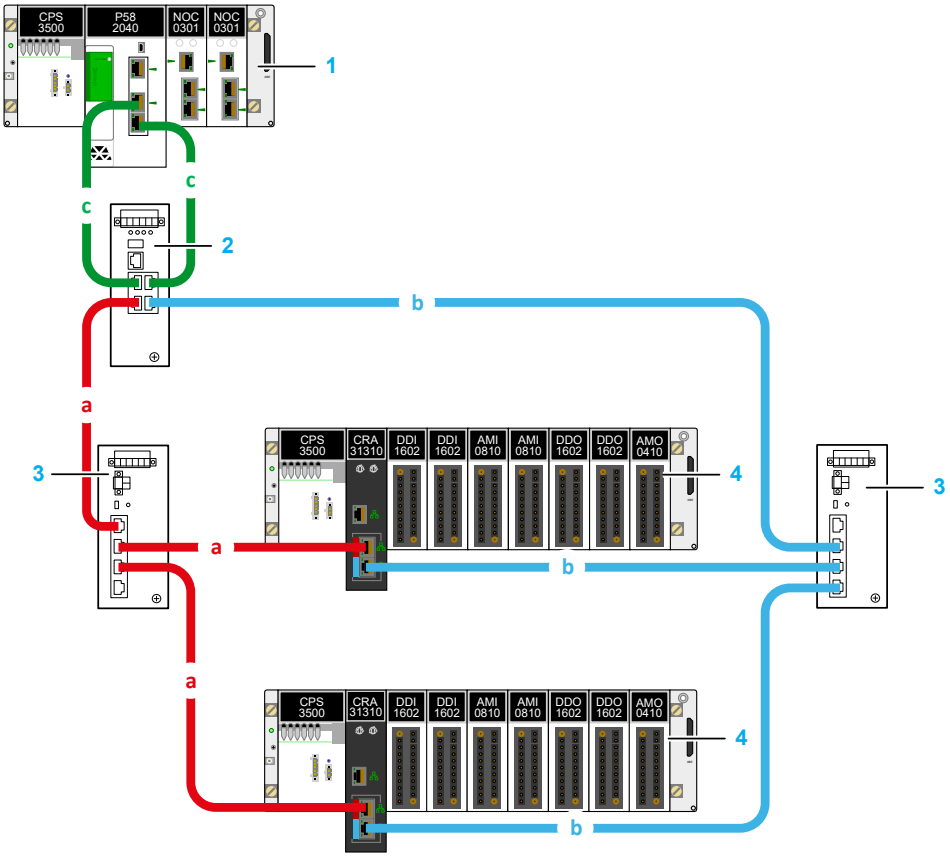
What's in This Chapter

Standalone Architecture

In a standalone architecture:

- The Modicon M580 controller is connected to the PRP network through a dedicated Modicon Redundancy switch, and
- Each RIO drop is managed by a BMECRA31310(H) adapter module.

NOTE: Redundancy of the adapter module is not possible in standalone architecture.



1 Modicon M580 local drop
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with one BMECRA31310(H) adapter module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

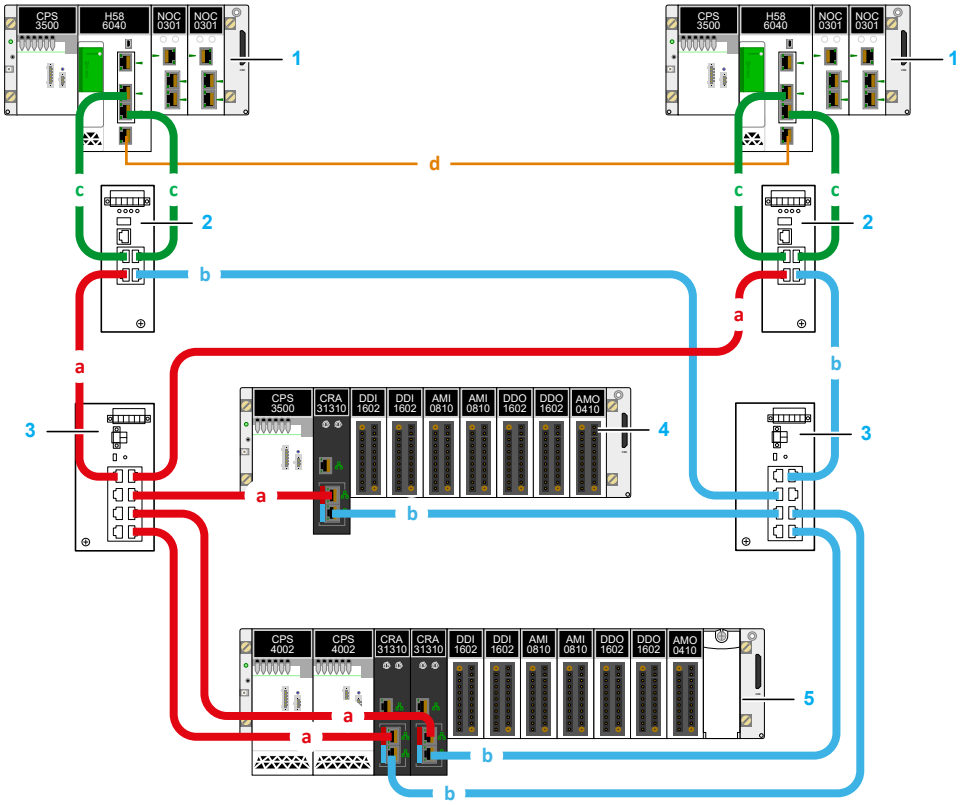
High-availability Architecture

In high-availability architecture:

- Both Modicon M580 controller (primary and standby) are connected to the PRP network through dedicated Modicon Redundancy switches
- Each RIO drop can be managed by one or two BMECRA31310(H) adapter modules

NOTE: Connecting both Modicon M580 controller (primary and standby) to a unique Modicon Redundancy switch is not allowed.

Using two BMECRA31310(H) adapter modules on the same RIO drop provides module redundancy. One adapter module is managing the drop while the other adapter module is in standby.



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with one BMECRA31310(H) adapter module (single mode)
5 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode)

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

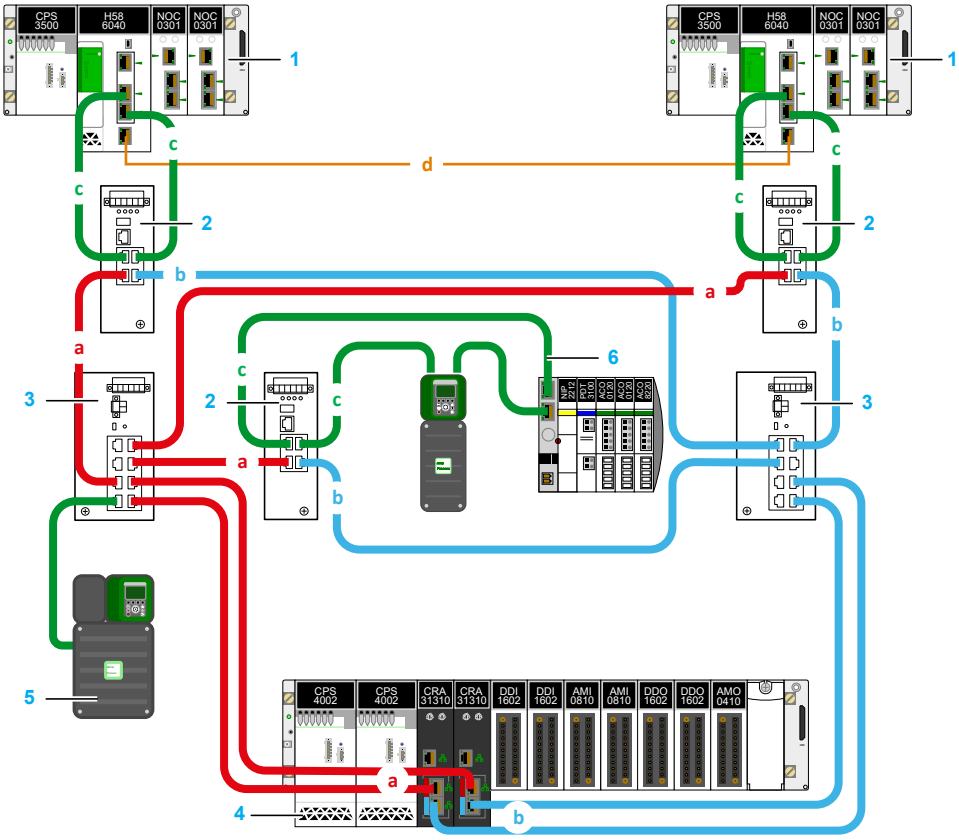
Connecting Distributed Equipment

In network management perspective, distributed equipment are SANs. There are two methods for connecting distributed equipment to the PRP network with their advantages and limitations.

A first method is to connect the distributed equipment using one of the Ethernet switches (item 5 of the below representation). In this case, it can communicate to the other devices on the LAN it is connected to and does not benefit from the PRP network redundancy.

A second method is to connect the distributed equipment behind a Modicon Redundancy switch (item 6). In this case there is no LAN restriction for communicating and it benefits from the redundancy of the PRP network.

Do not connect a DIO on the service port of a BMECRA31310(H) adapter module. More generally the service port is mainly provided for access to external tools and devices for configuring and diagnosing (Control Expert, ConneXium Network Manager, HMI, and so forth).



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode)
5 DIO connected to the LAN A through a Modicon switch
6 DIOs connected to the PRP network through a Modicon Redundancy switch

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

> **NOTE:** The BMENOS0300 module is not supported in an X80 RIO drop managed by BMECRA31310(H) adapter module(s) and cannot be used to connect distributed equipment to the PRP network.

Integrating non-PRP RIO Drops

Overview

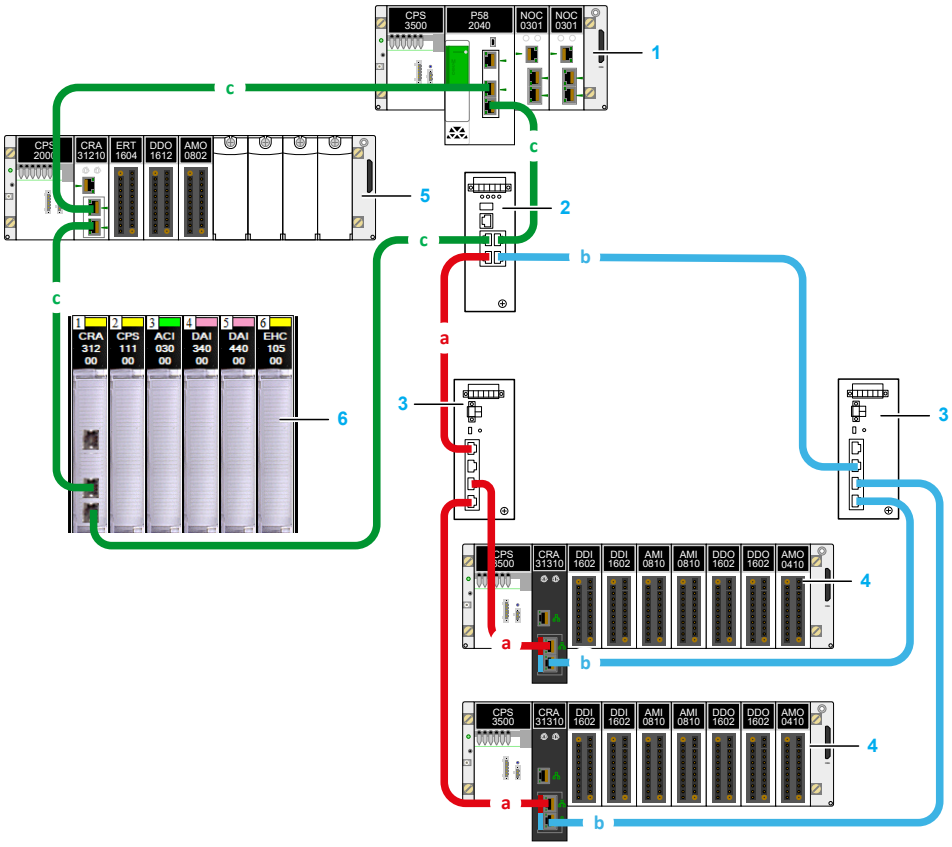
The BMXCRA31200, BMXCRA31210, BMECRA31210 and 140CRA31210 adapter modules are non-PRP devices. They manage RIO drops that can be integrated in the PRP network using a dedicated Modicon Redundancy switch.

In a standalone architecture alternative solutions are also possible for integrating RIO drops.

Standalone Architecture

There are two methods for connecting non-PRP RIO drops in a standalone architecture.

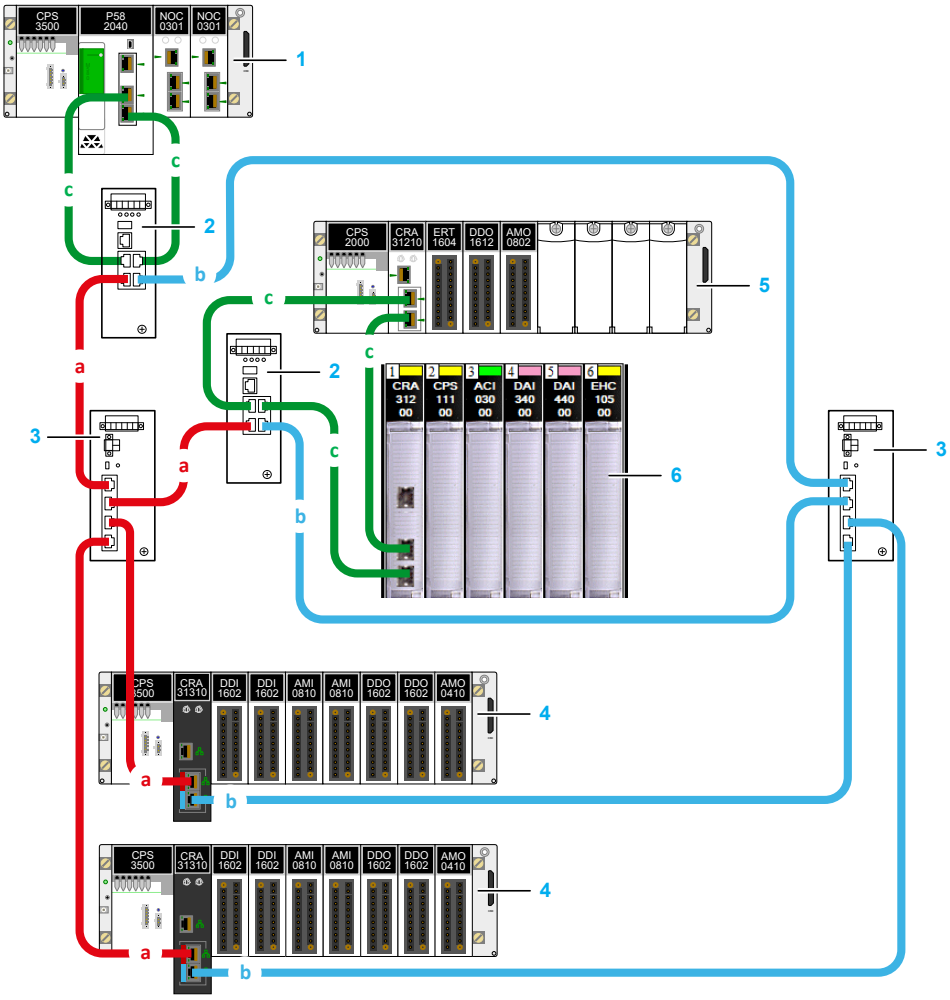
The first method is to connect the non-PRP RIO drops in the ring (RSTP LAN) built with the Ethernet I/O scanner of the M580 controller and the Modicon Redundancy switch allowing connection of the controller to the PRP network. In this ring the number of hops is limited to 31.



1 Modicon M580 local rack
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with a BMECRA31310(H) adapter module
5 X80 RIO drop with a BM•CRA312•0 adapter module
6 Quantum RIO drop with a 140CRA31210 adapter module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

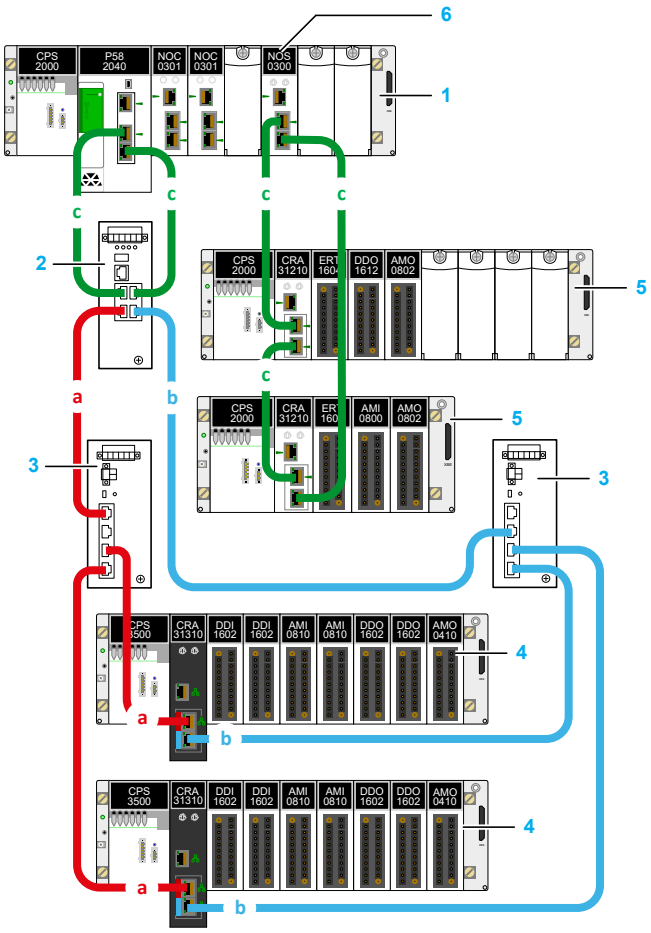
The second method is to connect the non-PRP drops behind a dedicated Modicon Redundancy switch.



1 Modicon M580 local rack
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with a BMECRA31310(H) adapter module
5 X80 RIO drop with a BM•CRA312•0 adapter module
6 Quantum RIO drop with a 140CRA31210 adapter module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

An alternative solution is to connect the non-PRP drops behind a BMENOS0300 module located in the main rack.



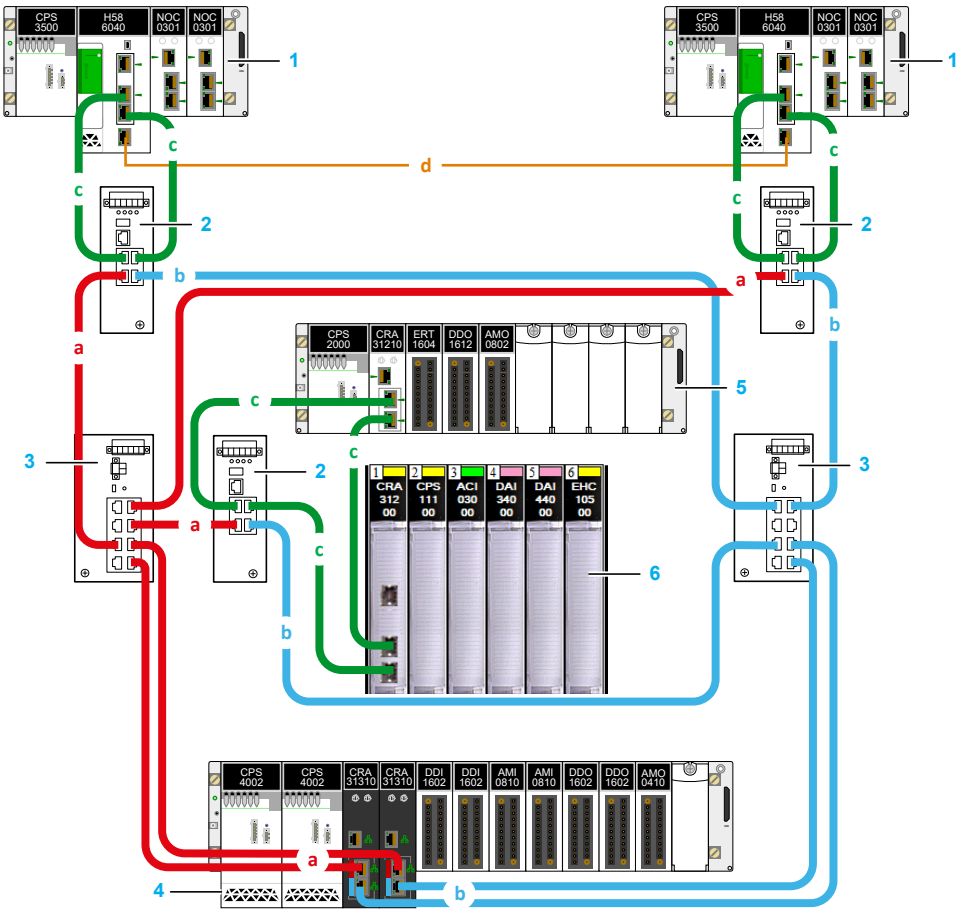
1 Modicon M580 local rack
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drops with BMECRA31310(H) adapter module
5 X80 RIO drops with BMECRA31210 adapter module
6 BMENOS0300 module connecting X80 RIO drops with BM•CRA312•0 adapter modules in a daisy chain

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

NOTE: The BMENOS0300 module is not supported in an X80 RIO drop managed by BMECRA31310(H) adapter module(s) and cannot be used to connect distributed equipment to the PRP network. Examples are provided in the chapter Incompatible RIO Sub-ring Connections, page 32.

High-availability Architecture

In high-availability architecture a dedicated Modicon Redundancy switch connects non-PRP RIO drops to the PRP network:



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode)
5 X80 RIO drop with a BM•CRA312•0 adapter module
6 Quantum RIO drop with a 140CRA31210 adapter module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

Incompatible Architectures

What's in This Chapter

Incompatible BMECRA31310(H) Module Connections

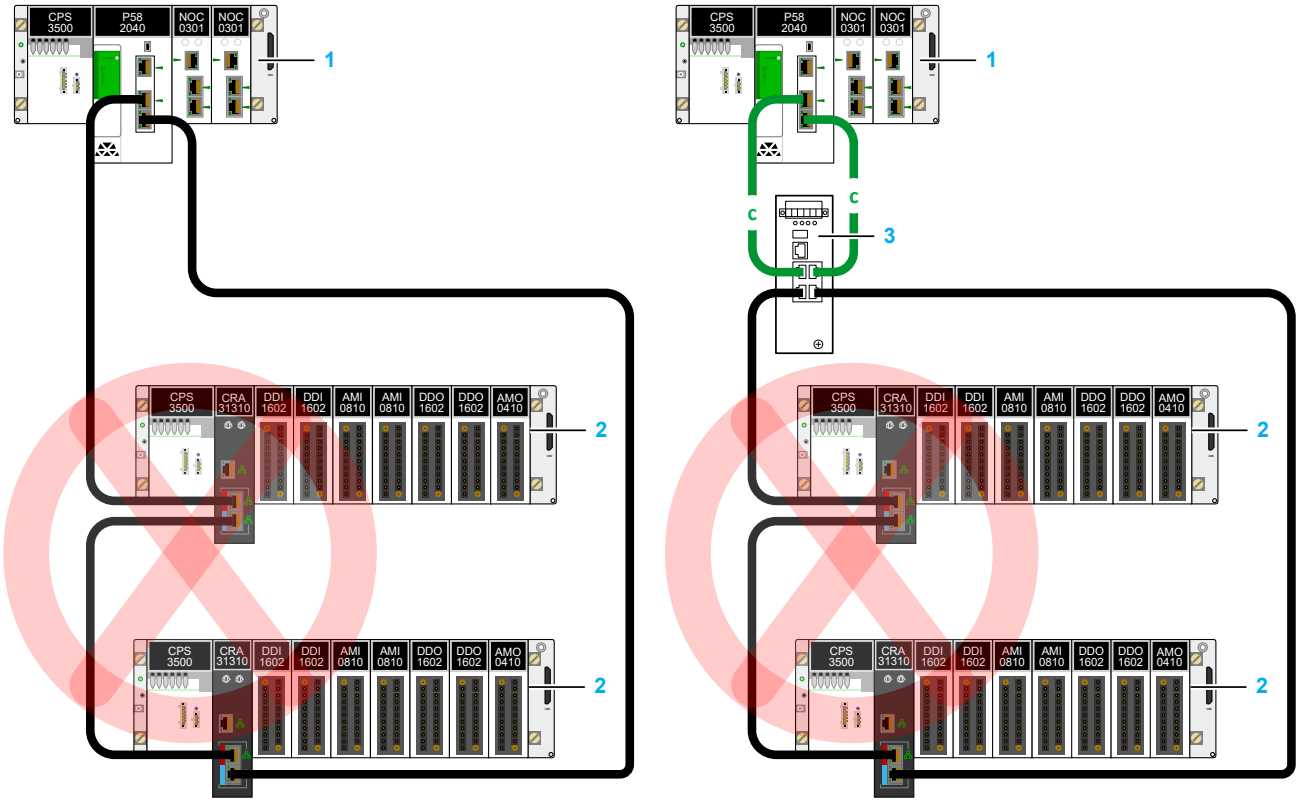
Overview

The BMECRA31310(H) adapter module do not support RSTP. Both redundant device network port A and B of the BMECRA31310(H) adapter module have to be connected to both independent networks LAN A and LAN B. This is also the case for the connection of the Modicon Redundancy switch.

NOTE: If you need to use RIO network architectures supporting RSTP, use BM•CRA312•0 adapter modules. Refer to *Modicon M580, RIO Modules, Installation and Configuration Guide* for additional information.

Standalone Architecture

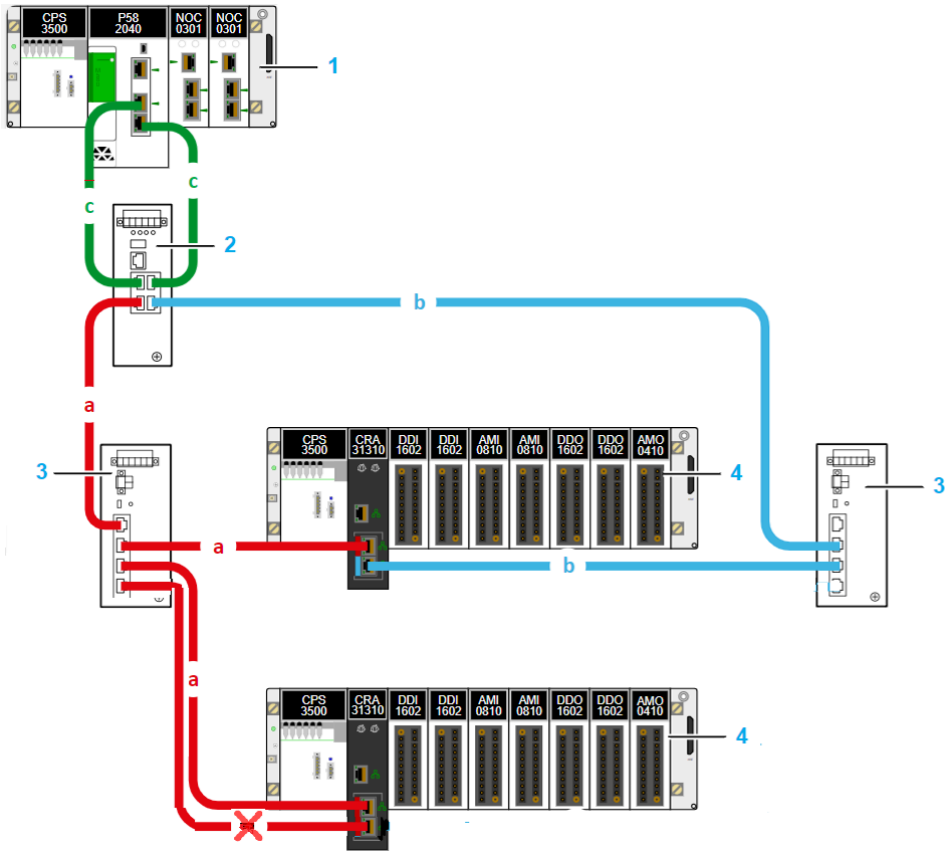
You cannot create a daisy-chain loop with X80 RIO drops managed by BMECRA31310(H) adapter modules. Neither directly connected to the Ethernet I/O scanner of the controller, nor connected to a Modicon Redundancy switch.



1 Modicon M580 local rack
2 X80 RIO drop with one BMECRA31310(H) adapter module (single mode)
3 Modicon Redundancy switch

Network legend:
c RSTP LAN – green

You cannot connect a BMECRA31310(H) adapter module directly to the PRP network as shown in the following illustration:

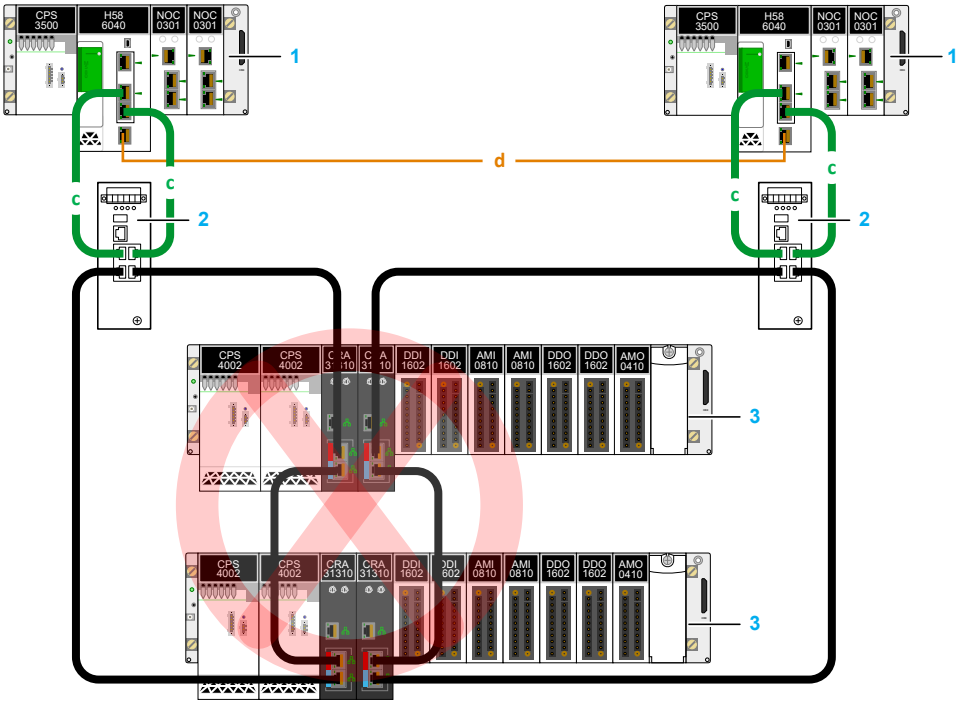


1 Modicon M580 local rack
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with one BMECRA31310(H) adapter module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

High-availability Architecture

The principles that make daisy-chain loop incompatible in designing the PRP network apply in high-availability architectures as illustrated below:



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode)

Network legend:
c RSTP LAN – green
d Hot standby communication link – orange

Incompatible Ethernet Switch Connections

In the PRP network, the connection between LAN A and LAN B only operates at a node level (DAN, RedBox).

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

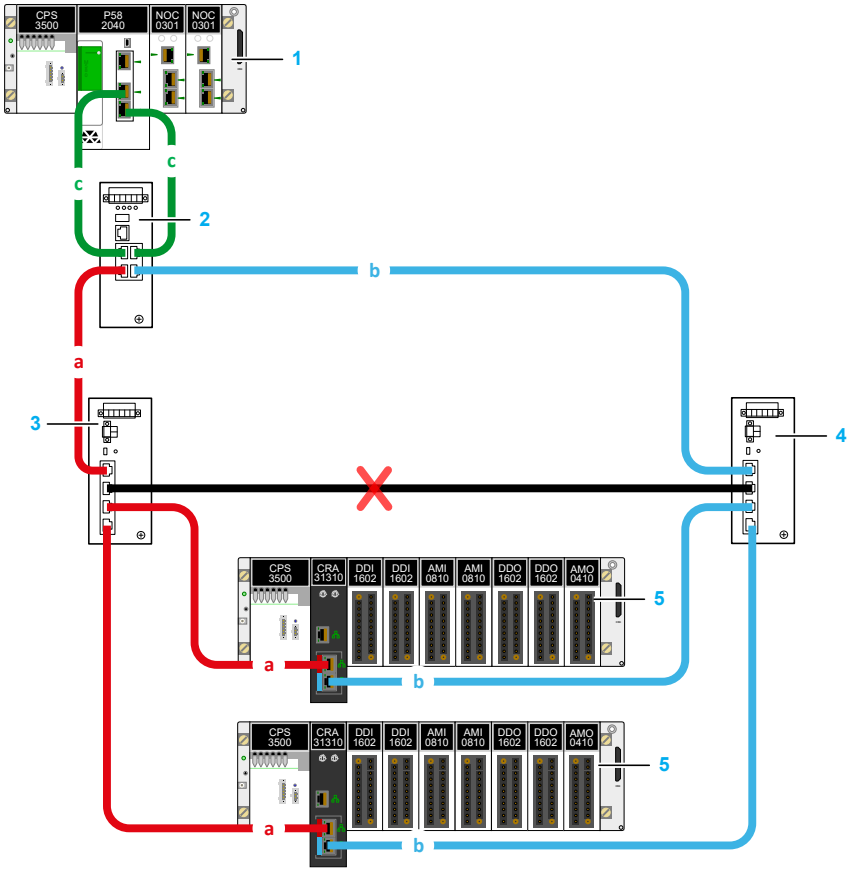
Do not connect LAN A to LAN B either directly or through a switch/hub.

Failure to follow these instructions can result in overload the network.

NOTE: Do not connect LAN A to LAN B either directly or through a switch/hub as this can result in an overload of the network, resulting in an error reaction from the M580 system.

You cannot connect a switch participant in the LAN A infrastructure to a switch participant in the LAN B infrastructure using:

- A direct link (as illustrated below), nor
- A non-PRP switch, nor
- Non-PRP ports of a device.



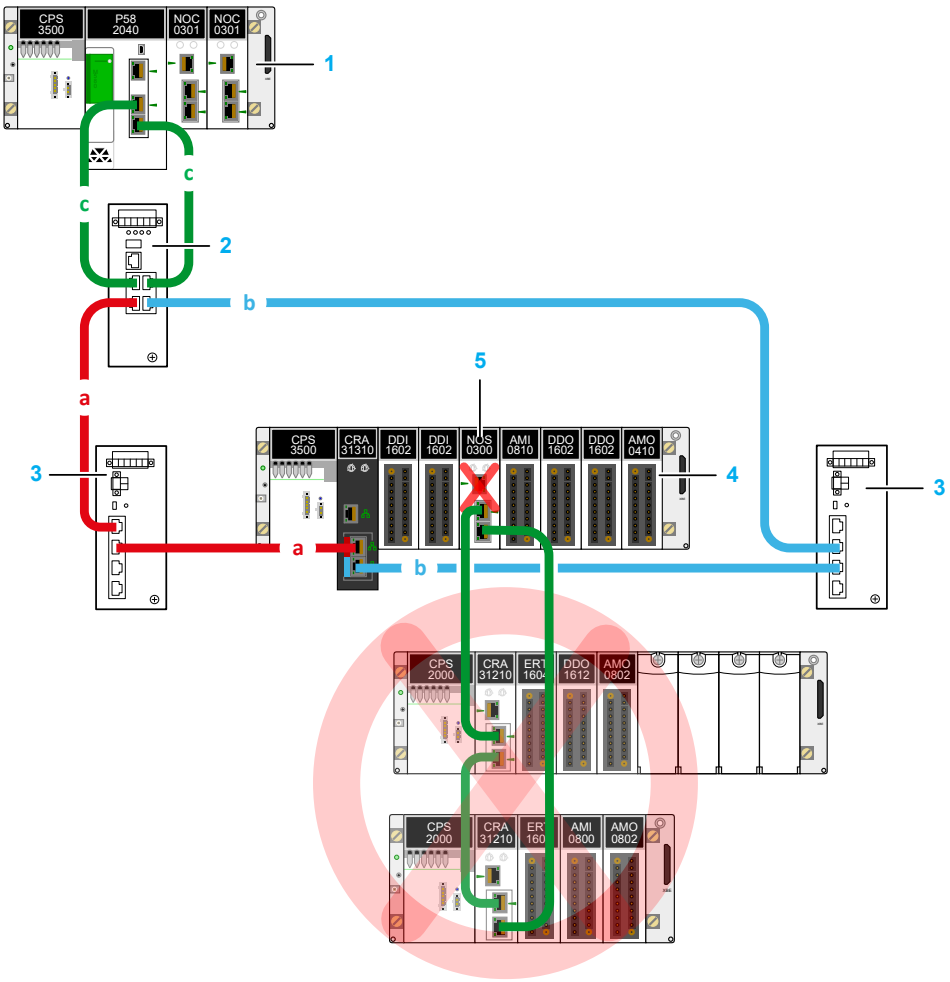
1 Modicon M580 local rack
2 Modicon Redundancy switch
3 Modicon switch for LAN A infrastructure
4 Modicon switch for LAN B infrastructure
5 X80 RIO drop with one BMECRA31310(H) adapter module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

Incompatible RIO sub-ring Connections

Standalone Architecture

In standalone architecture you cannot connect an RIO sub-ring to a BMENOS0300 located on an X80 RIO drop managed by a BMECRA31310(H) adapter module as illustrated below:

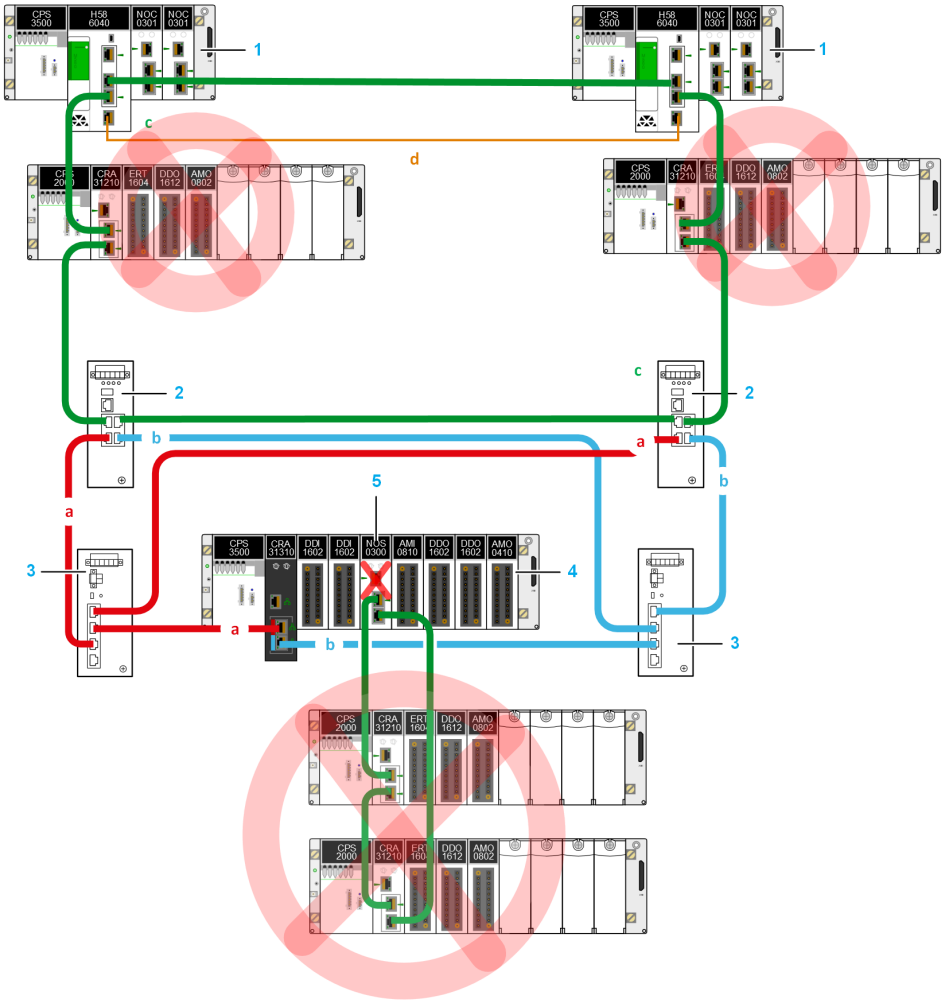


1 Modicon M580 local rack
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with a BMECRA31310(H) adapter module
5 RIO sub-ring connected to a BMENOS0300 module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

High-availability Architecture

In high-availability architecture you cannot connect an RIO sub-ring to a BMENOS0300 located on an RIO drop managed by one or two BMECRA31310 (H) adapter modules:



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with one BMECRA31310(H) adapter module (single mode)
5 X80 RIO sub-ring connected to a BMENOS0300 module

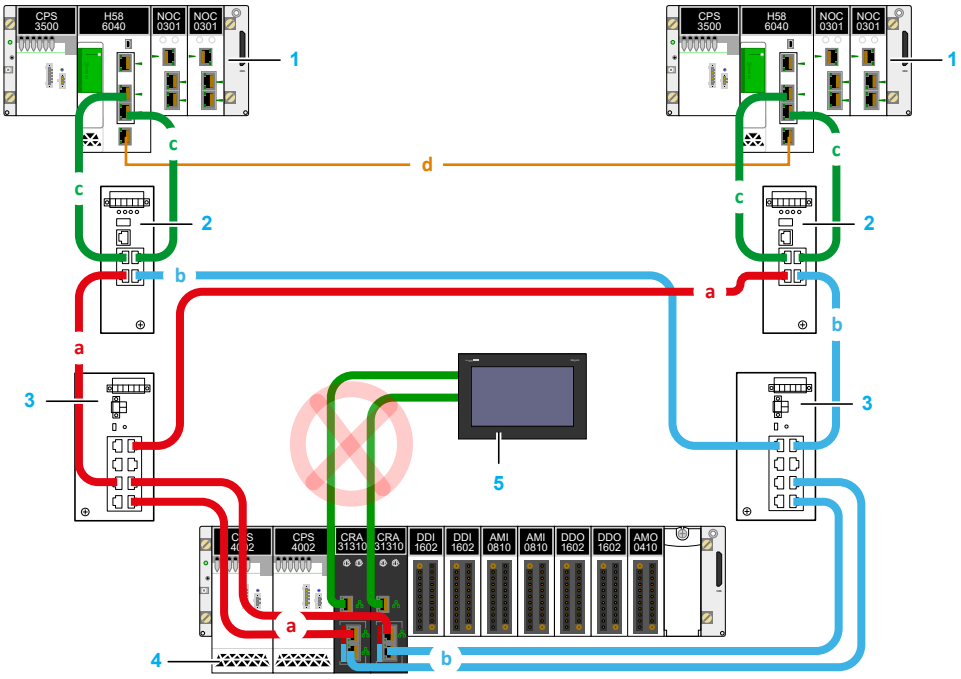
Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

Incompatible Distributed Equipment Connections

Follow the cabling rules to help avoid non-supported loops triggering broadcast storms. As the service ports do not support RSTP, connecting the service port of both BMECRA31310(H) adapter modules of an X80 RIO drop (redundant mode) in a daisy chain loop does not provide path redundancy. If you create such a loop, a broadcast storm can overload the network and delay or prevent the intended network communications.

NOTE: Do not create a daisy chain loop by connecting distributed equipment to the service port of both BMECRA31310(H) adapter modules of an X80 RIO drop in redundant mode. Doing so can create a broadcast storm and overload the network, resulting in an error reaction from the M580 system.

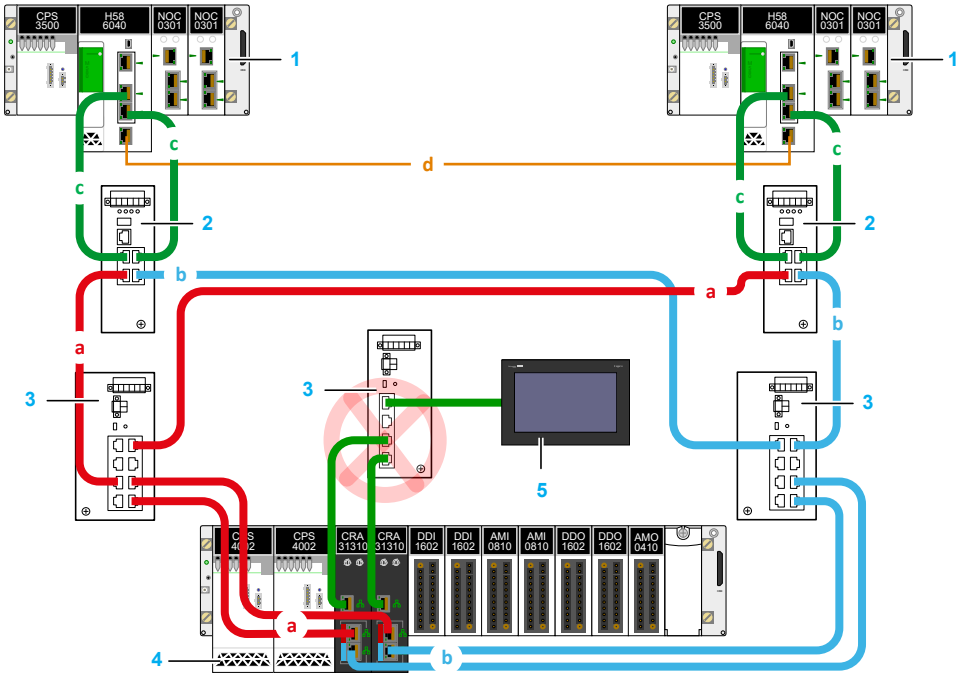
In redundant mode you cannot connect the service ports of both BMECRA31310(H) adapter modules to the same device as illustrated below:



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode)
5 HMI connected to the service port of both BMECRA31310(H) adapter modules

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

This cabling rule also applies when connecting distributed equipment through a Modicon switch as illustrated below:



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch connected to the service port of both BMECRA31310(H) adapter modules
4 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode)
5 HMI connected to the Modicon switch

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

> **NOTE:** In redundant mode, when connecting distributed equipment to the service port of one adapter module, there is an interruption of communication in case of switchover, page 106.

Network Design and Configuration

What's in This Chapter

Guidelines and Rules

When a DAN receives the first of the two duplicated PRP frames, it stores the RTC (Redundancy control trailer) in a dedicated buffer in order to be able to recognize and discard the second frame. This buffer being limited in size, the time between the original and the duplicated frame must not be too long. This time depend on several parameters (traffic rate, latency, number of hops …).

To establish a stable and predictable level of network performance, follow the rules and limitations provided hereafter.

Guidelines:

- LAN A and LAN B should be similar in topology, network speed, network latency and number of hops. Star or bus topologies are possible.
- Use either copper or fiber optic cables for both LANs. Do not use copper cables for LAN A and fiber optic cables for LAN B.

  NOTE: For cables of the same type, use the same category of cables.
- Use the same brand/model/type of switches on both LANs.

Rules:

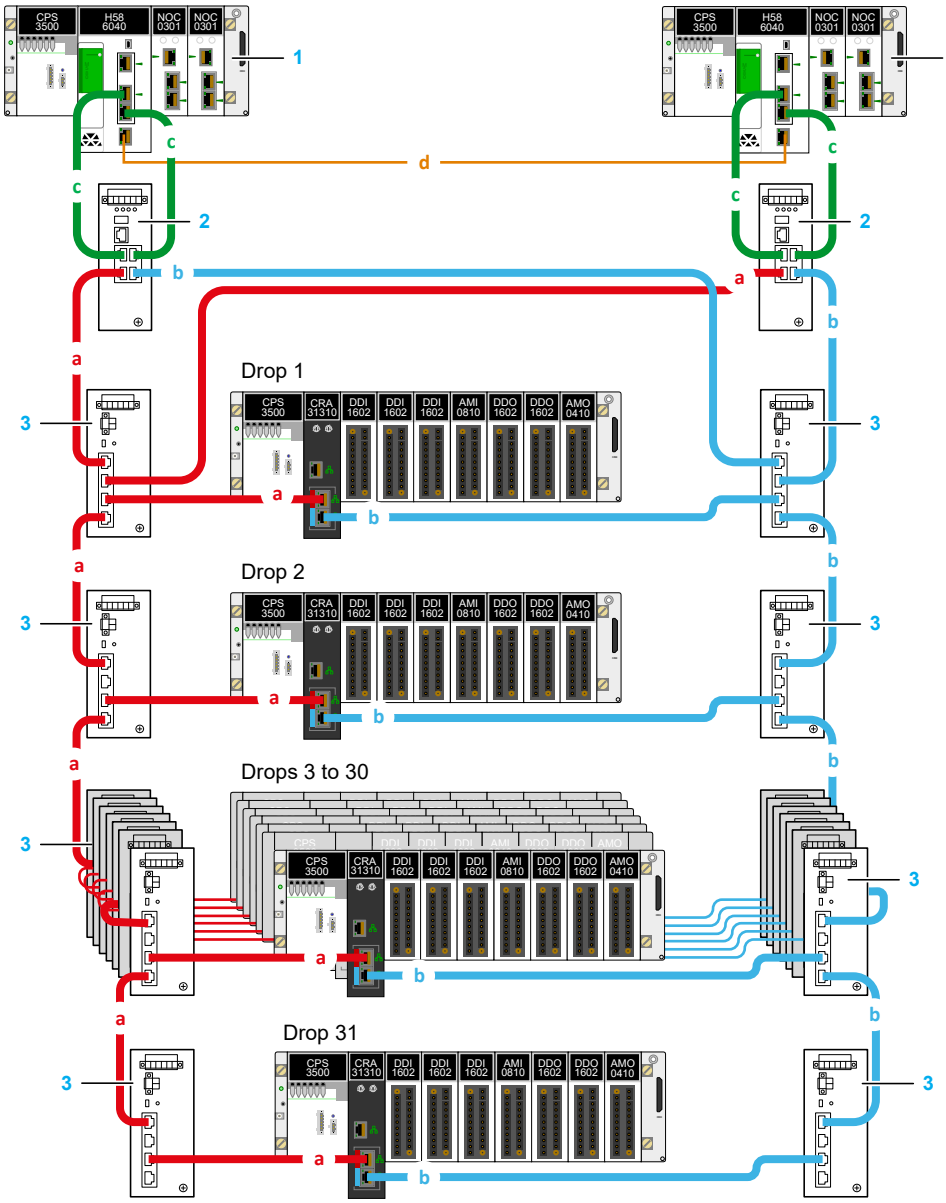
- The difference in number of hops between the controller and the drops in LAN A and in LAN B must not exceed 16.

  NOTE: The number of RIO drops in the network device remains limited to the controller performance in your configuration. For example up to 31 RIO drops with an M580 controller BMEP586040.

Bus Topology - Example 1

In the following bus topology example, each drop is respectively connected to both LAN A and LAN B using 2 dedicated Ethernet switches.

The number of hops (pass through switches along the path) from the M580 controller to a drop is the same over both LAN A and LAN B. Such bus topology follows the symmetry for the LANs.



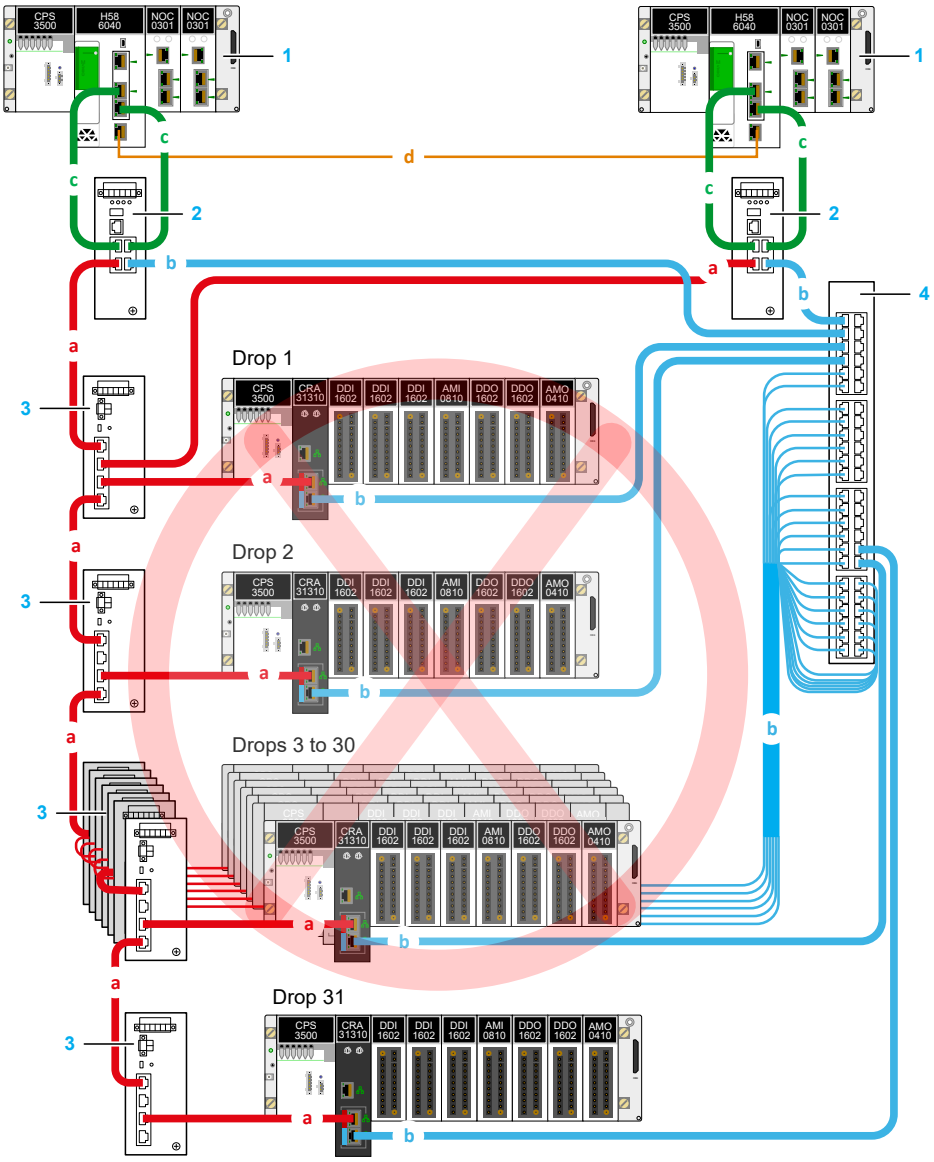
1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link — orange

Bus Topology - Example 2

In the following bus topology example, each drop is connected to the LAN A using a dedicated Ethernet switch whereas all drops are connected to the LAN B using one Ethernet switch.

The difference in number of hops the duplicated Ethernet packets pass through the LAN A and the LAN B is greater than 16 for the drops 17 to 31. Due to this imbalance number of hops, such asymmetrical network architecture is not allowed.



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch for LAN A
4 Modicon switch for LAN B

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link — orange

Network and Traffic Management

Modicon M580 system and the traffic managed in its network is regulated by switch configuration parameters like VLAN Identifier (VLAN-ID), QoS, and DSCP. By default, the VLAN-ID over Modicon M580 device network is VLAN-1.

On the device network, outgoing the controller, the transmitted packets are tagged VLAN-1, the QoS and DSCP related to the traffic usage - BPDU (bridge protocol Data Unit) service packets.

The BMECRA31310(H) adapter module manages the incoming / outgoing packet priority following DSCP / 802.1p marking and tags the packets with the proper DSCP.

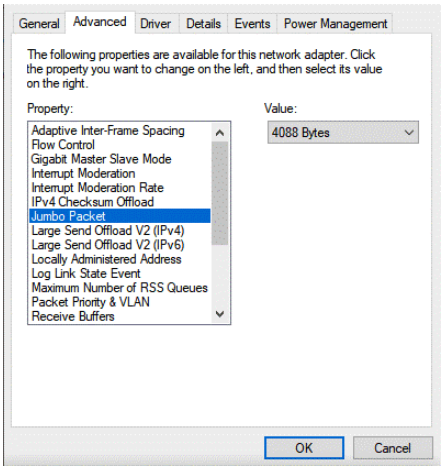
The traffic priority of the Ethernet packets between the M580 controller and the respective X80 RIO drops is set as following values in the table:

QoS Level	DSCP Value	Traffic priority bit (802.1p)	Traffic usage	Network usage
Urgent	55 (110111 bin)	5	Network time protocol (NTP) messaging	Not applicable
Scheduled	47 (101111 bin)	5	Implicit (I/O and safety-related)	Remote I/O (X80 RIO drops, X80 RIO safety-related drops) and CIP safety-related devices)
High	43 (101011 bin)	5	Implicit (I/O)	Distributed I/O (DIO) (EtherNet/IP or Modbus TCP) or controller to controller communication
Explicit	27 (011011 bin)	3	Explicit messaging	Configured equipment
PTP Event	59 (111011 bin)	7	Not applicable	Time synchronization
Other	0 (000000 bin) and other DSCP values	1	Other traffic	Other Messages (for example, DHCP, SNMP, FTP, TFTP, IGMP, SMTP, ICMP, and so on.)

NOTE: You can monitor and diagnose the PRP network infrastructure with SCADA, by programming it in the application, or by using standard network monitoring tool such SNMP server. For detailed information, refer to chapter Module Diagnostics, page 123.

Prerequisite

The Modicon Redundancy switches and Ethernet switches are configured using built-in web pages. To optimize the connection between the PC and the switch for configuring, set up the MTU value of the jumbo frames to 4088 Bytes.

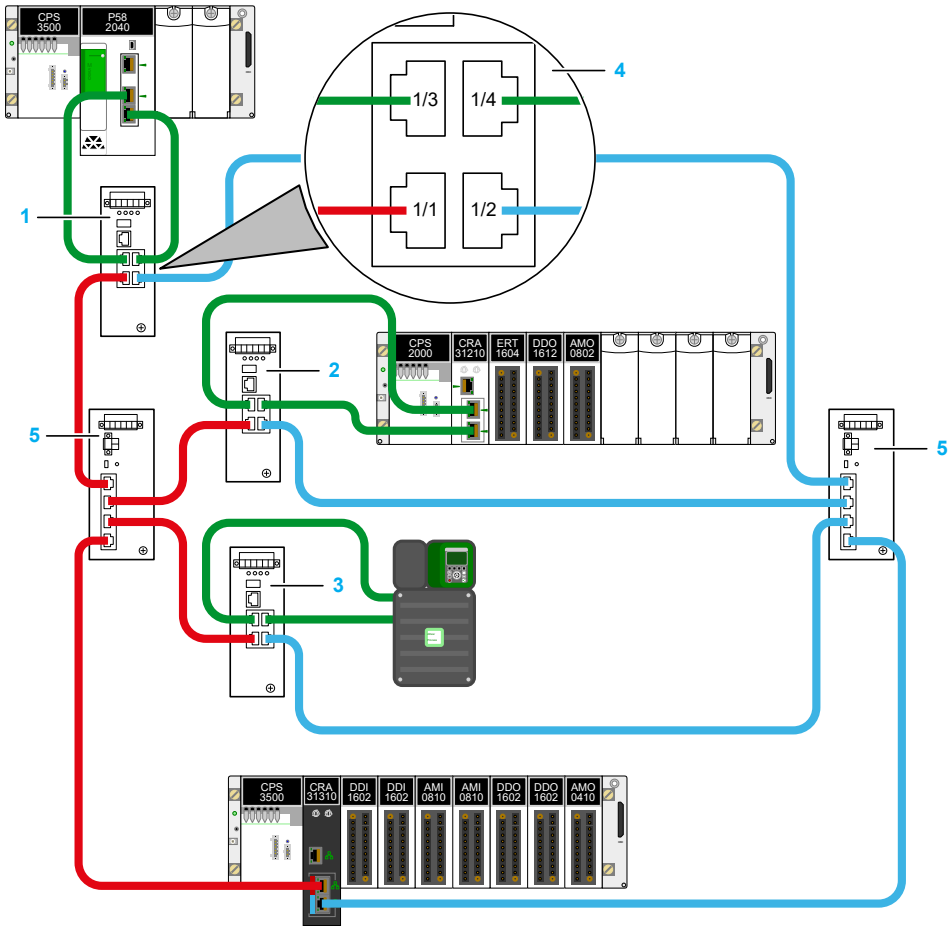
Step	Action
1	Open the **Control Panel**.
2	Click **Network and Internet**.
3	Click **Network and Sharing Center**.
3	On the left side of the Network and Sharing Center window, click **Change adapter settings**. **Result**: The Network Connections window opens.
4	Right-click the connection you are using to connect to the LAN, and select **Properties**. **Result**: The Properties window opens.
5	Click **Configure**. **Result**: The Properties window opens.
6	Select the **Advanced** tab. In the **Property** list, select **Jumbo Packet**. In the **Value** list, select 4088 Bytes. 
7	Click **OK** to apply the settings.

Modicon Redundancy Switch Configuration

Overview

NOTE: Use MCSESR043F2•••(C) Modicon Redundancy switch for connecting non-PRP device to the redundant PRP network.

There are three different types of devices that are connected to Modicon Redundancy switches as illustrated below:



1 Modicon Redundancy switch connecting the Modicon M580 local rack
2 Modicon Redundancy switch connecting an X80 RIO drop managed by a BM•CRA312•0 adapter module
3 Modicon Redundancy switch connecting a DIO
4 Ports location of the Modicon Redundancy switch
5 Modicon switch

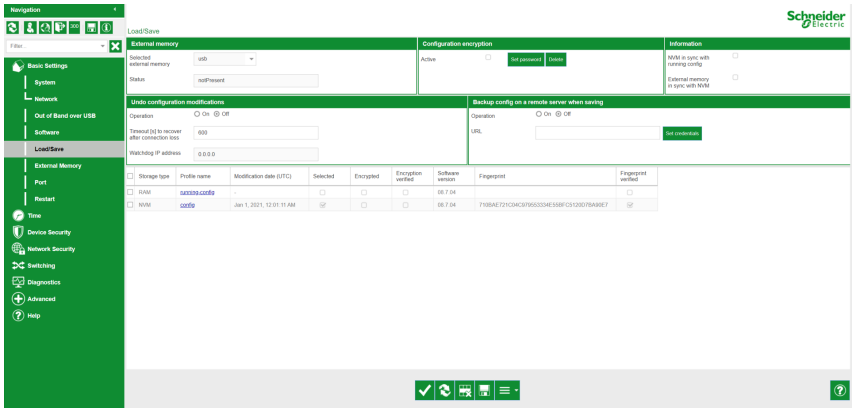
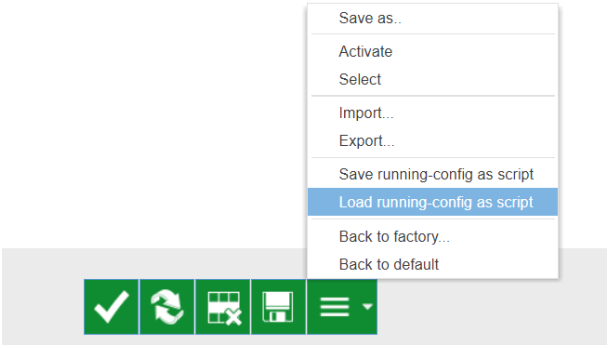
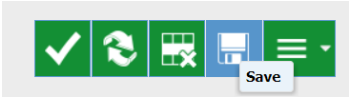
The steps for configuring the Modicon Redundancy are:

- Enabling the PRP function for ports 1/1 and 1/2
- Enabling the **Spanning Tree** function for ports 1/3 and 1/4
- Configuring the data packets transmission for the ports.

  NOTE: The VLAN tagging of the data packets is dependent to the device connected to the Modicon Redundancy switch and its way of communicating.
- QoS/Priority port configuration

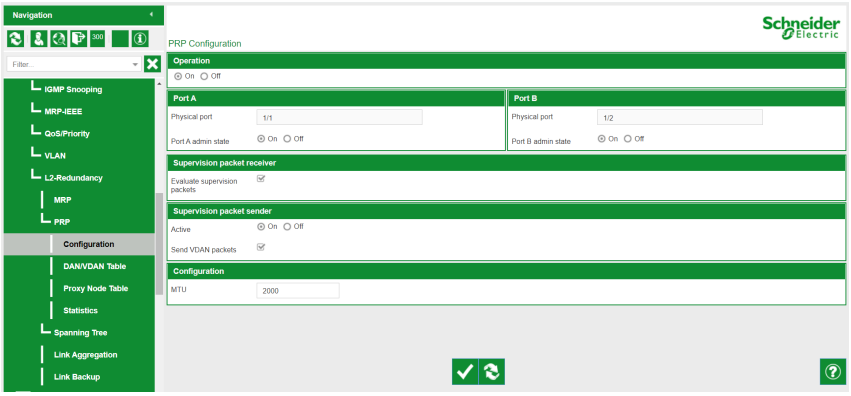
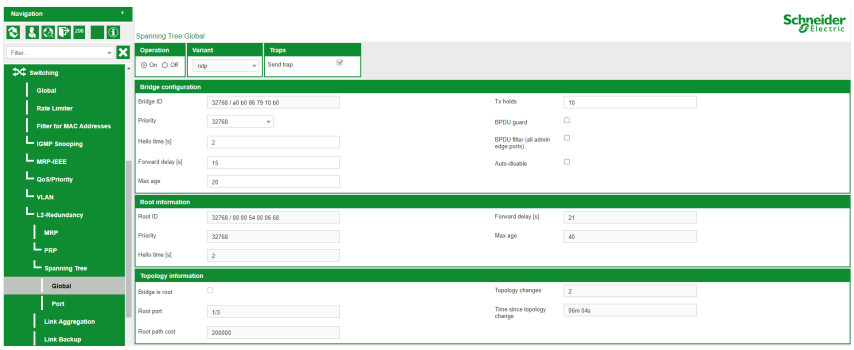
Factory Configuration of the Modicon Redundancy Switches

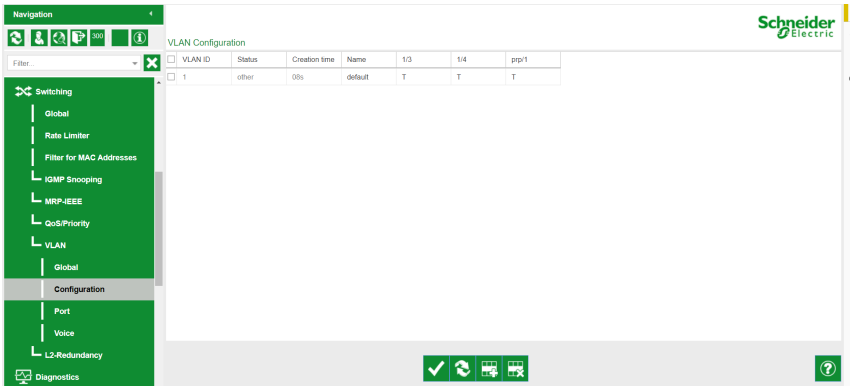
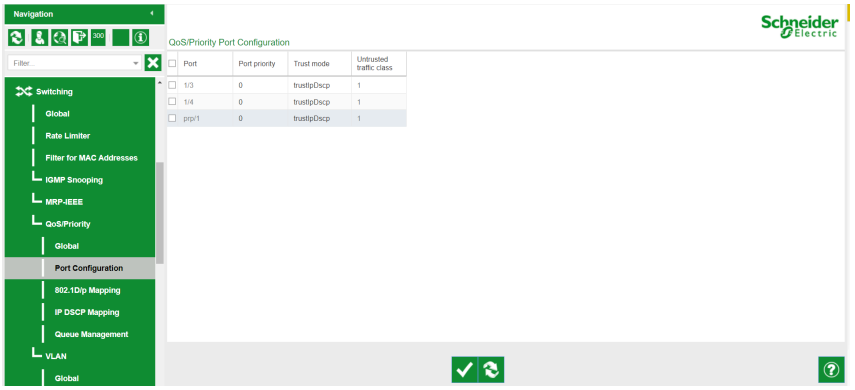
A new switch needs to be configured before it can be used with the Control Expert software.

Step	Action
1	Set the IP address of the switch, refer to Ethernet Switch Configurator Tool, page 49
2	Open an Internet browser and enter the URL: `https://[MCSESR IP address]` **NOTE:** [MCSESR IP address] is the IP address set in step 1. **NOTE:** The browser may display a message stating that the connection is not secure because it is not HTTPS. You can choose to continue by clicking **Advanced** and then clicking **Proceed to IPv4**. This procedure may vary slightly depending on your browser.
3	Enter the default **username/password** combination `admin/private` to login. **NOTE:** On the first login you are required to change the password.
4	On the **Navigation** left pane, select **Basic Settings** > **Load/Save**. 
5	In the bottom ribbon, select **Load running-config as script**. 
6	Select the pre configuration **CLI file** provided in Control Expert Extras folder. 
7	Click **OK** to apply the settings. **Result**: A notification message is displayed to let you know that the configuration has been successful.
8	Save running configuration to non-volatile memory (NVM).  **NOTE:** This is required for the configuration to be automatically re-applied in case of restart.

Manual Configuration

To configure the Modicon Redundancyswitch:

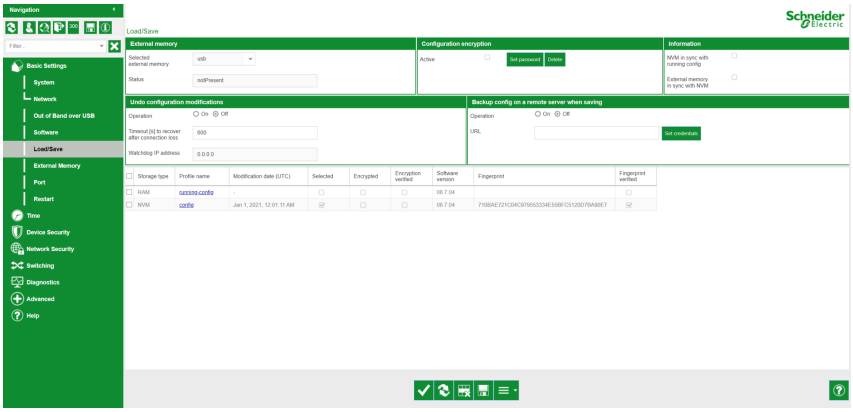
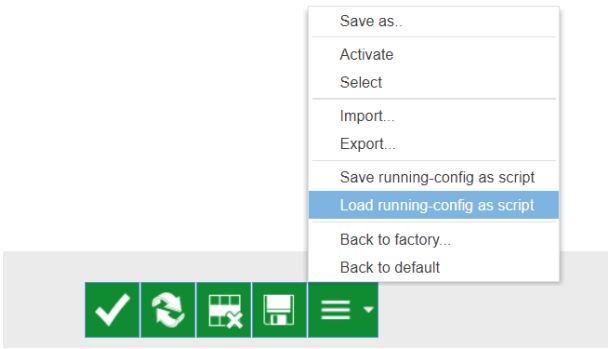
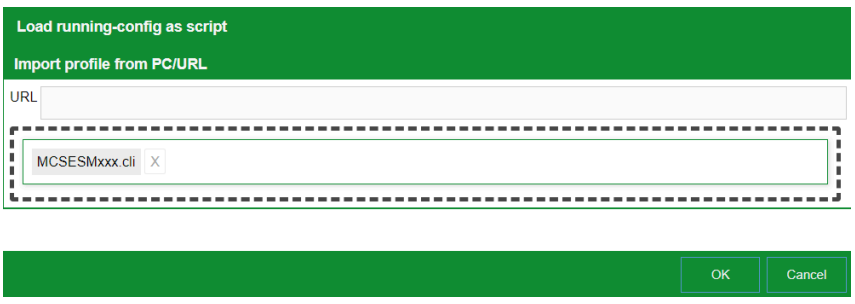
Step	Action
1	Open an Internet browser and enter the following URL: `https://[MCSESR IP address]`
2	Enter the **username/password** combination. **NOTE:** On the first login you are required to change the password. In that case, use the default **username/password** combination `admin/private` to log in.
3	To enable the PRP function:  A. On the **Navigation** left pane, select **Switching > L2 Redundancy > PRP > Configuration**. B. In the **Operation** area, select **On**. When PRP is active, it uses the interfaces `1/1` and `1/2`. **NOTE:** The PRP function replaces the interfaces `1/1` and `1/2` with the interface `prp/1` in the configuration window for VLAN and QoS/Priority port. C. Verify that the `MTU` value in the configuration area is greater than 1524 bytes (the default value is set to 2000 bytes). D. Click the icon to validate.
4	To enable the **Spanning Tree** function:  A. On the **Navigation** left pane, select **Switching > L2 Redundancy > Spanning Tree > Global**. B. In the **Operation** area, select **On**. **NOTE:** The **Spanning Tree** function cannot operate on the same ports as the PRP function. It uses the interfaces `1/3` and `1/4`. C. Click the icon to validate.

Step	Action
5	To configure the ports to transmit the data packets with a VLAN tag:  A. On the **Navigation** left pane, select **Switching > VLAN > Configuration**. B. Set the ports (1/3, 1/4, and prp/1) to tagged member (T) in VLAN 1. **NOTE:** If the Modicon Redundancy switch connects a device that communicates without VLAN tags, set ports 1/3 and 1/4 to untagged member (U) and prp/1 to tagged (T) member. C. Click the ✓ icon to validate.
6	To specify how the Modicon Redundancy switch handles a received data packet based on its QoS/priority information:  A. On the **Navigation** left pane, select **Switching > QoS/Priority > Port Configuration**. B. Set **Trust mode** for the ports (1/3, 1/4, and prp/1) to `trustIpDscp`. **NOTE:** The Modicon Redundancy switch transmits the data packet according to the traffic class assigned to the IP DSCP value contained in the IP header. For traffic class assignment, select **Switching > QoS/Priority > IPDSCPMapping**. C. Click the ✓ icon to validate.

Ethernet Switch Configuration

Factory Configuration of the Ethernet Switch Configuration

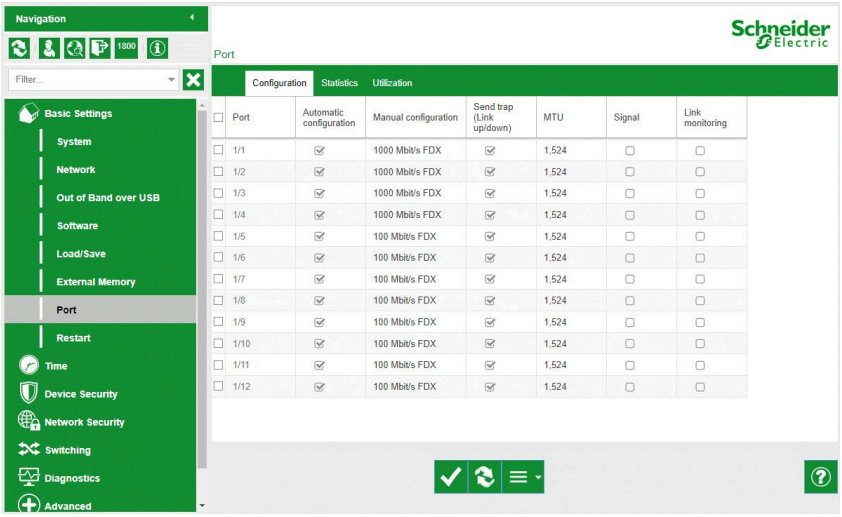
A new switch needs to be configured before it can be used with the Control Expert software.

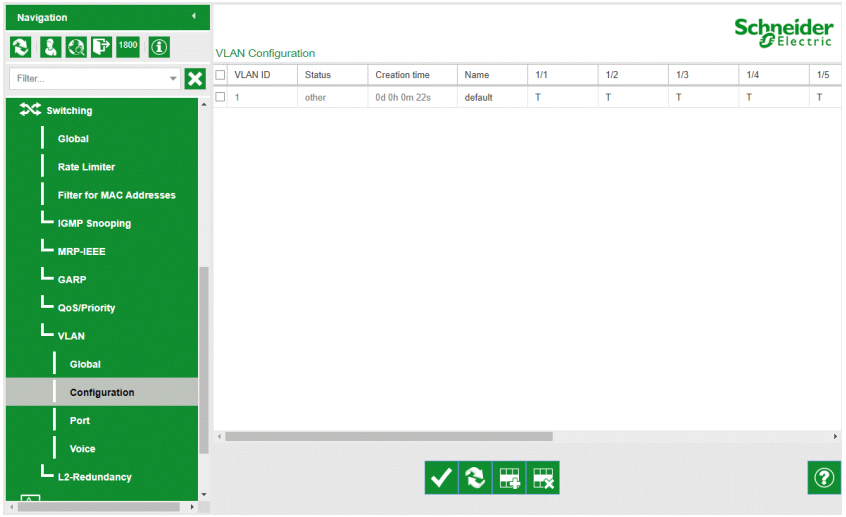
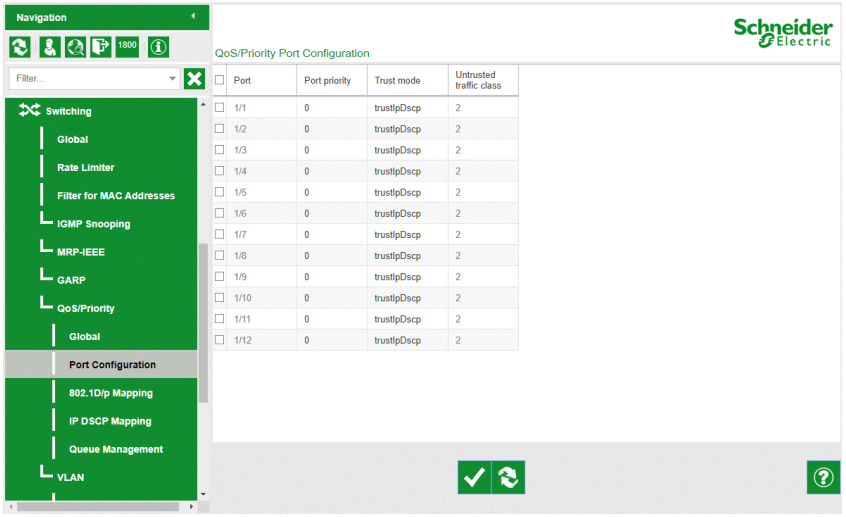
Step	Action
1	Set the IP address of the switch, refer to Ethernet Switch Configurator Tool, page 49
2	Open an Internet browser and enter the URL: `https://[MCSESR IP address]` **NOTE:** [MCSESR IP address] is the IP address set in step 1. **NOTE:** The browser may display a message stating that the connection is not secure because it is not HTTPS. You can choose to continue by clicking **Advanced** and then clicking **Proceed to IPv4**. This procedure may vary slightly depending on your browser.
3	Enter the default **username/password** combination `admin/private` to login. **NOTE:** On the first login you are required to change the password.
4	On the **Navigation** left pane, select **Basic Settings > >Load/Save**. 
5	In the bottom ribbon, select **Load running-config as script**. 
6	Select the pre configuration **CLI file** provided in Control Expert Extras folder. 

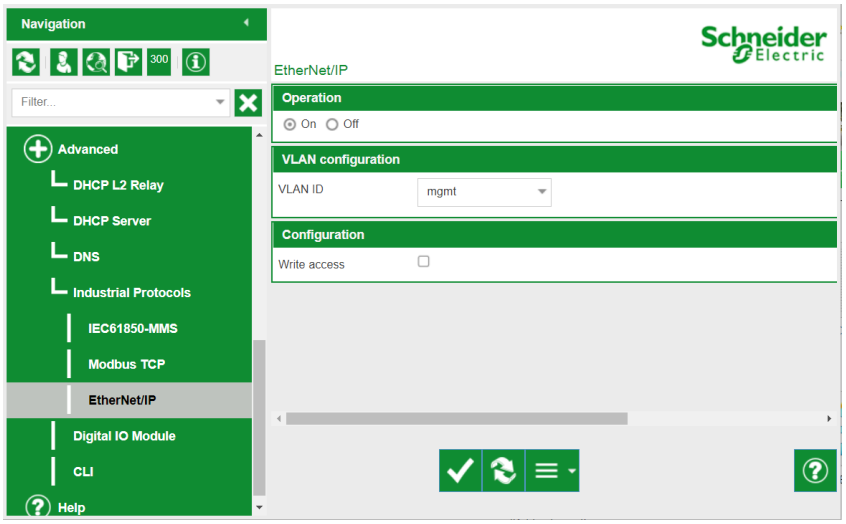
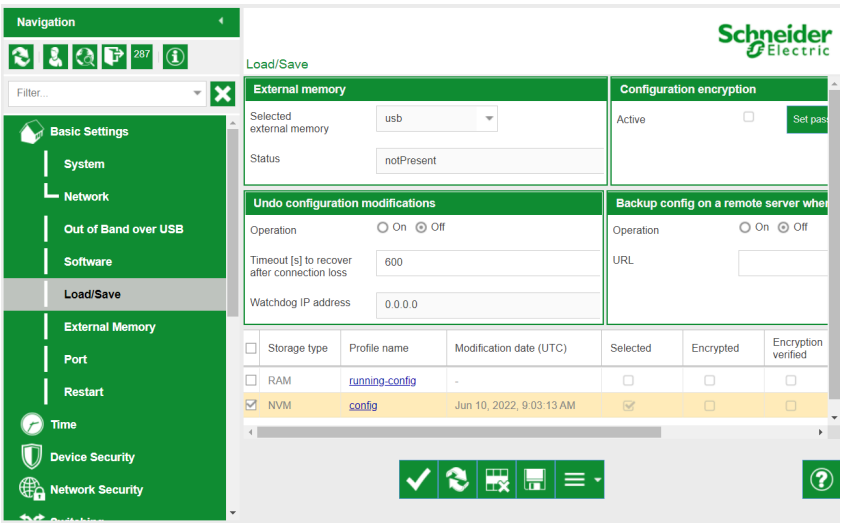
Step	Action
7	Click **OK** to apply the settings. **Result**: A notification message is displayed to let you know that the configuration has been successful.
8	Save running configuration to non-volatile memory (NVM).  **NOTE:** This is required for the configuration to be automatically re-applied in case of restart.

Manual Configuration

To configure the Ethernet switch for a typical setup with a 12TX port:

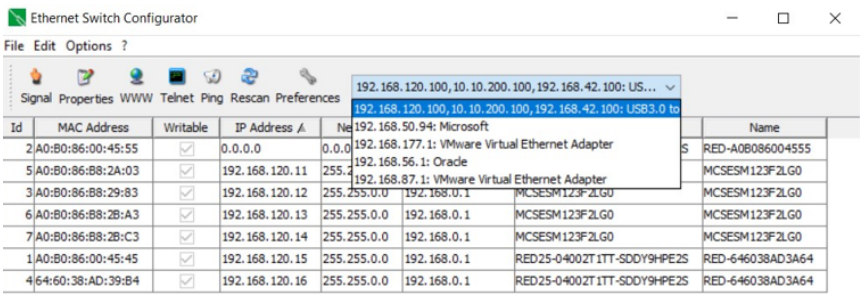
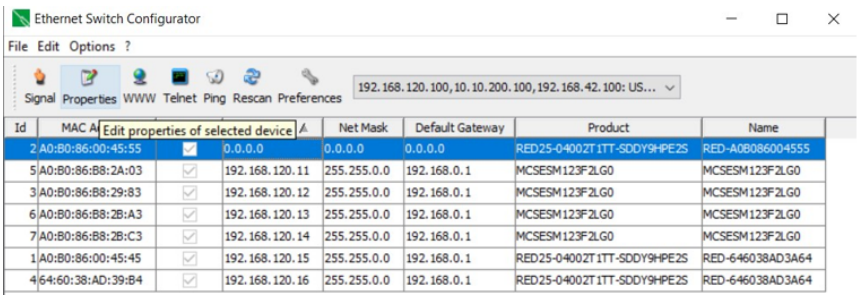
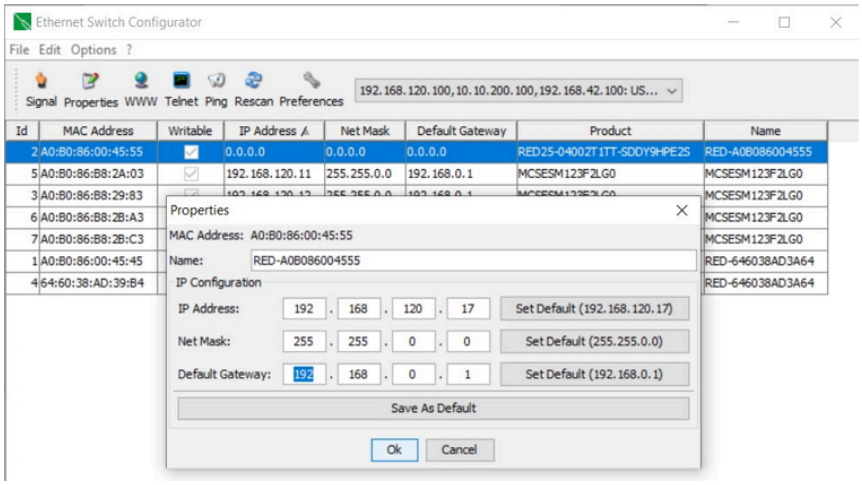
Step	Action
1	Open an Internet browser and enter the following URL: `https://[MCSESR IP address]`
2	Enter the **username/password** combination. **NOTE:** On the first login you are required to change the password. In that case, use the default **username/password** combination `admin/private` to log in.
3	To configure the maximum allowed size of Ethernet packets on the ports:  A. On the **Navigation** left pane, select **Basic Settings** > **Port**. B. In the **Configuration** tab, select the MTU value to 1524 bytes for the ports. C. Click the  icon to validate.

Step	Action
4	To configure the ports to transmit the data packets with a VLAN tag:  A. On the **Navigation** left pane, select **Switching > VLAN > Configuration**. B. Set the ports to tagged member (T) in VLAN 1. **NOTE:** If the Ethernet switch connects an end device that communicates without VLAN tags such as DIO, HMI, set the designated port to untagged member (U). C. Click the ✓ icon to validate.
5	To specify how the Ethernet switch handles a received data packet if the data contains QoS/priority information:  A. On the **Navigation** left pane, select **Switching > QoS/Priority > Port Configuration**. B. Set **Trust mode** for the ports to `trustIpDscp`. **NOTE:** The Ethernet switch uses the QoS information contained in the IP header to determine the traffic class. C. Click the ✓ icon to validate.

Step	Action
6	To enable the EtherNet/IP function in the switch for diagnostic purpose:  **1.** On the **Navigation** left pane, select **Advanced** > **Industrial Protocols** > **EtherNet/IP**. **2.** In **Operation**, select **On** for enabling the EtherNet/IP function. **3.** In **Configuration**, deactivate the write access of the EtherNet/IP protocol. (Only get requests are accepted by the EtherNet/IP protocol). **4.** Click the icon to validate.
7	To define the configuration profile for loading and saving the switch settings:  A. On the **Navigation** left pane select **Basic Settings** > **Load/Save**. B. In the **Storage type** table, select **NVM**. **NOTE:** In case of restart the switch loads the configuration profile from the non-volatile memory. C. Click the icon to save your changes.

Ethernet Switch Configurator Tool

Follow these steps to set the IP address of the switch:

Step	Action
1	Open the Ethernet Switch Configurator tool. **NOTE:** If required, change the network interface connection to be used for scanning. 
2	Select the Ethernet switch you want to configure and click **Properties**. 
3	Set the desired **IP address**, **Net Mask** and **Default Gateway**. 
4	Click **OK** to apply the settings. **Result:** The IP address is configured.

Installation and Configuration

What’s in This Part

Installation and Configuration

What's in This Chapter

Installing and Configuring the Module

Introduction

This chapter describes how to select an operating mode and install the X80 RIO drop redundant communication adapter on PRP network technology modules (BMECRA31310 and BMECRA31310H).

Installing and Configuring the Module

The following outline presents a sequence of tasks for installing and configuring the module:

1. Install the equipment, refer to Module Installation and Cabling, page 61.
2. Install the Power Supplies. For more information on Power Supply Modules Installation, refer to *Modicon X80 Racks and Power Supplies, Hardware, Reference Manual*.
3. Configure the Modicon Redundancy Switch, refer to Modicon Redundancy Switch Configuration, page 41.
4. Configure the Ethernet Switch, refer to Ethernet Switch Configuration, page 45.
5. If necessary, update the firmware module, refer to Module Firmware Update, page 145.
6. Configure the Control Expert application, refer to Module Configuration, page 75.
7. Deploy the application to controller.
8. Wire RSTP Loop to Modicon Redundancy switch.
9. Wire PRP LAN A, and then LAN B.
10. Perform Module Diagnostics, refer to Module Diagnostics, page 123
11. Wire your SCADA/Monitoring loop.

Module Presentation and Installation

What's in This Part

Modules Characteristics

What's in This Chapter

This chapter describes the BMECRA31310(H) module including physical characteristics, port descriptions, and environmental operating conditions. The list of compatible modules you can install in the RIO drop managed by the redundant adapter module is also provided in this chapter.

Module Description

Functionality

The X80 RIO drop redundant communication adapter PRP module BMECRA31310(H) connects the device using the Parallel Redundancy Protocol (PRP) technology to the network.

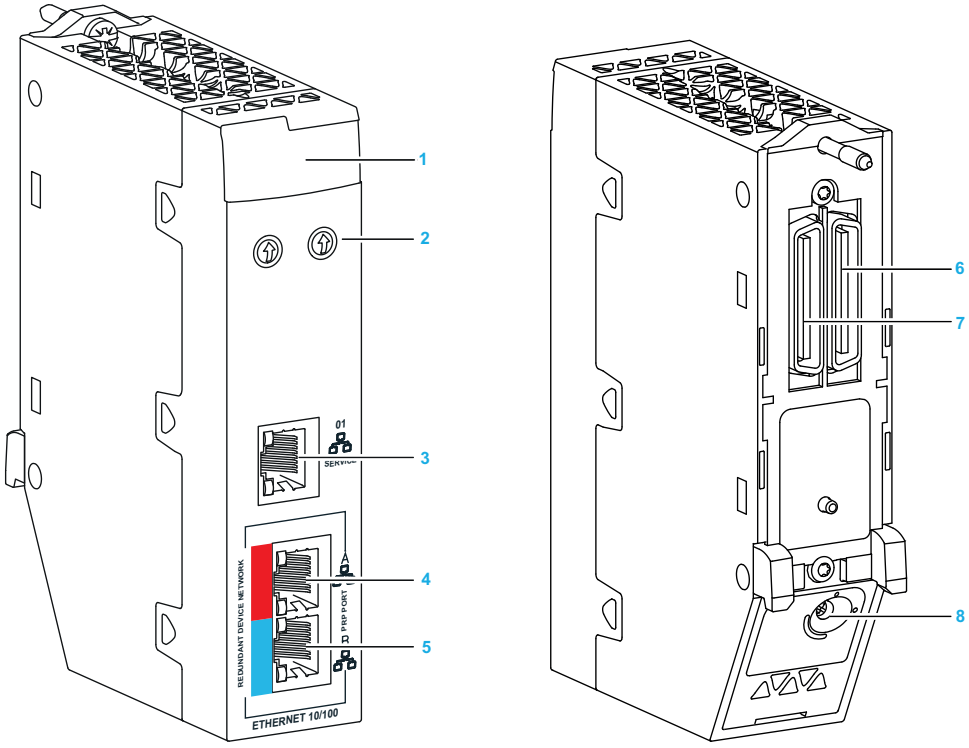
The adapter module exchanges data through the Ethernet I/O scanner service in the controller on the main local rack of the controller system:

- The input data from the RIO drop is collected and published to the I/O scanner.
- The output modules are updated with the data received from the I/O scanner.
- The protocol used for exchange is EtherNet/IP.
- The exchanges are deterministic, which means that the RIO logic is scanned regularly in a scheduled and predictable manner.

Adapter Module Redundancy

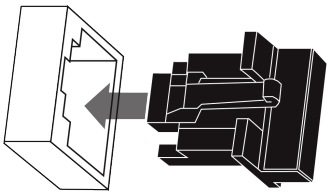
Two adapter modules configured in the RIO drop (with high-availability Modicon M580 controller) allows redundancy of the adapter module. A switchover occurs if the adapter module operating as the MASTER role is detected to be in error.

External Features

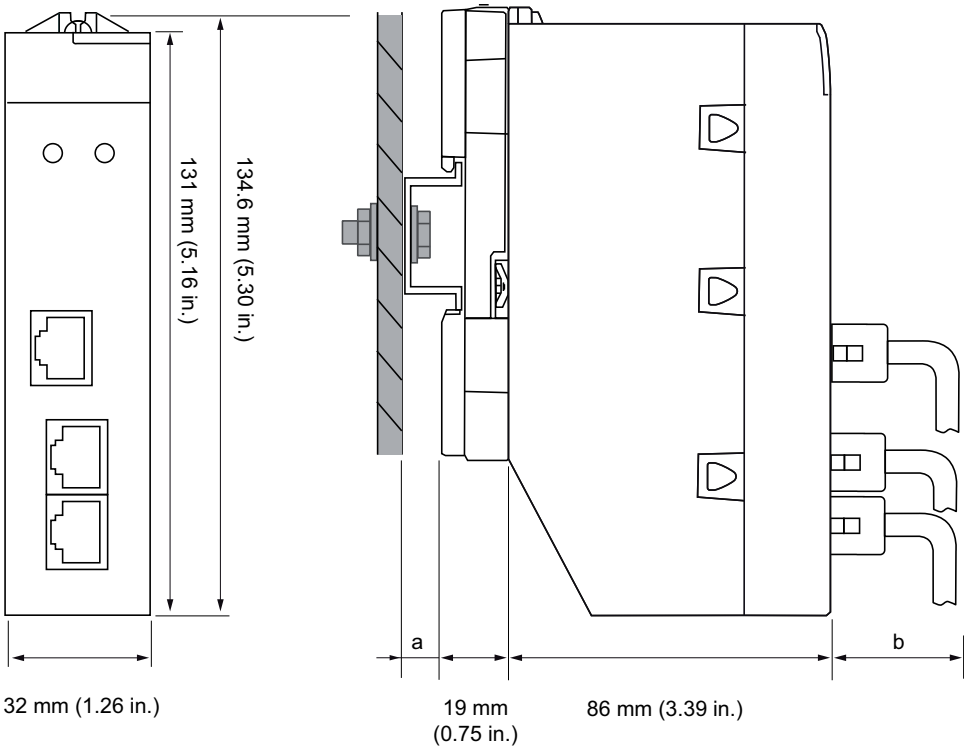


1 LED display
2 Rotary switches for device name
3 Service port (ETH 1)
4 Redundant Device Network PRP port A (LAN A- red marking)
5 Redundant Device Network PRP port B (LAN B- blue marking)
6 Ethernet backplane port
7 X bus backplane port
8 Rotary selector (reserved)

NOTE: Insert dust covers into the unused Ethernet ports on the adapter modules:



Dimensions



a DIN-rail depth: the value depends on the DIN-rail type used in your platform.
b Wiring depth: the value depends on the connector and the wires used in your platform.

Power Consumption

The BMECRA31310(H) adapter module consumes an average current of 140 mA on the backplane distributed voltage 3.3 V.

Ruggedized Versions

The BMECRA31310H (hardened) equipment is the ruggedized version of the BMECRA31310 (non-hardened) equipment. With conformal coating of the electronic boards, the hardened equipment can be used at extended temperatures -25...+70 °C (-13...+158 °F) and in harsh chemical environments.

For more information, refer to chapter *Installation in More Severe Environments* (see Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications).

Altitude Operating Conditions

The characteristics apply to the BMECRA31310(H) modules for use at altitude up to 2000 m (6560 ft). When a module operates above 2000 m (6560 ft), apply additional derating.

For detailed information, refer to chapter *Operating and Storage Conditions* (see Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications).

LED Description

Module LED Display

The LEDs are on the front of the adapter module:

LED Flash Rate

LED flashing rate:

- 200 ms ON
- 200 ms OFF

LED Description

LED	Color	Description
RUN	Green	The RUN LED indicates that outputs are managed by the controller (the controller is in RUN). • On: the module is in RUN mode • Flashing: the module is in STOP mode
I/O	Red	The I/O LED indicates a detected error that originates from a module of the drop (external error, internal error, configuration error). • Off: no error detected from modules of the drop • On: configuration error or missing module(s) in the drop
MS	Bi-color Green/ Red	The MS (Module Status) LED indicates an error is detected in the adapter module. • Off: the module is off • Green on: the module is operating correctly • Flashing green: the module is not configured • Red on: a non-recoverable error is detected • Flashing red: a recoverable error is detected
NS	Bi-color Green/ Red	The NS (Network Status) LED indicates the status of the Ethernet connection. • Off: no IP address has been assigned to the module • Green on: the module has established at least one CIP connection • Flashing green: IP address assigned but no CIP connection have been established • Red on: duplicate IP address detected or the module is downloading a firmware update • Flashing red: owner connection has timed out

LED	Color	Description
MASTER	Bi-color Green/ Red	In redundant mode, the LED indicates the adapter module is assigned to the MASTER role on the backplane I/O Bus. • Off: the module is off or is booting • Green on: the module is assigned to the MASTER role • Flashing green: the module is neither assigned to the MASTER nor NOT MASTER role (module not configured or an error is detected in the module with MASTER role) **NOTE:** Other colors than green for this LED are only used during the power-up sequence of the module.
NoMAS-TER	Bi-color Green/ Red	In redundant mode, the LED indicates the adapter module is assigned to the NOT MASTER role on the backplane I/O Bus. • Off: the module is off or is booting • Green on: the module is assigned to the NOT MASTER role • Flashing green: the module is neither assigned to the MASTER nor NOT MASTER role (module not configured or an error is detected in the module with MASTER role) **NOTE:** Other colors than green for this LED are only used during the power-up sequence of the module.
SEC	Bi-color Green/ Red	The LED is off and reserved. **NOTE:** During the power-up sequence of the module this LED is switched on.

NOTE: For more detailed information about the state of the module, refer chapter LED Diagnostic, page 124.

Module Ethernet Ports

Ethernet Port Description

The BMECRA31310(H) adapter module has three 10/100 Base-T Ethernet ports.

The upper Ethernet port is the service port (ETH1). Below the dual RJ45 connector groups the ports for connecting the module to LAN A and LAN B of the PRP network.

The nominal operating speed of the Ethernet ports is 10/100 Mbit/s with automatic speed recognition

Service Port (ETH1)

NOTE: Do not use the SERVICE port to connect DIO(s) or RIO-PRP device network, either directly or through a switch/hub. Doing so may affect system performance.

The SERVICE port can be used:

- To provide an access point that other devices or systems can use to monitor or communicate with the adapter module.
- To mirror the redundant device network ports for Ethernet diagnostics. The service port provides access to external tools and devices (Control Expert, ConneXium Network Manager, HMI, and so forth).

  NOTE: In redundant mode you cannot connect the service port of both BMECRA31310(H) to the same device. Refer to *Incompatible Distributed Equipment Connections*, page 34.

The SERVICE port supports these modes:

- Access port (default): This mode supports Ethernet communications.
- Port mirroring: In this mode, data traffic from one of the other 2 ports is copied to this port. This allows a connected management tool to monitor and analyze the port traffic.
- Disabled

NOTE: You can configure the SERVICE port either ONLINE or OFFLINE.

NOTE: In port mirroring mode, the SERVICE port acts like a read-only port, therefore you cannot access devices (ping, connection to Control Expert, and so forth) through the SERVICE port.

Refer to *Service Port Configuration*, page 90.

Redundant Device Network Ports

REDUNDANT DEVICE NETWORK — PRP Port A: This port (with red marking) is the upper connector of the dual RJ45 connector. It allows a connection to the LAN A of the PRP network.

REDUNDANT DEVICE NETWORK — PRP Port B: This port (with blue marking) is the lower connector of the dual RJ45 connector. It allows a connection to the LAN B of the PRP network.

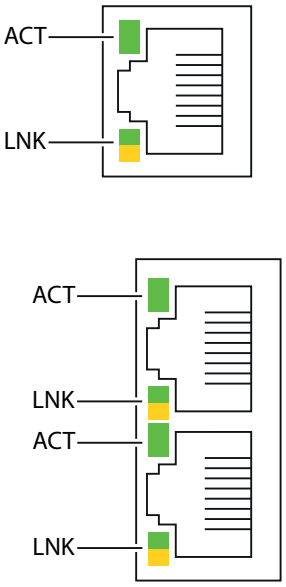
NOTE: Verify that the network cabling connections respect the separation of LAN A and LAN B such that LAN A is connected to PRP Port A and LAN B is connected to PRP Port B. Otherwise, crossed connections can result in an overload of the network, resulting in an error reaction from the M580 system.

NOTE: The number of drops in the Ethernet remote device network is limited and dependent to the M580 controller used in your architecture.

For more information, refer to *Modicon M580, Hardware, Reference Manual*.

Ethernet Port LED

Two LEDs are associated with each RJ-45 connector:



These LEDs report the activity and connectivity of the associated Ethernet port:

Name	Color	Status	Description
ACT	–	Off	No detected link
	Green	On	Inactive Ethernet link
	Green	Flashing	Active Ethernet link (transmit or receive)
LNK	–	Off	No detected link
	Green	On	Ethernet link detected with a speed equal to the module maximum capacity (100 Mbit/s).
	Yellow	On	Ethernet link detected with a speed less than the module maximum capacity (10 Mbit/s).

Standards and Certifications

Download

Click the link that corresponds to your preferred language to download standards and certifications (PDF format) that apply to the modules in this product line:

Title	Languages
Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	• English: EIO0000002726 • French: EIO0000002727 • German: EIO0000002728 • Italian: EIO0000002730 • Spanish: EIO0000002729 • Chinese: EIO0000002731

Module Installation and Cabling

What's in This Chapter

This chapter describes the hardware installation of the communication adapter PRP module BMECRA31310(H), the cable connection and how to set the location of the drop in the RIO device network.

Module Installation

Backplane Compatibility

X80 RIO drops can have one or two racks (main and extended) and the adapter modules are always located on the main RIO rack:

- In single mode, you can mount the adapter module on a Modicon X80 rack BMEXBP•••• (X Bus and Ethernet backplane or, if the Ethernet backplane is not required in your X80 RIO drop configuration you can mount the adapter module on a Modicon X80 rack BMXXBP•••• PV0.2 or subsequent supporting version(s) (X Bus backplane).
- In redundant mode, you can mount both adapter modules only on a Modicon X80 rack BMEXBP•••• (X Bus and Ethernet backplane). The Ethernet backplane of the main rack is mandatory for redundancy feature of the adapters.

The Modicon X80 rack reference you can use for the extended rack is BMXXBP•••• PV0.2 or subsequent supporting version(s) (X Bus backplane). You can also use a Modicon X80 rack BMEXBP•••• (X Bus and Ethernet backplane) but in this case the Ethernet backplane of the rack is not operational.

For more information on backplane, refer to *Modicon X80 Racks and Power Supplies, Hardware, Reference Manual*.

Position on the Rack

In single mode the adapter module is installed in slot 0 (marked 00) of the main rack.

In redundant mode the adapter modules are installed respectively in slot 0 and slot 1 (marked 00, 01) of the main rack.

NOTE: If you install an adapter module in other slots on the rack, the module is not operating.

Grounding Considerations

The adapter module is equipped with ground connection contacts at the rear for grounding purposes. These contacts connect the grounding bus of the module to the grounding bus of the rack.

To ground the rack, refer to the chapter *Grounding the Rack and Power Supply Module* (see Modicon X80, Racks and Power Supplies, Hardware Reference Manual).

Installation Procedure

⚠⚠DANGER

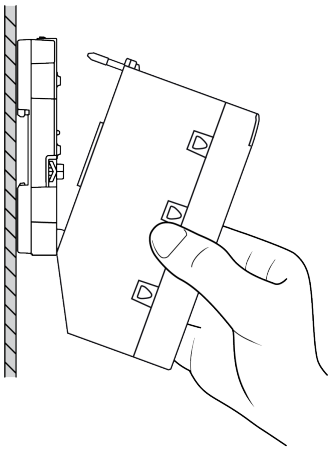
HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Disconnect all power from all equipment, including connected devices, prior to removing any covers or doors or installing or removing any accessories, hardware, cables, or wires except under the specific conditions specified in the appropriate hardware guide for this equipment.
- Always use a properly rated voltage-sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to the equipment.
- Use only the specified voltage when operating the equipment and any associated products.

Failure to follow these instructions will result in death or serious injury.

To mount the module on the backplane, follow these steps:

Step	Action
1	Remove the protective cover from the connector of the module slot on the Modicon X80 rack.
2	Position the locating pins situated at the rear of the module (on the bottom part) in the corresponding slot in the rack.
3	Swivel the module towards the top of the rack so that the module sits flush with the back of the rack.
4	Tighten the mounting screw on top of the module to hold in place on the rack. Tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).



An incorrect module connection can lead to an unintended operation of the system.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

Verify that the mounting screw is securely tightened to ensure the module is firmly attached to the rack.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

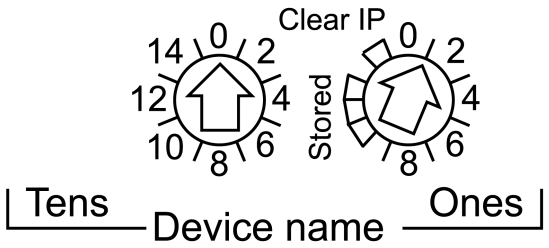
Setting the Location of the Ethernet Remote I/O Drop

Setting Rotary Switches

The rotary switches located on the front of the module are used to set the location of the drop on the RIO network. They can be set with a small, 5 mm flat-tipped screwdriver. No software is required to configure or enable the rotary switches.

The 3 digits valid values are: 000...159.

The following figure shows the positions of the rotary switches for a 3 digits value 001:



NOTE: Stored and Clear IP positions (Ones switch) are inoperative for the adapter modules.

The 3 digits value set on the rotary switches (*xxx*) is combined with the device prefix and its location on the rack to create the module identifier PCRA_*xxx*_0 or PCRA_*xxx*_1 for a physical module located respectively on the slot 0 or on the slot 1 of the rack.

The identifier in the physical module must be unique and must match with the identifier of the respective module configured in the application.

As the identifier of the physical module is used to communicate with DHCP server and FDR server, set the rotary switches before:

- Applying power to the module.
- Downloading the application.
- Installing the module on a powered drop (hot-swap).

Any modification are applied during a power cycle.

If you change the rotary switch settings after the module has powered up, the LED MS (Module Status) is red flashing and a mismatch message is logged in the module diagnostic.

If you want to return to the original setting of a modified rotary switch (and provided the other switch was not changed), turn the switch until the LED MS (Module Status) goes from red flashing to green on.

Redundant System Settings

In a redundant system, the values of the rotary switches must be set identically for both adapter modules in slot 0 and in slot 1 of the rack to allow the redundancy. Otherwise, they remain in INIT state and have no IP address (DHCP not enabled).

NOTE: A redundant drop can be activated with only one redundant adapter module installed in the slot 0 or slot 1. However, in this case the redundant drop operates in single mode.

The adapter modules can continue their normal operation and start-up if a redundant drop is energized with both adapter modules already inserted:

- and the values of the rotary switches are set identically for both adapter modules
- and the rotary switches values are the same as one in the application

- and there is no other redundant drop that has already been powered up with the same values

If a redundant drop is already powered up with an adapter module already inserted and in the CONNECTED/CONFIGURED state, and a second adapter module is inserted with different rotary switch values to the one already running, the second adapter module will not start and the existing one will not be affected and will remain in its state.

In all cases, the error is reported in the Control Expert and through the adapter module led panel with the specific status.

Duplicate IP Address Verification

Introduction

Each adapter module has a single IP address for its Ethernet ports. Therefore, the address conflict detection algorithm (duplicate IP verification) is performed based on the status (link up, link down) of the ports.

NOTE: Verify the status of the LED and especially the NS (Network Status) LED to detect a duplicate IP address.

Link Down

These conditions apply when links are inoperative:

Link Status	Description
A transition has occurred from one connected link to the other links down.	When no module ports are connected to a cable (the links are down), the services are reset. For example, I/O connections, Modbus connections, and explicit EtherNet/IP connections close, but low-level network services like switches are not affected.
There is one link down and at least one connected link.	There is no impact on services that are running in the module.

Link Up

These conditions apply when links are added:

Link Status	Description
A transition has occurred from no connected links to one connected link.	A duplicate IP verification is performed: • *no duplicate*: All services start. • *duplicate*: I/O services stop. The adapter module gets new configuration and downloads the IP configuration again. The system goes to default IP and the I/O modules are set to the fallback mode.
A transition has occurred from at least one connected link to an additional connected link.	A duplicate IP verification is performed: • *no duplicate*: The services continue. • *duplicate*: The services stop.

Cable Installation

Follow all local and national safety codes and standards.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK

If you cannot prove that the end of a shielded cable is connected to the local ground, the cable must be considered as dangerous and personal protective equipment (PPE) must be worn.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

EXPLOSION HAZARD

Do not connect or disconnect the equipment unless power has been switched off and/or the area is known to be non-hazardous.

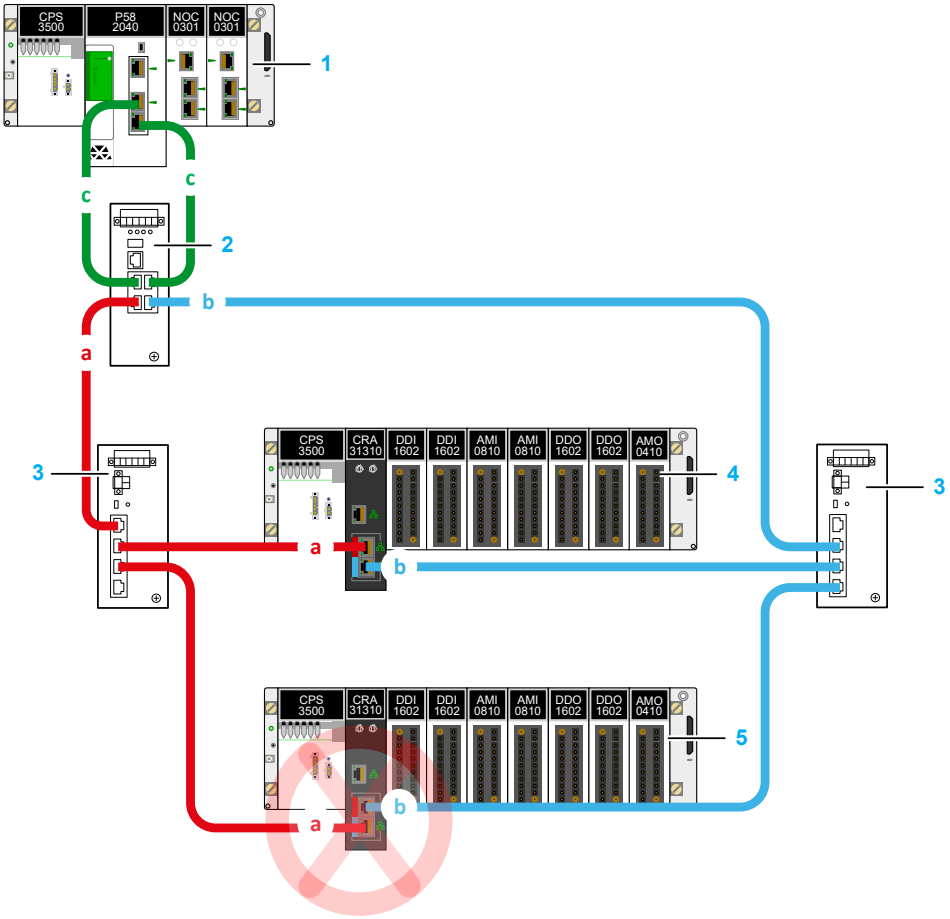
Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: Refer to the ground protection information provided in the documentations: *Electrical installation guide* and *Control Panel Technical Guide, How to protect a machine from malfunctions due to electromagnetic disturbance*.

Connection Principles

The color used for the PRP network follows the standard. The redundant device network ports of the adapter module are LAN-dependent.

Respectively connect the cable belonging to the LAN A to the device network port A (red marking) and the cable belonging to the LAN B to the device network port B (blue marking) of the adapter module.



1 Modicon M580 local rack
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with BMECRA31310(H) adapter module correctly connected to the PRP network
5 X80 RIO drop with BMECRA31310(H) adapter module incorrectly connected to the PRP network

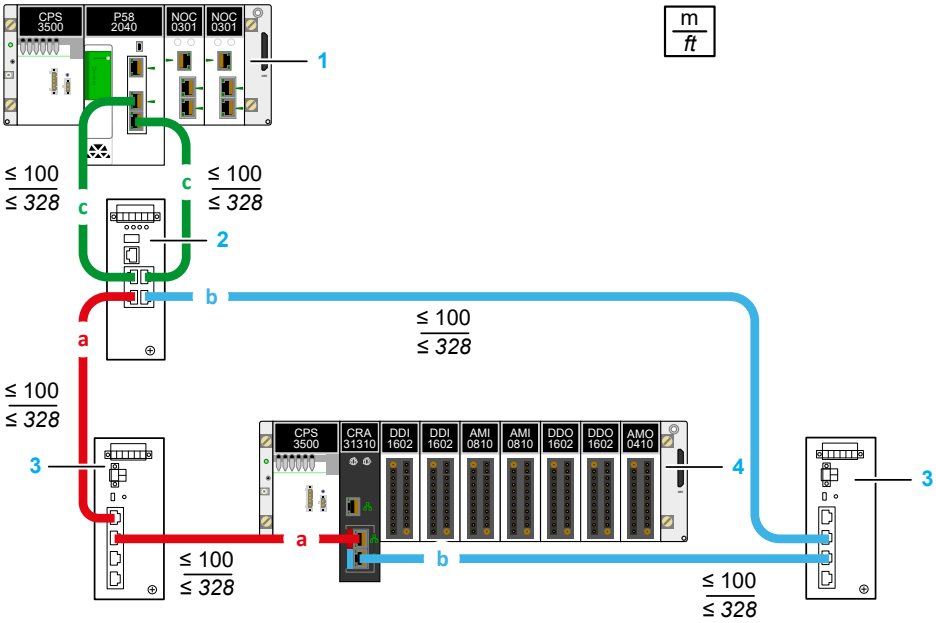
Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

> **NOTE:** To detect the crossed cable between PRP LAN A and LAN B monitor the error counter parameters *PRP_WRONG_LAN_A* and *PRP_WRONG_LAN_B* in the DDDT, page 133.

Copper Cables

Use CAT5e or CAT6 copper shielded twisted four-pair cables to connect adapter modules to Ethernet switches in a PRP network. Use 490NTC000•• ConneXium cables.

A copper cable connection cannot exceed 100 m between nodes in the device network:



1 Standalone M580 Controller
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with one BMECRA31310(H) adapter module

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green

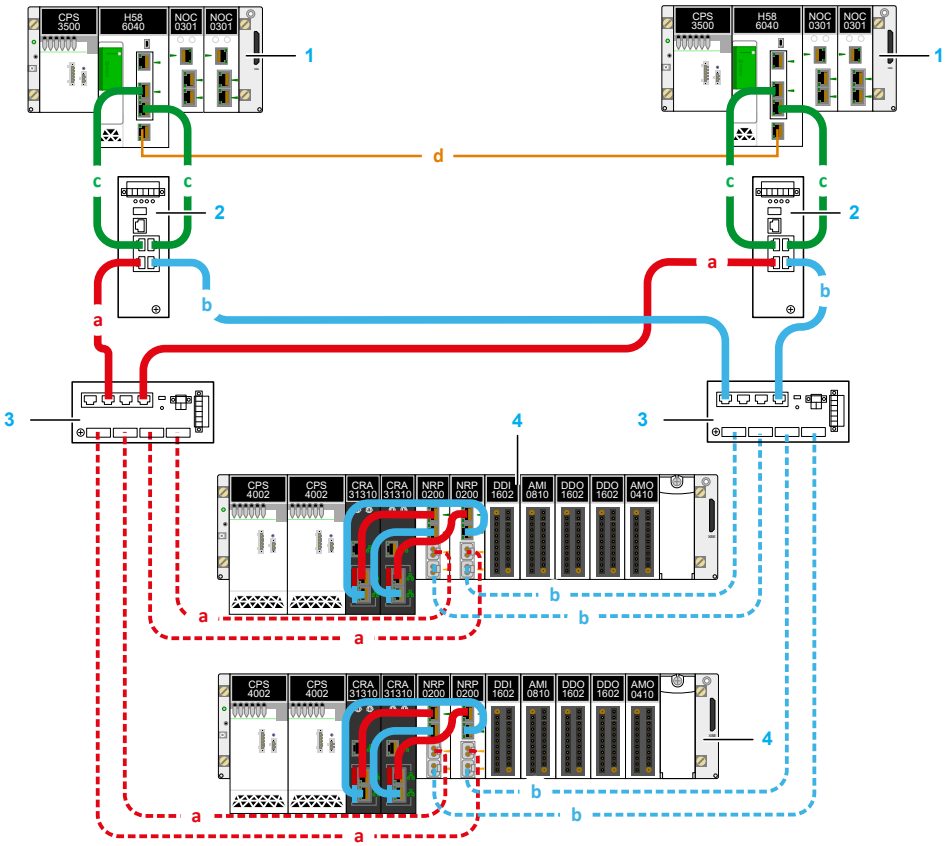
Using Fiber Optic

Fiber optic cable is an alternative to the copper cable allowing you to extend the distance between two network components.

Fiber Optic Converter Modules

Use fiber optic converter BMXNRP020• modules and Ethernet switches with copper and fiber optic connectors to extend the distance between the main local rack and the RIO drops beyond 100 m:

- In multimode the distance is up to 2 km between the BMXNRP0200 converter module and the Ethernet switch is connected to.
- In single mode, the distance is up to 15 km between the BMXNRP0201 converter module and the Ethernet switch is connected to.



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch with copper and fiber optic connectors
4 X80 RIO drop with BMECRA31310(H) adapter modules connected to BMXNRP020• fiber converter modules

Network legend (dotted lines represent fiber optic cables and solid lines represent copper cables):
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

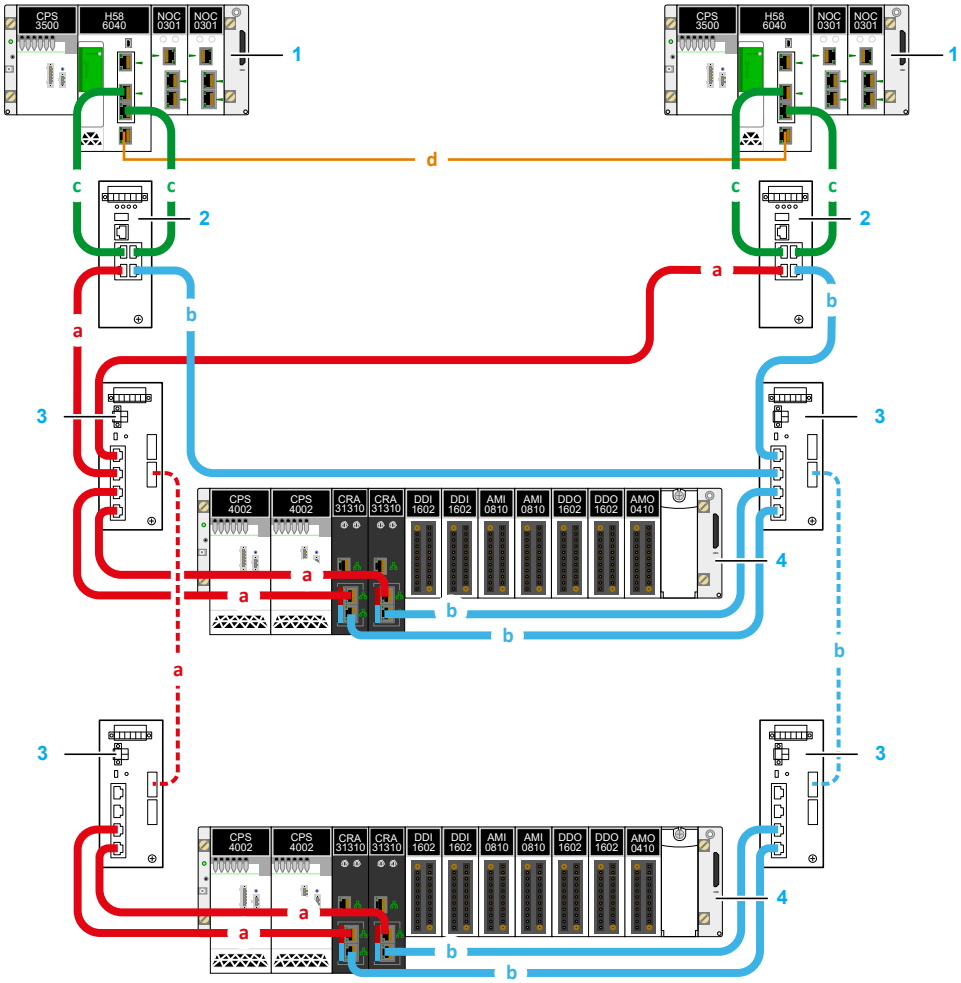
Refer to *Modicon X80, BMXNRP0200/0201 Fiber Converter Modules, User Guide* for additional information.

With Ethernet Switches

Use Ethernet switches with copper and fiber optic connectors to extend the distance between RIO drops beyond 100 m.

Depending on the Ethernet switch model:

- In multimode the distance is up to 4-5 km between two Ethernet switches
- In single mode the distance is up to 30 km between two Ethernet switches



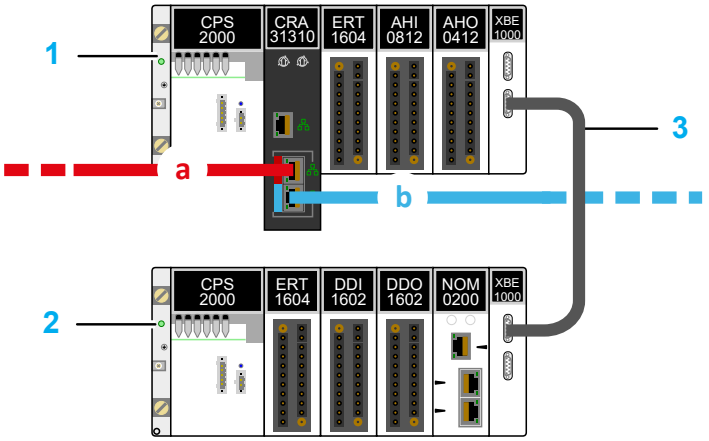
1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch with copper and fiber optic connectors
4 X80 RIO drop with BMECRA31310(H) adapter modules

Network legend (dotted lines represent for fiber optic cables and solid line represent copper cables):
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

Device Compatibility and X80 Drop Limitations

Overview

The following figure represents a multi-rack X80 RIO drop managed with one BMECRA31310(H) adapter module:



1 Main remote rack
2 Extended remote rack
3 Extension cable between both BMXXBE1000 modules

Network legend:
a PRP LAN A – red
b PRP LAN B – blue

NOTE: The modules that require Ethernet across the backplane can be installed in the main remote rack with a model reference BMEXBP••••. They cannot be installed in the extended remote rack.

Analog Modules

The following analog modules can be installed on an X80 RIO drop managed by BMECRA31310(H) adapter module(s):

Module	Type of Module	Installation on...	
		Main Remote Rack	Extended Remote Rack
BMX AMI ••••	X80 Analog Input Modules	+	+
BMX AM0 ••••	X80 Analog Output Modules	+	+
BMX AMM ••••	X80 Analog Input/Output Modules	+	+
BMX ART ••••	X80 Analog Isolated Input Modules	+	+
BME AHI 0812(1)(2)	X80 Analog Isolated HART Input Module	+	-
BME AH0 0412(1)	X80 Analog Isolated HART Output Modules	+	-

(1) These modules require a BMEXBP•••• (X-Bus and Ethernet backplane) Modicon X80 rack.

(2) In an M580 high-availability architecture, after a controller swap or switchover, the LED BS (bus status) of the BME AHI 0812 module may flash green up to 2 s. This is the time for the switches in the network to automatically re-configure with the new controller is acting as primary, however there is no interruption of I/O.

+ Allowed

- Not allowed

Discrete Modules

The following discrete modules can be installed on an X80 RIO drop managed by BMECRA31310(H) adapter module(s):

Module	Type of Module	Installation on...	
		Main Remote Rack	Extended Remote Rack
BMX DAI •••• BMX DDI ••••	X80 Discrete Input Modules	+	+
BMX DA0 •••• BMX DD0 ••••	X80 Discrete Output Modules	+	+
BMX DDM ••••	X80 Discrete Isolated Input/Output Modules	+	+
BMX DRA •••• BMX DRC ••••	X80 Discrete Relay Modules	+	+
BMX ERT 1604	X80 Discrete Time Stamp Module	+	+
+ Allowed			

Expert and Communication Modules

The following modules can be installed on an X80 RIO drop managed by BMECRA31310(H) adapter module(s):

Module	Type of Module	Installation on...	
		Main Remote Rack	Extended Remote Rack
BMX EAE 0300	X80 Synchronous Serial Interface Module	+	+
BMX EHC ••••	X80 Counting Modules	+	+
BMX ETM 0200H	X80 Turbomachinery Expert Input Frequency Module	+	+
PME PXM 0100(1)	Profibus DP/DPV1 Master Module	+	-
BMX NOM 0200	X80 Serial Link Module	+	+
BMX NRP 020•	X80 Fiber Converter Modules	+	+
BMECXM0100(H)2	X80 CANopen Master Module	+	+
(1) Installing the module in an X80 RIO drop is only compatible with standalone architecture. **(2)** Only for standalone architectures. **+** Allowed **-** Not allowed			

Third Party Module

The following third party module can be installed on an X80 RIO drop managed by BMECRA31310(H) adapter module(s):

Module	Type of Module	Installation on...	
		Main Remote Rack	Extended Remote Rack
PME GPS 0100	Partner Ethernet GPS Module	+	+
+ Allowed **-** Not allowed			

I/O Channel Limitation

The maximum number of channels in an X80 RIO drop managed by BMECRA31310(H) adapter module are:

- 1024 discrete channels
- 256 analog channels
- 36 application-specific (expert) channels among the following:
  - Counter modules (BMX EHC ••••)
  - Time stamping module (BMX ERT 1604)
  - SSI encoder module (BMX EAE 0300)
  - Serial link module (BMX NOM 0200)
  - Frequency Input (BMX ETM 0200H)

I/O Memory Limitation

The RIO drop memory size is limited to 1,400 input bytes and 1,400 output bytes per application program task.

Module Configuration

What's in This Part

Control Expert is used to configure your module and provides two access levels:

- **Control Expert**: It includes the Topology Manager that manage a system project. One or several controllers (with their own control project) can constitute a system project. Control projects for each controllers are managed by starting Control Expert Editor instances.
- **Control Expert Classic**: It manages one control project at a time.

Depending on wether you are working on a system project or a control project, the way to configure the Modicon X80 redundant adapter module may differ.

Control Expert System (Topology Manager)

What's in This Chapter

Overview

The instructions given in this chapter, for configuring the BMECRA31310(H) adapter module in Control Expert System (Topology Manager), assume that you have already added the module in your system. Refer to *EcoStruxure™ Control Expert, Topology Manager, User Manual* for more details on Topology Manager.

NOTE: When configuring a BMECRA31310(H) adapter module in a system project, certain parameters are set in the Topology Manager when the others are set in the Control Expert Editor.

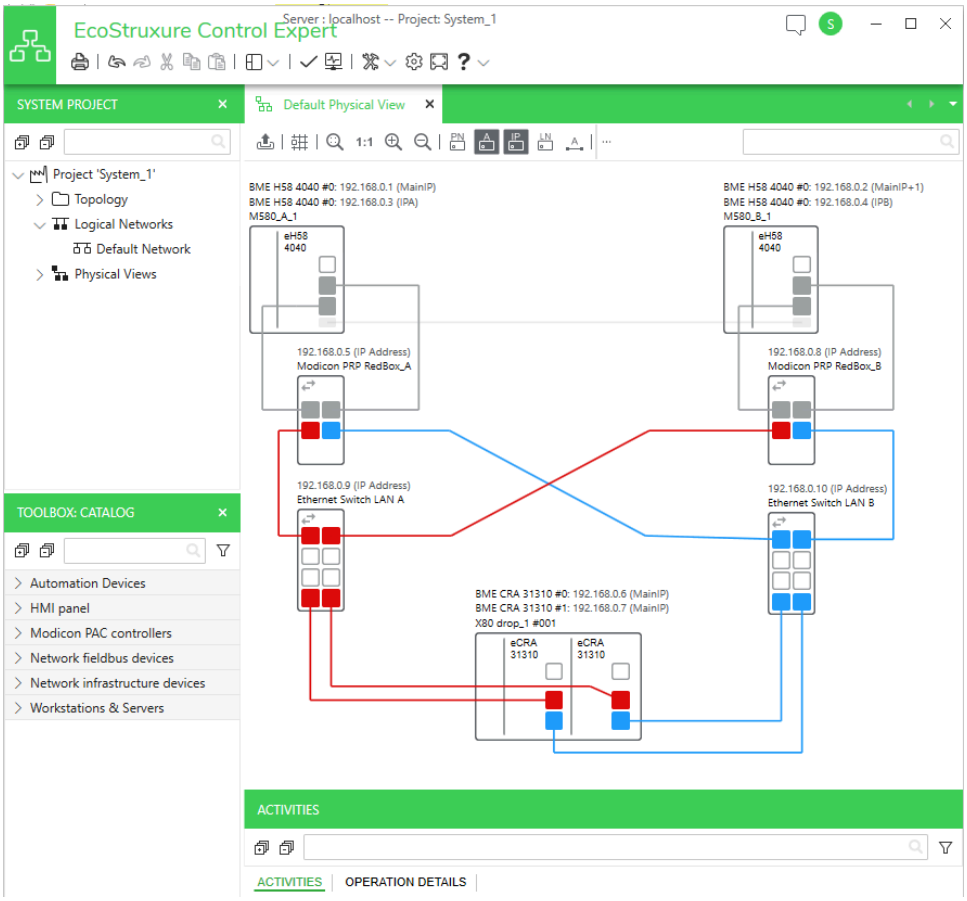
The table indicates in which tool you need to configure the BMECRA31310(H) adapter module parameters:

Configuration	**Topology Manager**	**Control Expert Editor(2)**
Instance name of the Implicit Device DDT	—	**Device DDT**/ **Redundant Device DDT** tabs
IP address	**PROPERTIES** Pane - **CONFIGURATION** tab(1)	—
PRP parameters	Not configurable	Not configurable
Identifier for DHCP	**PROPERTIES** Pane - **SERVICE** tab	—
SNMP service	**PROPERTIES** Pane - **SERVICE** tab	—
Service Port	**PROPERTIES** Pane - **CONFIGURATION** tab (ETH1)	—
Hold up time	—	**Parameters** tab
Connection parameter (RPI)	—	**Parameters** tab
Time Stamping buffer	—	**TimeStamping** tab

(1) IP address can also be assigned in the **LOGICAL NETWORK VIEW**

(2) Control Expert Editor is the name given to Control Expert Classic that opens inside the Topology Manager when you edit the control project of a Modicon controller.

Topology Manager



In a physical view or the SYSTEM PROJECT pane, right-click the adapter module and select **Open with > Properties Inspector**.

General Category - CONFIGURATION Tab

Attribute	Default value	Description
Name	–	Name of the object in the system project. It is not editable. The format is BME CRA 31310 #<*position*>. In single mode the **Name** of the device is BME CRA 31310 #0. In redundant mode the **Name** of the devices are respectively BME CRA 31310 #0 and BME CRA 31310 #1 for the device located in slot 0 and slot 1 of the X80 RIO drop.
Part Number	–	Part number of the device.
Version	–	Version of the device.
Comment	Blank	Optional. You can enter a comment by using free-form text.
Path	–	Read-only. Path to the object in the **System Project Explorer** pane. It is a concatenation of the following names: • X80 drop name • X80 rack name • X80 adapter name Example: `X80 drop_1 #008\BME XBP 0602 #0\BME CRA 31310 #1` This path corresponds to the adapter module located in the slot 1 (#1) of a BMEXBP0602 main rack (#0) of the X80 RIO drop which number in the application is 8 (#008).
Under Construction	False (cleared)	The value is read-only and inherited from the parent object.
Configuration File	Blank	Optional. Lets you save a copy of a file to the repository of Control Expert. The file can be, for example, a configuration project that is managed by an external program. Click **Attach** to select a file on the local computer or a network location. Files with extension .exe or .bat cannot be selected. Each file is saved with a unique, randomly created name. Once attached, the file can be managed from the context menu of the device by one user at a time.
Last Attached By **Last Attached On**	Blank	Date/time when the file specified under **Configuration File** was attached last and username of the user who performed the action. The attributes are also updated when you have opened a file by using the **Configuration File > Open** command and your changes have been saved to the repository.
Web Page Link	Blank	Optional. Enter a URL that uses the HTTP or HTTPS protocol to open the corresponding webpage. (The URL needs to start with *http://* or *https://*.)

Interfaces Category - CONFIGURATION Tab

Attribute	Description
Ethernet Protocol	The communication protocol that is used by the interface is **EtherNet/IP**.

The IP address can be configured manually or automatically by assigning the device to a logical network or by using the **LOGICAL NETWORK VIEW**.

Attribute	Description
MainIP	**MainIP** is the IP address of the device.

For the IP address of the device, the following attributes are available.

Attribute	Description
Logical Network	Logical network that the interface of the object belongs to. You can assign an interface to an existing logical network or to a new one by using the list. This sets the IP address to the next available address on this logical network. The list contains the following entries: • **NOCONF**: Not configured. Sets the IP address, **Subnet Mask**, and **Gateway Address** to *0.0.0.0*. The interface of the object is not assigned to a logical network. • Existing logical networks: Assigns the interface to the logical network that you select. • **New**: Create a new logical network by entering its name and configuring its properties. The interface of the object is assigned to the newly created logical network.
Subnet Mask **Gateway Address**	The attribute is read-only and configured based on the configuration of the logical network that the interface of the module is assigned to (**Logical Network** attribute). The value is preconfigured or inherited from the controller module (the adapter module and controller are on the same sub network) and is read-only.
MAC Address	Lets you enter the identification number of the physical device for services that require identification by MAC address. Format: *MM-MM-MM-SS-SS-SS* where *MM* (vendor identification) and *SS* (device-specific identification) are hexadecimal numbers.
Associated Physical Ports	Lists the ports of the device to which the interface settings (such as Ethernet protocol, IP address, logical network) apply.

Physical Ports Category - CONFIGURATION Tab

BKP Backplane Port Section:

Attribute	Description
Port Type	The type of network supported by the backplane port is **DIO**.

ETH1 Service Port Section:

Attribute	Description
Enabled	Clearing the checkbox disables the port and its services. If possible, disable a port when it is not used. **NOTE:** When the attribute is not present, the port is enabled and cannot be disabled.
Service Port Mode	Possible values: • **Access Mode** • **Mirroring Mode**: Enables **Mirrored Ports**.
Port Type	The type of network supported by the service port is **DIO**.
Mirrored Ports	The ports that are mirrored are shown in the text field when the list is collapsed. You can select a combination of ports from the following: • **Internal**: Embedded interface • **BKP**: Backplane port • **ETH2**: Device network port A — LAN A • **ETH3**: Device network port B — LAN B To be selected, a port must be enabled.

NOTE: In redundant mode, the configuration of the service port of one of the BMECRA31310(H) adapter modules automatically applies to the second one.

ETH2 and **ETH3** Device Network Port Sections:

Attribute	Description
Port Type	The type of network supported by the service port is **RIO**.

SNMP Category - SERVICES Tab

SNMP service:

Attribute	Description
Enabled	When selected, enables SNMP for the module and lets you configure attributes of the **SNMP** category. Your configuration is retained when you select/clear the checkbox. **NOTE:** The checkbox is selected and read-only when **Version** is set to **V1**. Disabling the SNMP service is possible when **Version** is set to **V3**.
Version	Version of SNMP that is used for communication. The adapter module supports: • **V1**. • **V3**. **NOTE:** The SNMPv3 service is configured in unsecured mode (no authentication and no privacy). Your configuration is retained when you switch SNMP versions.

IP Address Managers:

Attribute	Description
IP Address Manager 1	IP addresses of the first and second SNMP managers to which the agent that runs in the device sends trap notifications. The IP addresses must be different.
IP Address Manager 2	

Authentication:

This subcategory is available only for SNMPv3.

Attribute	Description
User Name	Required. To be valid, the user name must satisfy the following rules: • 32 characters maximum. • Contains only any combination of ASCII characters from 33 to 122. • Spaces are not allowed.

Agent:

Attribute	Description
Enable SNMP Manager	When selected (true), the **Location (SysLocation)** and **Contact (SysContact)** attributes are hidden and managed by the SNMP manager.
Location (SysLocation)	Enter the physical location of the device by using characters of the US-ASCII table (32 characters maximum).
Contact (SysContact)	Enter the contact information of the person in charge of device maintenance by using characters of the US-ASCII table (32 characters maximum).

Community Names:

This subcategory is available only for SNMPv1.

Attribute	Default value	Description
Set	*private*	Password that the agent requires before it executes write commands received from the SNMP manager.
Get	*public*	Password that the agent requires before it executes read commands received from the SNMP manager.
Trap	*alert*	Password that the SNMP manager requires before it accepts trap notifications from an agent.

Security:

This subcategory is available only for SNMPv1.

Attribute	Description
Enable “Authentication Failure” Trap	When selected (true), the agent sends a trap notification to the SNMP manager in case it receives a *Get* or *Set* request from a device that it cannot authenticate.

DHCP Client Category - SERVICES Tab

Configuration Sub-category:

Attribute	Description
Enabled	The checkbox is selected by default and read-only. The adapter module subscribes to the DHCP service of the controller (DHCP server).
DHCP Server Name	The attribute value is predefined and read-only for the adapter module. The DHCP server service is provided by the controller.
Protocol	The adapter supports the **DHCP** protocol.
Identified by	The DHCP server identifies the adapter module by its device name (identifier).
Identifier	At module insertion in your project, a default **Identifier** is assigned depending to the slot position and the drop number. The identifier is in the format *PCRA_[Drop Number]_[Slot]* where: • the PCRA is the prefix of the BMECRA31310(H) adapter module and cannot be changed. • *[Drop Number]* is a 3 digits number of the drop in the configuration. • [Slot_number] is 0 or 1 depending in the position of the adapter module on the drop. The software accepts only values that comply with module-specific format requirements. Each adapter needs to be assigned a unique Identifier within the application. **NOTE:** The rotary switch numerical values of the physical module must match with the 3 digits representing the drop number in the module **Identifier**. Refer to chapter Setting the Location of the Ethernet I/O Drop, page 64.

Control Expert Editor

In a physical view or the **SYSTEM PROJECT** pane, right-click the adapter module and select **Edit Control Project**.

Refer to the chapter Control Expert Project (Classic), page 85 for details on configuration parameters in Control Expert Editor.

Control Expert Project (Classic)

What's in This Chapter

Overview

NOTE: The device configuration procedure is valid when configuring a project with Control Expert Classic. When you configure your device from a system project, some commands are disabled in the Control Expert editor. In this case, you need to configure these parameters at the system level by using the Topology Manager.

Some parameters, fields are enabled or disabled according to the mode you configure for the adapter modules (single or redundant).

Configuration	**Control Expert Tab**
Instance name of the Implicit Device DDT	**Device DDT**/ **Redundant Device DDT** tab
Rotary switches values for device name matching	**Parameters** tab
IP address	**Parameters** tab(1)
PRP parameters	Not configurable
Identifier for DHCP	**Parameters** tab(1)
SNMP service	**SNMP** tab
Service Port	**ServicePort** tab
Hold up time	**Parameters** tab
Connection parameter (RPI)	**Parameters** tab
Time Stamping buffer	**TimeStamping** tab
(1) You can edit IP address and Identifier (device name) directly in the **Ethernet Network Manager**.	

Device DDT / Device DDT Redundant Tabs

Introduction

Use the device Derived Data Type (DDT) for diagnosis.

Device DDT Instance

Each adapter module is associated with one implicit device DDT instance.

In redundant mode:

- the implicit device DDT in the **Device DDT** tab is linked to the adapter module located in the slot 0 of the RIO drop.
- the implicit device DDT in the **Device DDT Redundant** tab is linked to the adapter module located in the slot 1 of the RIO drop.

Each **Implicit device DDT** fields contains a name and a type.

The Device DDT instance name can be defined manually but, when adding a module, a default device DDT instance name (see EcoStruxure™ Control Expert, Program Languages and Structure, Reference Manual) is defined by Control Expert.

Parameter		Description
Implicit device DDT	Name	The default names are: • EIO2_d*x*_r0_s0_ECRA31310 for adapter module in single mode and adapter module in the slot 0 in redundant mode • EIO2_d*x*_r0_s1_ECRA31310 for adapter module in the slot 1 in redundant mode *x* represents the drop number.
	Type	T_M_CRA_EXT2_IN (read only)
Goto details		Click this link to access the implicit device DDT in the **Data Editor** window.

Refer to Device DDT Structure, page 133 for more details on diagnostic parameters in implicit exchanges.

SNMP Tab

About SNMP

An SNMP agent is a software component of the SNMP service that runs on the module and gives you access to diagnostic and management information for the module. You can use SNMP browsers, network management software, and other tools to access this data.

In addition, the SNMP agent can be configured with the IP addresses of 1 or 2 devices (typically PCs that run network management software) to be the targets of event-driven trap messages. Such messages inform the management device of events like cold starts and the inability of the software to authenticate a device.

The SNMP agent can connect to and communicate with 1 or 2 SNMP managers.

The X80 RIO drop redundant communication adapter PRP module supports SNMPv1 and SNMPv3.

NOTE: By default, SNMP is disabled.

SNMPv1 Parameters

The SNMPv1 service includes:

- Authentication verification by the module of a SNMP manager that sends SNMP requests
- Management of events or traps

Set the following parameters when SNMPv1 is selected:

Field	Parameter	Description	Value
IP Address managers	IP Address manager 1	The address of the first SNMP manager to which the SNMP agent sends notices of traps.	0.0.0.0 ...255.255.255.255
	IP Address manager 2	The address of the second SNMP manager to which the SNMP agent sends messages of traps.	
Agent	Location (SysLocation)	Device location	31 characters (maximum)
	Contact (SysContact)	Information about the person to contact for device maintenance	
	Enable SNMP manager	*cleared* (default): You can edit the **Location** and **Contact** parameters. *selected*: You cannot edit the **Location** and **Contact** parameters.	selected/cleared
Community names	Set	Password that the SNMP agent requires to read commands from an SNMP manager (default = **Public**)	15 characters (maximum)
	Get		
	Trap		
Security	Enable “Authentication failure” trap	*cleared* (default): not enabled. *selected* (enabled): The SNMP agent sends a trap message to the SNMP manager if an unauthorized manager sends a **Get** or **Set** command to the agent.	selected/cleared

SNMPv3 Parameters

The SNMPv3 service is configured in unsecured mode (no authentication and no privacy).

Set the following parameters when SNMPv3 is selected:

Field	Parameter	Description	Value
IP Address managers	IP Address manager 1	The address of the first SNMP manager to which the SNMP agent sends notices of traps.	0.0.0.0 ...255.255.255.255
	IP Address manager 2	The address of the second SNMP manager to which the SNMP agent sends messages of traps.	
Agent	Location (SysLocation)	Device location	31 characters (maximum)
	Contact (SysContact)	Information about the person to contact for device maintenance	
	Enable SNMP manager	*cleared* (default): You can edit the **Location** and **Contact** parameters. *selected*: You cannot edit the **Location** and **Contact** parameters.	selected/cleared
Username		Define the name of the SNMP agent.	32 characters (maximum)

Offline IP Address Verification

Offline tests are done to verify that the IP addresses of the managers do not include the following types of IP addresses:

- Multicast: 224.0.0.0 or higher
- Loop back: Any address that starts with 127
- Broadcast: 255.255.255.255

PRP Tab

About PRP

The Redundant Ethernet standard (IEC62439-3:2011/FDISA) defines several parameters for PRP Incoming and outgoing traffics on PRP network are duplicated on both LAN A and LAN B.

PRP Parameters

PRP default values are implemented in the adapter module.

This table displays the non editable settings:

Parameter	Value	Description
Supervision Frame Multicast Address	01-15-4E-00-01-00	Target MAC Address for multicast supervision frame
Life Check Interval	2 s	Period between transmission of supervision frames
PRP Mode	Duplicate Discard	Duplicate address is not supported in PRP mode.
Node Forget Time	60 s	Time after which a node entry is cleared.
Node Reboot Interval	500 ms	Duration after a reboot during which no PRP frames must be transmitted.

ServicePort Tab

Service Port Configuration

The adapter modules have a service port that can be configured for Ethernet communications or for port mirroring.

NOTE: In redundant mode, the configuration of the service port of one of the BMECRA31310(H) adapter module automatically applies to the second one.

Service Port Parameters

Set the following parameters to configure the service port of the adapter module:

Field	Parameter	Value	Comment
Service Port	**Enabled**	—	Enable port and edit port parameters.
	Disabled	—	Disable port parameters.
Service Port Mode	**Access** (default)	—	This mode supports Ethernet communications.
	Mirroring	—	In port mirroring mode, data traffic from one or more of the other ports is copied to this port. A connected tool can monitor and analyze port traffic. **NOTE:** In this mode, the service port acts like a read-only port. You cannot access devices (ping, connection to Control Expert, etc.) through the service port. **NOTE:** The data from the ports connected to the PRP does not contain any RCT or VLAN tag information.
Access Port Configuration	**Service Port Number**	ETH1	You cannot edit the value in the **Service Port Number** field.
Port Mirroring Configuration	**Source Port(s)**	**Internal Port**	Ethernet traffic through the internal port
		ETH2	Ethernet traffic through the PRP port A
		ETH3	Ethernet traffic through the PRP port B
		Backplane Port	Ethernet traffic through the backplane port

Online Behavior

The parameters configured for the service port are stored in the application, however you can reconfigure (change) the parameters in the connected mode. Values that you reconfigure in the connected mode are sent to the adapter module in explicit messages. If the adapter module does not respond to the explicit messages, a message appears.

NOTE: The changed values are not stored, so a mismatch can exist between the parameters that are being used and those that are in the stored application.

NOTE: The configuration of the service port can be read and modified online using the Service Port Control Object, page 197 CIP object.

Parameters Tab

Remote Drop Configuration

In the Control Expert **Parameters** tab, you can:

- verify address information for the adapter modules (name, IP address, and subnetwork mask).
- verify the rotary switch values to set in the physical module.
- specify the hold up time applying to the devices of the drop.
- specify I/O refresh rates.

Address information Parameters

The module address information are read-only in the **Parameters** tab.

NOTE: Identification (**Device Name** / **Identifier**) is used by the adapter module to get an IP address from DHCP server and configuration from FDR server.

Parameter	Comment

Device Name	Displays the device name of the adapter module located on slot 0 of the rack.
	
	At module insertion in Control Expert project configuration, a default device name PCRA_*xxx*_0 is assigned to the adapter module. The 3 digits *xxx* represent the drop number in the configuration. For example the device name of redundant adapter module in slot 0 of the drop number 1 is PCRA_001_0.
	
	In your project configuration, the adapter device name does not change if you move the drop on the EIO Bus configuration.
	
	To modify the device name you need to modify the **Identifier** in the **Ethernet Network Manager** by clicking the **Update IP/DHCP configuration** link. (For adapter modules, **Device Name** and **Identifier** are identical).
	
	Each adapter needs to be assigned a unique **Identifier** within the application. A message like this appears in the Control Expert **Output Window** when analysis detects a duplicate identifier:
	
	`Device Network Manager (errors found):`
	
	`— [PCRA_001_0] Identifier not unique`
	
	`— [PCRA_002_0] Identifier not unique`

Device Name **Redundant CRA**	In redundant mode, displays the device name of the redundant adapter module located on the slot 1 of the rack (PCRA_*xxx*_1). **NOTE:** The rules described above (unique **Identifier**, device name in Control Expert application) apply for the device name of the redundant adapter module.
Tens **Ones**	Displays the values to be set on the rotary switches of the physical module to match with the module identification in the application. **NOTE:** In redundant mode, set the same rotary switches values to both physical adapter modules of the drop. Refer to chapter Setting the Location of the Ethernet I/O Drop, page 64.
IP Address **IP Address Redundant CRA** **Sub Network**	Displays IP addresses of the adapter modules located respectively on the slot 0 and slot 1 (in redundant mode only) and the sub network. The IP address are used for communication on the Ethernet RIO network. When configuring the adapter module in Control Expert, a unique IP address is assigned to the module. Each adapter module has the same IP address on both LAN A and LAN B. Controller and RIO drops are on the same sub network. **NOTE:** To modify the assigned IP address of the adapter module click **Update IP/DHCP configuration** link to access the **Ethernet Network Manager**.

Parameter	Comment
Redundancy Status	The radio button is automatically set according to the RIO drop configuration. **Single mode** is set when one adapter module is configured on the slot 0 of the rack. **Redundant mode** is set when the redundant adapter module is configured on the slot 1 of the rack. Only possible with redundant M580 controllers.

Ethernet Network Manager

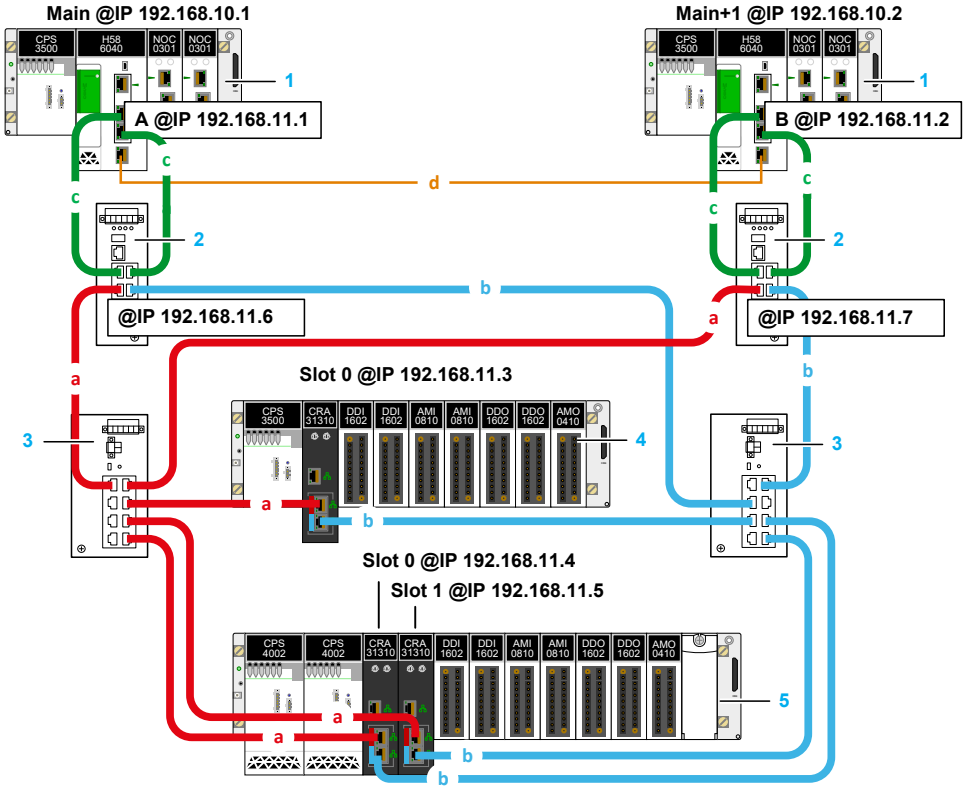
The **Ethernet Network Manager** tool provides a snapshot of IP address settings for devices included in network topologies that are part of your application.

If the tool detects a duplicate IP addressing, it displays a message like this in the Control Expert **Output window**:

```
Device Network Manager (errors found)
- [PCRA_001_0] IP Address not unique
- [PCRA_002_0] IP Address not unique
```

For more detailed information about the network configuration, refer to chapter *Using the Ethernet Network Manager* (see *Modicon M580, Hardware, Reference Manual*).

The following figure provides an example of IP addressing:



1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with one BMECRA31310(H) adapter module (single mode)
5 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode)

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

Hold up Time Parameter

There is one hold up time per RIO drop :

Parameter	Comment
Hold up time	The hold up time represents the time (ms) that device outputs are maintained in their states after a communication disruption and before taking their fallback values: • **default value**: 1000 ms • **valid value range**: 50...65,530 ms The hold up time value to configure is: • **6 * PAC scan time** for a periodic application, or • the **configured watchdog value** for a cyclic application.

If you assign a hold up time value that is less than the value in the table above, an I/O module may move to its fallback state. When communications are restored, the I/O module restarts and may not operate as anticipated.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

Do not configure a hold up time value that is less than the configured watchdog value for a cyclic application, or 6 * PAC scan time for a periodic application.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Connection parameter

The RPI values define the I/O refresh rates of the modules located on the RIO drop managed by the adapter module.

The following tables describes both connection parameters associated to each task:

Parameter	Comment
CRA->Scanner RPI	**Inputs:** The RPI is the input refresh rate at which the adapter module sends inputs to the controller with Ethernet I/O scanner service.
Scanner->CRA RPI	**Outputs:** Outputs are passed from the controller with Ethernet I/O scanner service to the adapter. You cannot edit this value. The outputs are published synchronously or immediately at the end of the task.

Only the **CRA->Scanner RPI** value for the MAST task can be set by selecting **Custom RPI**.

The other RPI values are set to default values which calculation is given in the table below according to the task mode:

Task	Mode	CRA->Scanner RPI	Scanner->CRA RPI
MAST	Periodic	default value = 0.5 * period	default value = 1.1 * period
	Cyclic	default value = 0.25 * watchdog	default value = 0.25 * watchdog
FAST AUX 0 AUX 1	Periodic	default value = 0.5 * period	default value = 1.1 * period

NOTE: For a periodic MAST task, the period value allows the complete execution of the logic. (The MAST can overrun when its execution time exceeds this value). Valid values: 1...255 ms (increment: 1 ms).

NOTE: For a cyclic MAST task, the outputs are sent upon the completion of the task. The watchdog value (10 ... 1500 ms, increment: 10 ms, default = 250 ms) must be greater than the execution time, otherwise the process times out.

For more detailed information on tasks, refer to chapter *Description of Tasks and Processes* (see *EcoStruxure™ Control Expert, Program Languages and Structure, Reference Manual*).

TimeStamping Tab

Module Performance

The BMECRA31310(H) redundant communication adapter module has the following time stamp features:

- The time accuracy is 15 ms.
- The maximum of discrete I/O channels (located on the RIO drop) time stamped is 256.
- The maximum size of the buffer is 4000 events.

Time stamping of the events starts as soon as the adapter module is configured.

NOTE: In redundant mode, only the adapter module assigned to the *MASTER* role time stamps the events.

Time Synchronization

As long as the M580 controller has NTP enabled as either a client or a server, the BMECRA31310(H) module is a client of the controller and uses NTPv4 for the clock synchronization.

NTPv4 includes a dynamic server discovery.

The number of available NTP servers depends on the configuration of the NTP service of the M580 controller:

- If the NTP service of the M580 controller is set to Server only, the BMECRA31310(H) module synchronizes its clock with the M580 controller.
- If the NTP service of the M580 controller is set to client/server, the BMECRA31310(H) module synchronizes its clock with the best NTP server, according to the NTPv4 RFC5905 standard, among the list of the NTP servers configured for the M580 controller and the M580 controller itself.

If the external NTP servers are unreachable, BMECRA31310(H) modules synchronize directly with the M580 controller. If you replace a BMECRA31310(H) module, it synchronizes with the clock of the M580 controller if no NTP server is available.

NOTE: To verify if the external NTP servers of BMECRA31310(H) modules are available, verify the SERVICE_STATUS2, NTP_SYNC value from the M580 controller: 1 = Synchronized, 0 = Otherwise. Refer to chapter *Standalone DDT Data Structure for M580 CPUs* (see *Modicon M580, Hardware, Reference Manual*).

For more detailed information about the NTP service of the M580 controller, refer to chapter *NTP Tab* (see *Modicon M580, Hardware, Reference Manual*).

Local Buffer Configuration

The **local buffer** refers to the buffer in the adapter module.

The **Time Stamping** settings are as follows:

Parameter	Value	Comment
On buffer full	**Stop the recording** (Default value)	Stop the recording when the events buffer is full.
	Overwrite buffer	The oldest events are overwritten when new events occur and the events buffer is full.
On power on	**Reset the local buffer**	The events buffer is cleared.
	Nothing (Default value)	New events are added to the existing events buffer if the application is the same. If the time stamping application is different, the buffer is cleared.
On STOP to RUN	**Reset the local buffer**	The events buffer is cleared.
	Nothing (Default value)	New events are added to the existing events buffer if the application is the same. If the time stamping application is different, the buffer is cleared.

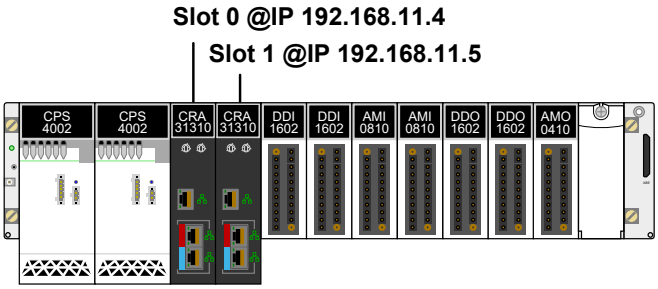
NOTE: When the adapter module is re-configured the local buffer is reset.

Applicative Time Stamping

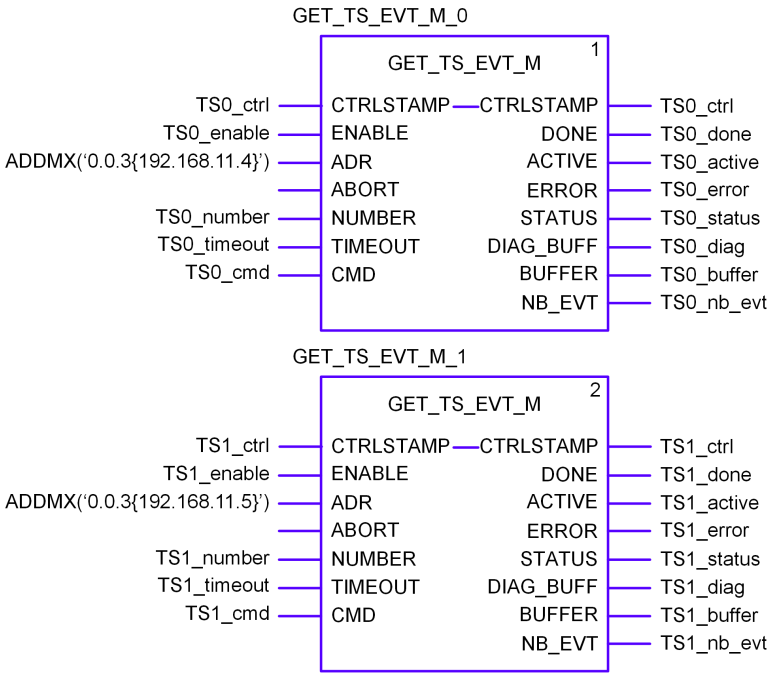
The applicative time stamping is supported in both single and redundant modes.

In redundant mode, only the adapter with the MASTER role time stamps the events. In case of switchover the adapter with MASTER role is assigned to the NOT MASTER role keeping the events logged in its buffer. The adapter which is now assigned to the MASTER role, starts event logging in its buffer.

NOTE: You have to program your application in order to read continuously both adapter module buffers and concatenate them in the application.



Use two `GET_TS_EVT_M` function blocks to get the time stamped data in both redundant BMECRA31310(H) adapter modules (`TS0_buffer` and `TS1_buffer`) as illustrated below in FBD programming language:



For more information, refer to chapter *GET_TS_EVT_M: Reading the M340 and M580 Time Stamped Event Buffer* (EcoStruxure™ Control Expert, System, Block Library).

NOTE: Using the implicit device DDT of the redundant adapter modules to activate one of the two `GET_TS_EVT_M` function blocks may result in the loss of events.

NOTICE
LOSS OF EVENTS Monitor the loss of events counter to determine the impact of this in your application. **Failure to follow these instructions can result in equipment damage.**

System Time Stamping

The system time stamping is supported in single mode only.

For more information, refer to *System Time Stamping, User Guide*. In this user guide, the information dedicated to the Modicon X80 Ethernet RIO drop in an M580 application are applicable to the X80 RIO drop managed by a BMECRA31310(H) adapter module.

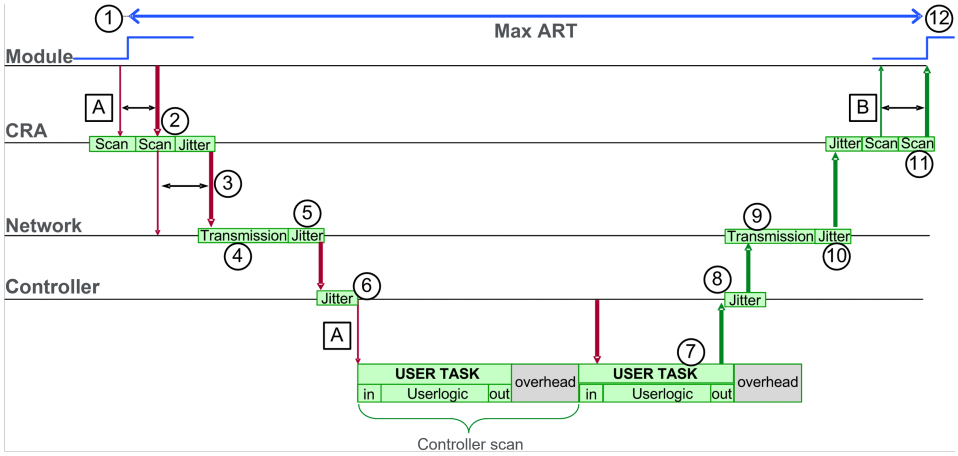
Application Response Time

What's in This Chapter

Application Response Time (ART)

Overview: ART Computation Parameters

The following diagram displays ART-related events and computation parameters. Refer to the *Design Principles of M580 Networks* appendix (see Modicon M580 Standalone, System Planning Guide for, Frequently Used Architectures) for details.



A: missed input scan	6: controller input jitter
B: missed output scan	7: operation of application logic (1 scan)
1: input turns ON	8: controller output jitter
2: CRA drop processing time	9: network delay
3: CRA input request packet interval (RPI) rate	10: network jitter
4: network delay	11: CRA drop processing time
5: network jitter	12: output applied

The ART computation parameters and their maximum values (in milliseconds) are described below:

ID	Parameter	Maximum value (ms)	Description
2	CRA drop processing time (CRA_Drop_Process)	4.4	The sum of CRA input scan time and queue delay
3	CRA input RPI (RPI)	–	Controller task. Default = 0.5 * Controller period, if MAST is in periodic mode. If MAST is in cyclic mode, the default value is watchdog/4).

<table>
<tr><th>ID</th><th>Parameter</th><th>Maximum value (ms)</th><th colspan="2">Description</th></tr>
<tr><td rowspan="8">4</td><td rowspan="8">network input time (Network_In_Time)</td><td rowspan="8">2.496 (0.078 * 32)
NOTE: The value 2.496 ms is based upon a packet size of 800 bytes and 32 hops[1].</td><td colspan="2">The product of (network delay based on I/O packet size) * (the number of hops[1] the packet travels). The network delay component can be estimated as follows:</td></tr>
<tr><td>I/O packet size (bytes):</td><td>Estimated network delay (µs):</td></tr>
<tr><td>128</td><td>26</td></tr>
<tr><td>256</td><td>35</td></tr>
<tr><td>400</td><td>46</td></tr>
<tr><td>800</td><td>78</td></tr>
<tr><td>1200</td><td>110</td></tr>
<tr><td>1400</td><td>127</td></tr>
<tr><td>5</td><td>network input jitter (Network_In_Jitter)</td><td>6.436 ((30 * 0.078) + (32 * 0.128))
NOTE: This value is based on a packet size of 800 bytes for RIO drops and 1500 bytes for DIO traffic.</td><td colspan="2">Formula: ((number of RIO drops) * (network delay)) + ((number of distributed equipment hops[1]) * network delay)</td></tr>
<tr><td>6</td><td>controller input jitter (Controller_In_Jitter)</td><td>5.41 (1 + (0.07 * 63))</td><td colspan="2">Controller input queue delay (due to RIO drops and DIO traffic)</td></tr>
<tr><td>7/8</td><td>controller input jitter scan time (controller input jitter_ Scan)</td><td>–</td><td colspan="2">User defined Control Expert scan time, which can be either fixed or cyclic.</td></tr>
<tr><td>9</td><td>controller output jitter (Controller_Out_Jitter)</td><td>2.17 (1 + (0.07 * 31))</td><td colspan="2">Controller output queue delay.</td></tr>
<tr><td>10</td><td>network output time[2] (Network_Out_Time)</td><td>2.496</td><td colspan="2">See calculation above for Network_In_Time.</td></tr>
<tr><td>11</td><td>network output jitter (Network_Out_Jitter)</td><td>4.096 (32 * 0.128)</td><td colspan="2">Calculated as Network_In_Jitter without I/O frames from RIO drops.</td></tr>
<tr><td>12</td><td>CRA drop process time (CRA_Drop_Process)</td><td>4.4</td><td colspan="2">The sum of CRA queue delay and output scan time.</td></tr>
<tr><td colspan="5">1. A hop is a switch that a packet passes through on the path from a source (transmitting) device to a destination (receiving) device. The total number of hops is the number of passthrough switches along the path.</td></tr>
</table>

Estimating ART

Using the parameters described in the preceding table, you can compute the maximum estimated ART based on the maximum number of RIO modules and distributed equipment for an application.

The maximum ART value is equal to the sum of values in the **Maximum value** column. Therefore, the ART calculation for a controller scan time (Controller_ Scan) of 50 ms and an RPI value of 25 ms is as follows:

4.4 + 25 + 2.496 + 6.436 + 5.41 + (2 * 50) + 2.17 + 2.496 + 4.096 + 4.4 = **156.904** ms ART

NOTE: If a cable break occurs or a cable is reconnected on the network, add an additional time period to the above ART calculation to allow for RSTP recovery. The additional time to be added equals: 50 ms + Controller_Scan/2.

Modicon X80 Drop Operation

What's in This Part

Modicon X80 Drop Operation

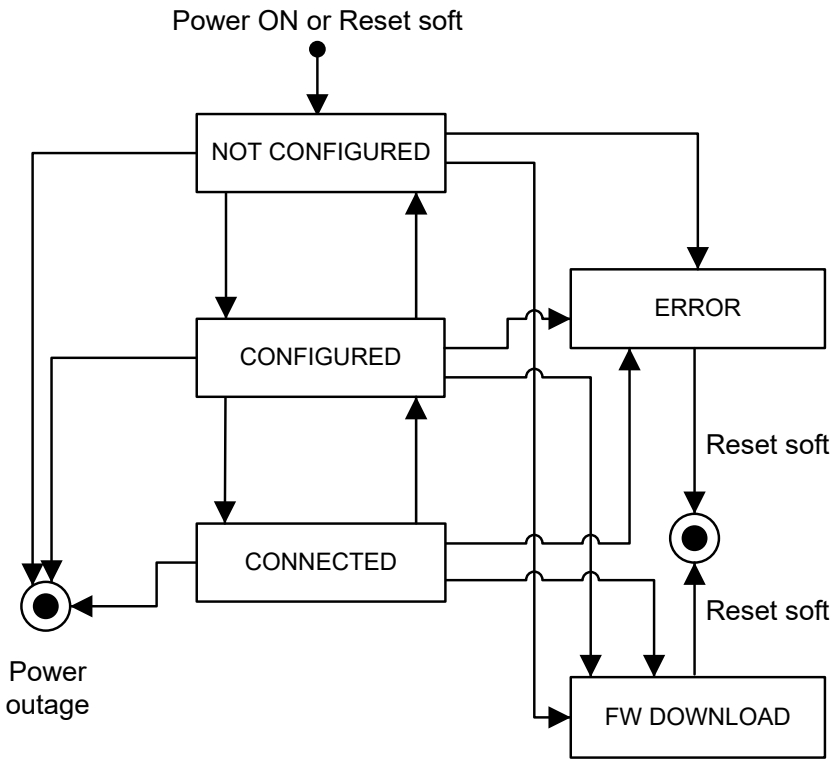
What's in This Chapter

This chapter gives the operating states of the adapter module and the redundancy operation modes. In addition the behavioral response to some case study scenarios in high-availability architectures is also presented.

Module Operating States

Diagram

The following diagram presents the module operating states:



Main Operating States Description

At power on (or following a soft reset), the adapter module performs an auto-test and reads the value of the rotary switches which determines the physical module identifier.

After a successful auto-test, it goes through the three main states: ***NOT CONFIGURED > CONFIGURED > CONNECTED***.

Module State	Description
NOT CONFIGURED	In this state the adapter module proceed to: • Get IP address (from DHCP) according to its identifier. **NOTE:** When the IP address is already used by another device, the adapter module stays in this state until you change the rotary switches values or you assign another IP address. A restart of the adapter module is required for both modifications. • Get configuration file (from FDR server). The adapter module configures itself and all the drop modules that are declared in configuration file. **NOTE:** During this configuration phase, the I/O modules on the drop go in fallback state.
CONFIGURED	In this state the adapter module and the modules on the drop are configured. While waiting an open EtherNet/IP connection with the controller (RIO scanner), the adapter module scan the input modules. After 5 s, if the expected connection is not opened, the adapter restarts its DHCP process. If the IP address has changed, the adapter module also checks its configuration file on the FDR server. During this state, the output modules of the drop enter in fallback configured mode or stay in fallback security mode according to their previous state: • If the output modules were in run state and hold up time is ended, they go in fallback configured mode. • If their previous state were fallback security they stay in this state. During this state, the input modules are scanned but are not published on the RIO network. **NOTE:** When configured, the time stamping of the inputs starts during this state.
CONNECTED	In this state, the adapter module manages the outputs and inputs modules according to the controller/task states received from the RIO scanner. • When a task enters in *STOP* state, or the controller enters in *HALT* state, the adapter module puts the output modules associated to the task in fallback configured or in fallback security state if the task has not been in *RUN* state. The inputs are still published. **NOTE:** The transition from *CONNECTED RUN* to *CONNECTED STOP* happens when all tasks associated with the adapter module enters in *STOP* state. • When a task enters in *RUN* state the adapter module applies the outputs values subscribed from the RIO scanner to the outputs modules, and inputs modules are published. **NOTE:** The transition from *CONNECTED STOP* to *CONNECTED RUN* happens as soon as one task associated with the adapter module enters in *RUN* state. **NOTE:** In redundant mode (there are two adapter modules per drop), the above behavior applies to the adapter module with the *MASTER* role. Refer to Adapter Redundancy Operation, page 106

When the local rack of the remote drop is de-energized, the I/O modules of the local and extended racks are in fallback mode. When the extended rack of the remote drop is powered off, the I/O modules of this extended rack are in fallback mode and the I/O modules of the local rack are not impacted.

Transitions

The following table presents the transitions between the three main states of the adapter module:

Transition	This transition occurs when ...
NOT CONFIGURED to *CONFIGURED*	The adapter module and all the modules of the RIO drop are configured.
CONFIGURED to *CONNECTED*	All of the following exist: • An EtherNet/IP connection is open between the adapter module and the RIO scanner. During the open connection, the timeout connection is configured with the value sent by the RIO scanner. • The handshake (that is exchange of signatures) is validated between RIO scanner and the adapter module verifying system consistency is validated. **NOTE:** It requires less than 10 seconds for the adapter module to enter in *CONNECTED* state.
CONNECTED to *CONFIGURED*	One of the following exist: • TCP/EIP timeout due to RIO scanner detected error, watchdog, or power interruption. • The physical link between RIO scanner and adapter module is not operational. • The RIO scanner closes the EIP connection. • The adapter module closes the EIP connection for firmware downloading.
CONFIGURED to *NOT CONFIGURED*	One of the following exist: • Invalid configuration signature detected during the CIP open connection. • New FDR file which is not compatible with the active one. • The adapter module has been deleted in the FDR server.

ERROR State Description

The adapter module enters in this state when an error is detected. Then the module restarts.

- In single mode (there is one adapter module per drop) to help prevent inconsistencies of the outputs set the same values to the configured fallback as the fallback security values.

  NOTE: Use an alarm relay to detect the adapter module entering in *ERROR* state.

- In redundant mode (there are two adapter modules per drop):
  - If the adapter module with the *MASTER* role enters in *ERROR* state, the adapter module with the *NOT MASTER* role switches to the *MASTER* role and manage the modules on the drop without inconsistencies of the outputs.
  - If the adapter module with the *NOT MASTER* role enters in *ERROR* state, the adapter module with the *MASTER* role carries on managing the modules on the drop without inconsistencies of the outputs.

FW DOWNLOAD State Description

In this state, the firmware update is in progress and EtherNet/IP connections with the controller are stopped. Only the firmware update tool can communicate with the adapter module.

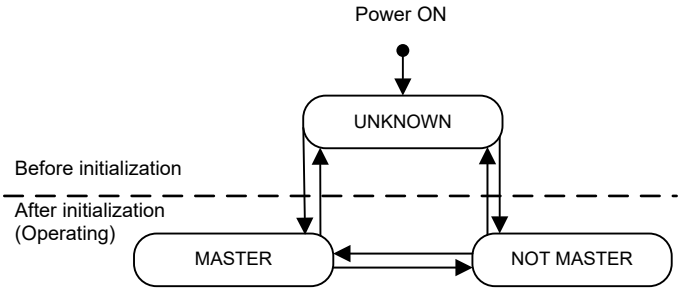
- In single mode (there is one adapter module per drop) input modules are no more read and output modules goes in fallback mode.

- In redundant mode (there are two adapter modules per drop):
  - If the firmware update is performed for the adapter module with the *MASTER* role, the adapter module with the *NOT MASTER* role switches to the *MASTER* role and manage the modules on the drop without bump on the outputs.
  - If the firmware update is performed for the adapter module with the *NOT MASTER* role, the adapter module with the *MASTER* role carries on managing the modules on the drop without inconsistencies of the outputs.

Module Redundancy States

Diagram

The following diagram presents the redundancy states for adapter module. They are managed in parallel of the operating states.



Redundancy States

State	Description
UNKNOWN	The adapter module enters in this state at boot up and in case of detected error.
MASTER	In this state the adapter module have the *MASTER* role in the drop. The adapter module writes the data to the output modules and provides the input data to the controller.
NOT MASTER	In this state the adapter module have the *NOT MASTER* role in the drop. The adapter module is ready to have the *MASTER* role in case of detected error of the adapter module which have the *MASTER* role.

Role Assignment

The role assignment is performed once the adapter role module state reaches the *CONNECTED* state. Otherwise the adapter module state stays in *UNKNOWN* until the detected error is cleared.

When the adapter module reaches the CONNECTED state:

- If two adapter modules are physically installed on the rack, the adapter module located in slot 0 is assigned to the *MASTER* role and the adapter module located in slot 1 is assigned to the *NOT MASTER* role.
- If only one adapter module is physically installed on the rack, it is assigned to the *MASTER* role whatever its position on the rack (slot 0 or slot 1).

Heartbeat Message

During normal operation the adapter modules with *MASTER* and *NOT MASTER* roles exchange heartbeat messages informing the peer adapter module about its state and activity.

The heartbeat message contains data about:

- Traffic quality on Ethernet ports A and B of the adapter module
- Firmware update
- Communication with the RIO scanner on the controller

The cycle time for the heartbeat messages is 5 ms allowing the system to detect a switchover causal event within 5 ms.

NOTE: The adapter module with *NOT MASTER* role does not consume data on the X bus apart from the heartbeat message. As a consequence you cannot rely on `IO_HEALTH_RACK0` and `IO_HEALTH_RACK1` parameters of the device DDT instance corresponding to the adapter module with the *NOT MASTER* role.

Switchover Conditions

A present and healthy adapter module with *NOT MASTER* role on the drop is a prerequisite for a switchover.

One of the following events cause a switchover:

- The adapter module with *MASTER* role has detected an unrecoverable hardware or system error.
- The adapter module with *MASTER* role is removed from the rack.
- The adapter module with *MASTER* role has no connection with the Primary controller whereas the adapter module with the *NOT MASTER* role maintains at least one connection with the Primary controller.
- The adapter module with *MASTER* role has successfully downloaded new firmware and is ready to start the firmware update.

Switchover Execution Time

The maximum time necessary for completing a switchover is around 20 ms in the case that the MASTER CRA is incapacitated. In the case of the loss of the network, there is a 0 ms recovery time.

Switchover Effects on RIO Drops

The switchover is transparent for the outputs modules on the drop.

Transitions – Use Cases

The following table presents the transitions when an event is detected:

Module state before the event				Event	Module state after the event	
Slot 0		Slot 1			Slot 0	Slot 1
Module on the rack	Initial State	Module on the rack	Initial State			
Yes	*MASTER*	No	—	Insert adapter module in slot 1	*MASTER*	*NOT MASTER*
No	—	Yes	*MASTER*	Insert adapter module in slot 0	*NOT MASTER*	*MASTER*
Yes	*MASTER* (Connected Run)	Yes	*NOT MASTER* (Connected Run)	Disconnect adapter module in slot 0	*NOT MASTER* (Connected Stop)	*MASTER* (Connected Run)
Yes	*NOT MASTER* (Connected Run)	Yes	*MASTER* (Connected Run)	Disconnect adapter module in slot 0	*NOT MASTER* (Connected Stop)	*MASTER* (Connected Run)

Similar to a switchover, a swap is a controlled event that transfers control of the drop from the adapter module with the *MASTER* role to the adapter module with the *NOT MASTER* role. A swap can be performed by the execution of the `RED_PRP_DROP_SWAP` command (device DDT of the controller) by either program logic, or in an animation table in forcing mode.

NOTE: Before you execute a swap, confirm that the adapter module with the *NOT MASTER* role is ready to assume the *MASTER* role, which allows the swap to occur. Verify that the *REDUNDANT* parameter in *CRA_DIAGNOSTIC* is in active mode. See T_M_CRA_EXT2_IN Structure, page 133.

Interruption of I/O Connection

Single Mode Condition

Communication can be interrupted between the controller and remote I/O modules of a drop managed by one BMECRA31310(H) adapter module under these conditions:

- Performing a hot swap by replacing the redundant adapter module with the same type.
- There is no RIO cable connection neither on LAN A nor LAN B on Redundant Device Network PRP ports.
- The I/O connection is closed while the controller is reconfigured.

Redundant Mode Condition

Communication can be interrupted between the controller and remote I/O modules of a drop managed by two BMECRA31310(H) adapter modules in redundant mode under these conditions:

- There is no RIO cable connection neither on LAN A nor LAN B on Redundant Device Network PRP ports of both adapter modules (MASTER and NOT MASTER).
- The I/O connection is closed while the controller is reconfigured.

Remote Adapter Fallback

In some instances, the redundant adapter module can lose I/O connections for a period longer than the configured hold up time. During the hold up time, the redundant adapter module tries to get IP and configuration parameters from the M580 controller. If the redundant adapter module does not obtain those parameters during the hold up time, the following happens:

- *inputs*: retain last known values
- *outputs*: set to configured fallback value

NOTE:

- Configure the hold up time on the Control Expert **Parameter** tab.
- In high availability architectures, this situation occurs when the redundant adapter module loses the connection to the primary and secondary controllers.

Interruption of Connection to HART I/O Modules

If the connection between the controller and a drop managed by one (single) or two (dual) BMECRA31310(H) adapter modules is interrupted, communication with the HART I/O modules in the drop is restored after approximately four seconds after the BMECRA31310(H) is reconnected to the RIO network.

X80 Drop CCOTF

What's in This Chapter

CCOTF Overview

In Control Expert, CCOTF (change configuration on the fly) is called a **configuration online modification in RUN mode**, and is part of online action.

You can perform several types of CCOTF modifications on an RIO drop, in standalone or high-availability architectures. The types of modifications include adding/deleting modules, modifying module parameters, and adding an RIO drop.

When you perform CCOTF on an RIO drop, the change does not affect the other drops in the configuration.

CCOTF Instructions and Limitations

The instructions and limitations related to RIO drop in general and RIO drop managed by BM•CRA31210 adapter modules apply to RIO drop managed by BMECRA31310(H) adapter module(s):

- Adding an adapter module is supported
- Deleting a drop is not supported
- Modifying adapter parameters is not supported
- In an RIO drop configuration:
  - Adding a module is supported
  - Deleting a module is supported
  - Changing a module parameter is supported
  - Moving a module is not supported
  - Adding or deleting an extension rack is not supported

CCOTF Status: Verify %SW66 when %S10 and %S117, %S119 are set to 0. The %SW66 sets the bits 1 and 2 in the word `CRA_DIAGNOSTIC` of the device DDT instance.

CCOTF counter: %SW101 indicates the number of times CCOTF has been processed by the controller. If one BMECRA31310(H) adapter module is configured the counter is incremented by one after CCOTF is processed. If two BMECRA31310(H) adapter modules are configured, the counter is incremented by two after the CCOTF is processed, even if one of the adapter modules is disconnected before the processing the CCOTF.

For more information on instructions and limitations, refer to *Modicon M580, Change Configuration on the Fly, User Guide*

Operating Mode Scenarios

What's in This Chapter

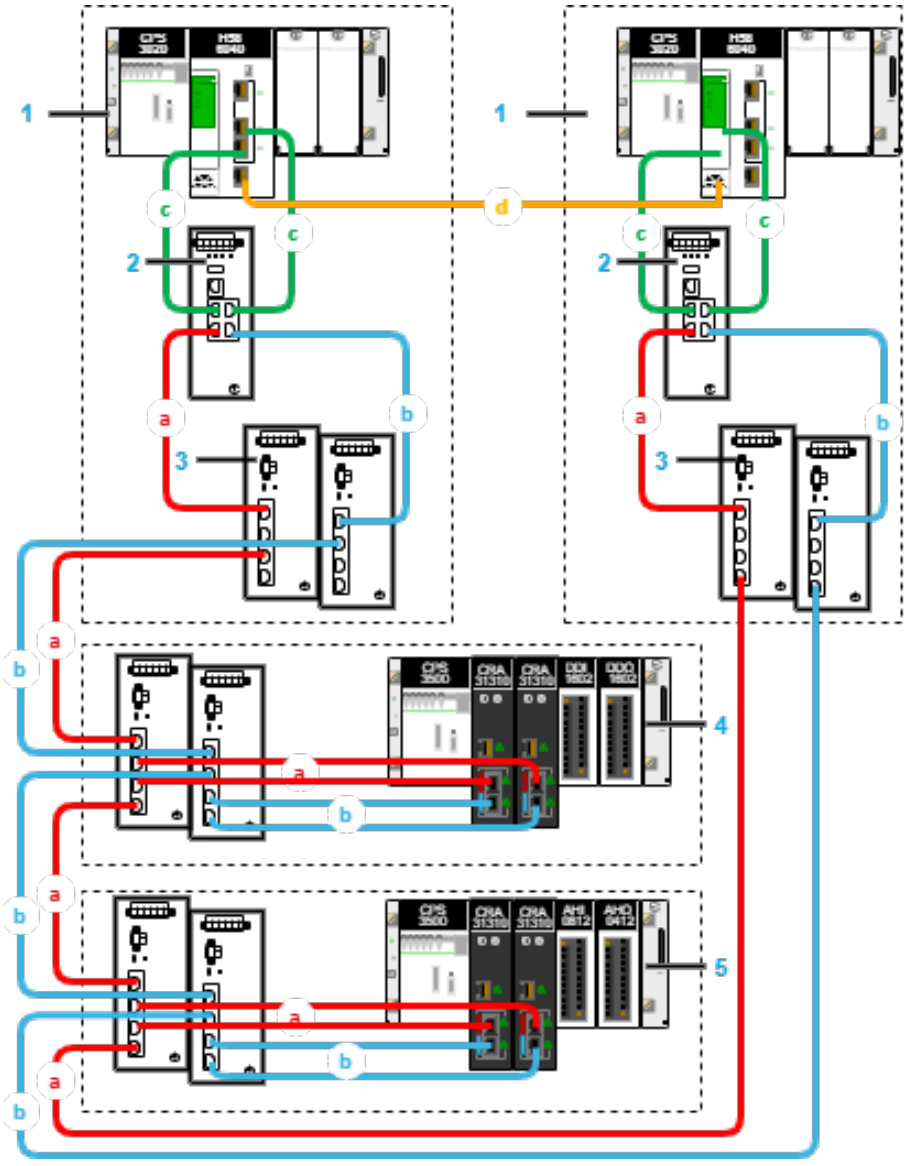
This chapter presents visual examples of communication interruptions located at different points in a M580 high-availability architecture.

Overview

An M580 high-availability architecture with Ethernet switches designing a tree topology is used for illustrating the operating state scenarios. Each Ethernet switch is dedicated to one LAN.

The different communication interruptions are grouped by location in the architecture:

- Primary/standby controller level
- PRP-RIO network level
- RIO drop level



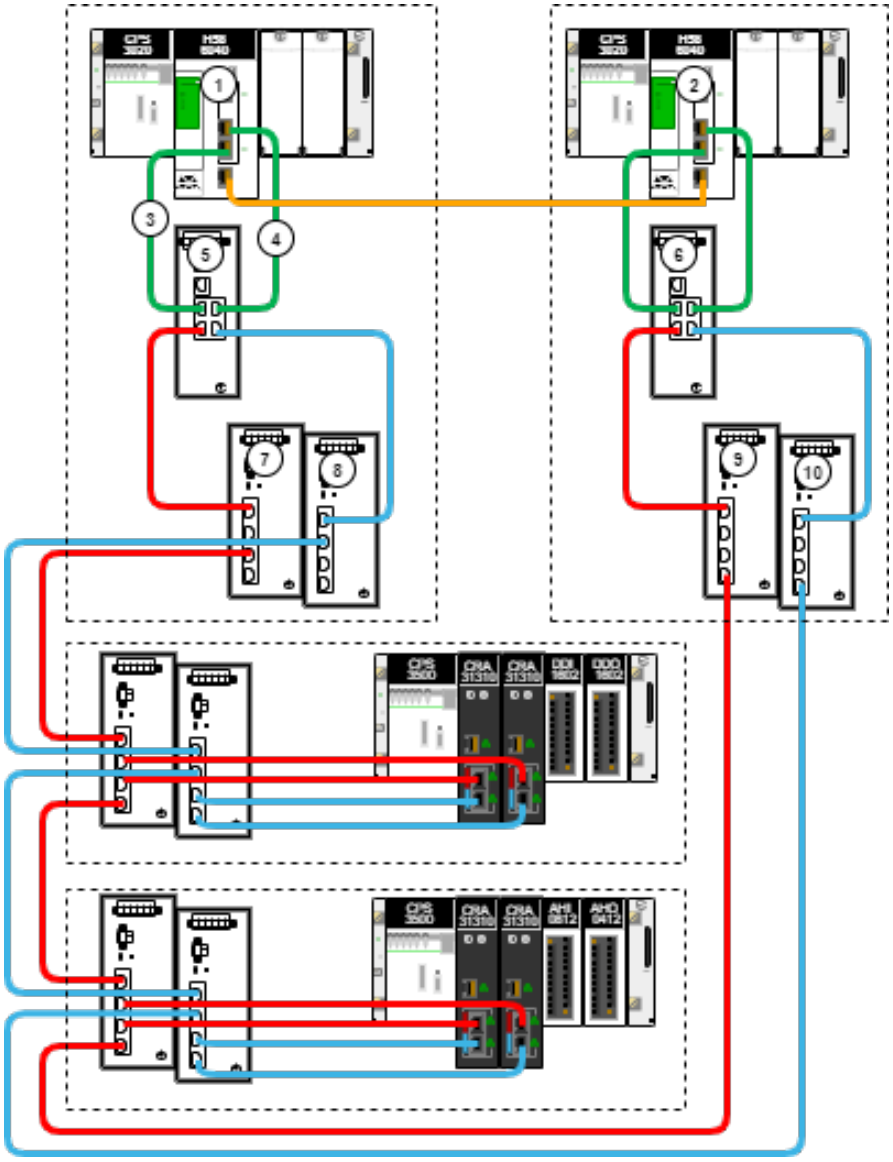
1 Modicon M580 local rack (primary / standby)
2 Modicon Redundancy switch
3 Modicon switch
4 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode) and modules using X-bus backplane for communicating.
5 X80 RIO drop with two BMECRA31310(H) adapter modules (redundant mode) and modules using both X-bus and Ethernet backplane for communicating such as HART modules.

Network legend:
a PRP LAN A – red
b PRP LAN B – blue
c RSTP LAN – green
d Hot standby communication link – orange

Communication Interruptions at Primary/Standby Controller Level

The communication interruptions presented below are related to the primary or standby controller with their dedicated Modicon Redundancy switch. It also includes the Ethernet switches connecting both primary and standby controller to the ring of the PRP-RIO network.

NOTE: The primary and standby controller with their dedicated Modicon Redundancy switches and Ethernet switches are generally located in two separate cabinets.



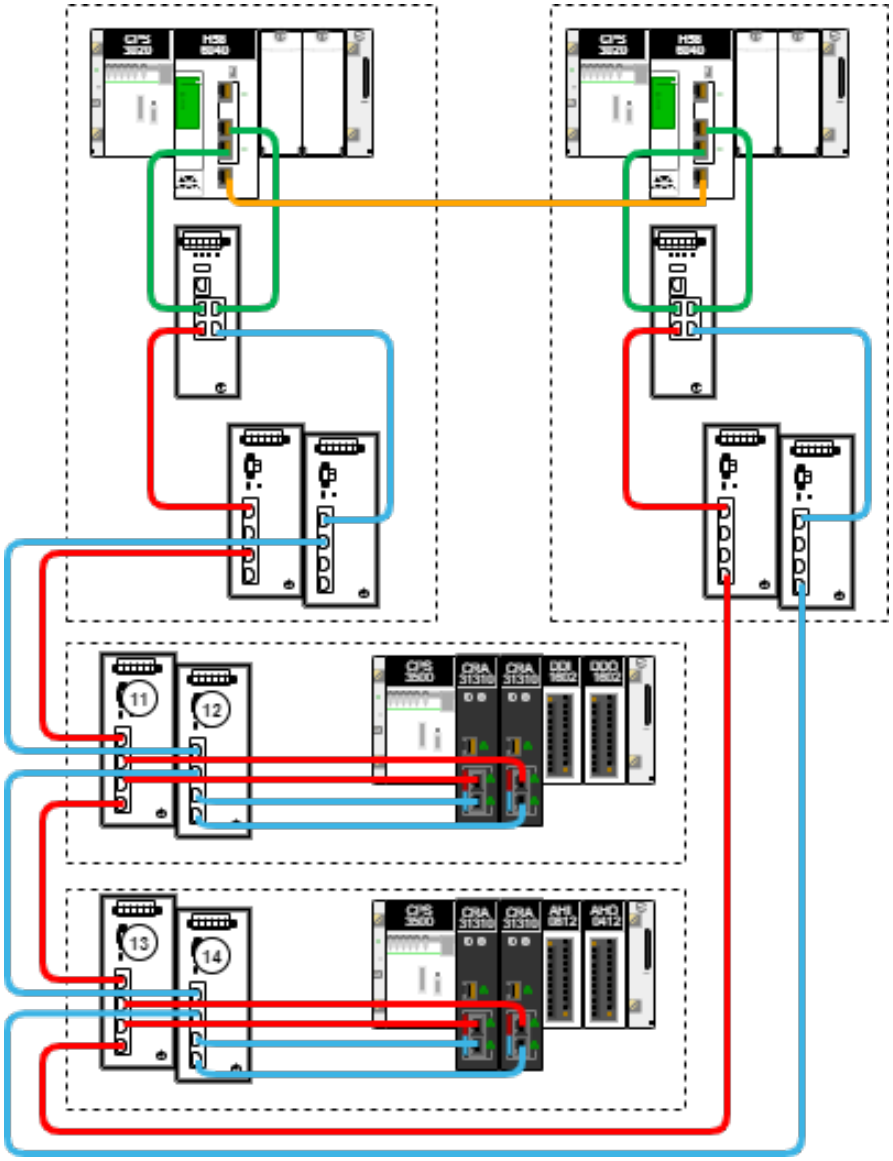
Item	Event	M580 system behavior	Diagnostic / Detection
1	The primary controller is not operational.	Controller switchover	Interruption of heartbeat on the HSBY and eRIO Implicit `REMOTE_STS_VALID` data located in the controller device DDT of type T_M_ECPU_HSBY_EXT.
2	The standby controller is not operational.	No effect	Interruption of heartbeat on the HSBY and eRIO Implicit data `REMOTE_STS_VALID` located in the controller device DDT of type T_M_ECPU_HSBY_EXT.

Item	Event	M580 system behavior	Diagnostic / Detection
3 or 4	One Ethernet link connecting the primary controller to the Modicon Redundancy switch is not operational.	No effect	Port link diagnostic Implicit data `PORT2_LINK` or `PORT3_LINK` located in the controller device DDT of type T_M_BMEP58_ECPU_EXT2.
3 and 4	Both Ethernet links connecting the primary controller to the Modicon Redundancy switch are not operational.	Controller switchover	Port link diagnostic Implicit data `PORT2_LINK` and `PORT3_LINK` located in the controller device DDT of type T_M_BMEP58_ECPU_EXT2.
5	The Modicon Redundancy switch connecting the primary controller to the PRP-RIO network is not operational.		
6	The Modicon Redundancy switch connecting the standby controller to the PRP-RIO network is not operational.	No effect	Global status of the Modicon Redundancy switch connected to the standby controller Implicit `Freshness` data located in the device DDT of the Ethernet device.
7 or 8	One Ethernet switch connecting the primary controller to the PRP-RIO network is not operational.	No effect	Global status of the Ethernet switch (s) Implicit `Freshness` data located in the device DDT of the Ethernet device(s).
9 or 10	One or both Ethernet switches connecting the standby controller to the PRP-RIO network are not operational.	No effect	Global status of the Ethernet switch (s) Implicit `Freshness` data located in the device DDT of the Ethernet device(s).
9 and 10			

For more detailed information on controller switchover, refer to *Modicon M580 Hot Standby, System Planning Guide for Frequently Used Architectures*

Communication Interruptions at PRP-RIO Network level

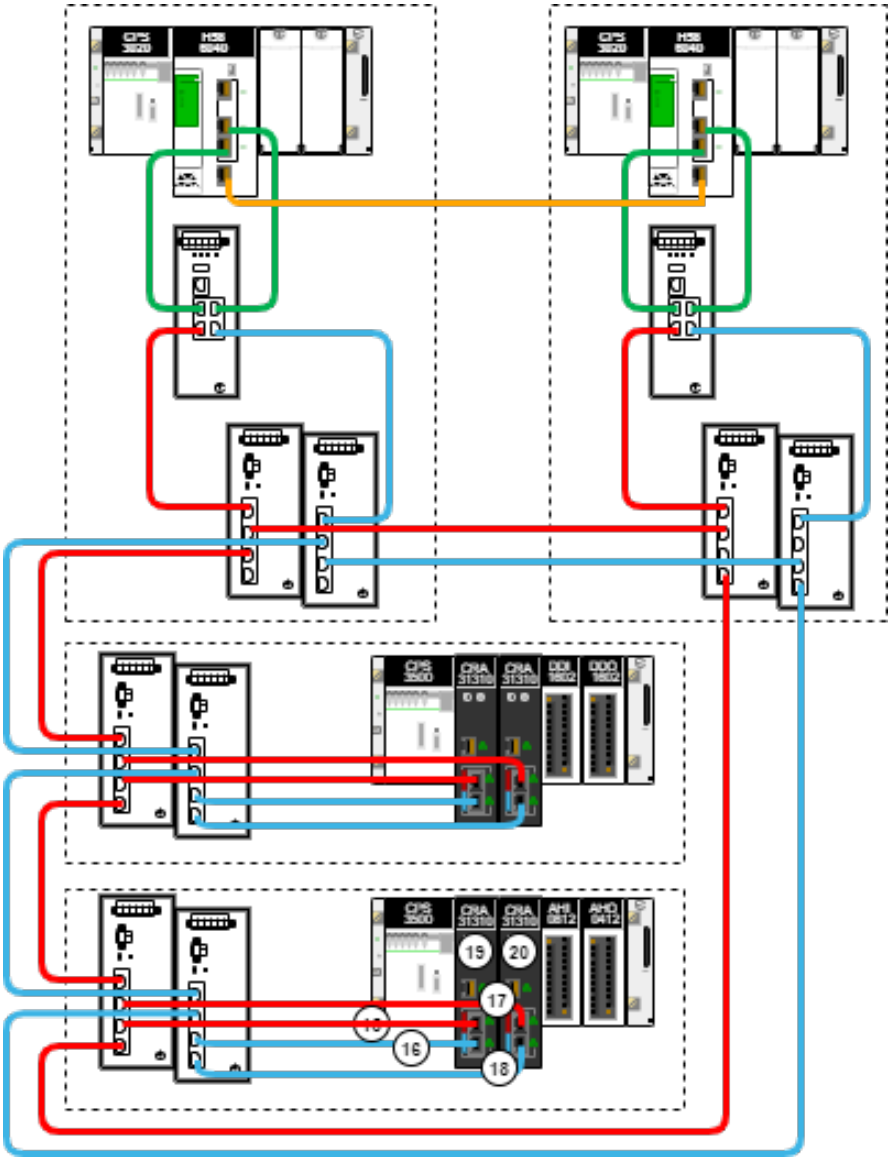
The communication interruptions presented below are related to the Ethernet switches connecting the RIO drops to the ring of the PRP-RIO network.



Item	Event	M580 system behavior	Diagnostic / Detection
11 or 12 13 or 14	One Ethernet switch connecting one RIO drop to the PRP-RIO network is not operational.	No effect	Port link diagnostic of the CRA Implicit data `PORT2_LINK` and/or `PORT3_LINK` located in the CRA device DDT of type T_M_CRA_EXT2_IN.
11 and 12 13 and 14	Both Ethernet switches connecting one RIO drop to the PRP-RIO network are not operational.	The RIO drop is no more operational	Interruption of connection to the RIO drop Implicit `DROP_HEALTH` data located in the controller device DDT of type T_BMEP58_ECPU_EXT2.

Communication Interruptions at RIO Drop Level

The communication interruptions presented below are related to the redundant RIO drops.



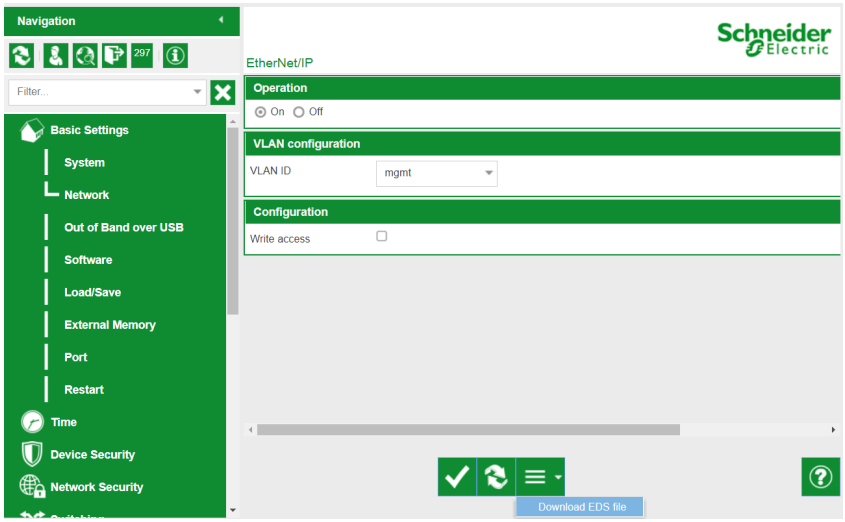
Item	Event	M580 system behavior	Diagnostic / Detection
15 or 16	One Ethernet link (LAN A or LAN B) connecting the adapter assigned to the MASTER role to the PRP-RIO network is not operational.	No effect	Port link diagnostic of the CRA Implicit data `PORT2_LINK` and/or `PORT3_LINK` located in the CRA device DDT of type T_M_CRA_EXT2_IN.
15 and 16	Both Ethernet links (LAN A and LAN B) connecting the adapter assigned to the MASTER role to the PRP-RIO network are not operational.	CRA switchover	CRA diagnostic Implicit `CRA_STATE` data located in the CRA device DDT of type T_M_CRA_EXT2_IN.
17 and 18	Both Ethernet links (LAN A and LAN B) connecting the adapter assigned to the NOT MASTER role to the PRP-RIO network are not operational.	No effect	CRA diagnostic Implicit `CRA_STATE` data located in the CRA device DDT of type T_M_CRA_EXT2_IN.

Item	Event	M580 system behavior	Diagnostic / Detection
19	The adapter assigned to the MASTER role is not operational.	CRA switchover	CRA diagnostic Implicit `CRA_STATE` data located in the CRA device DDT of type T_M_CRA_EXT2_IN.
20	The adapter assigned to the NOT MASTER role is not operational.	No effect	CRA diagnostic Implicit `CRA_STATE` data located in the CRA device DDT of type T_M_CRA_EXT2_IN.

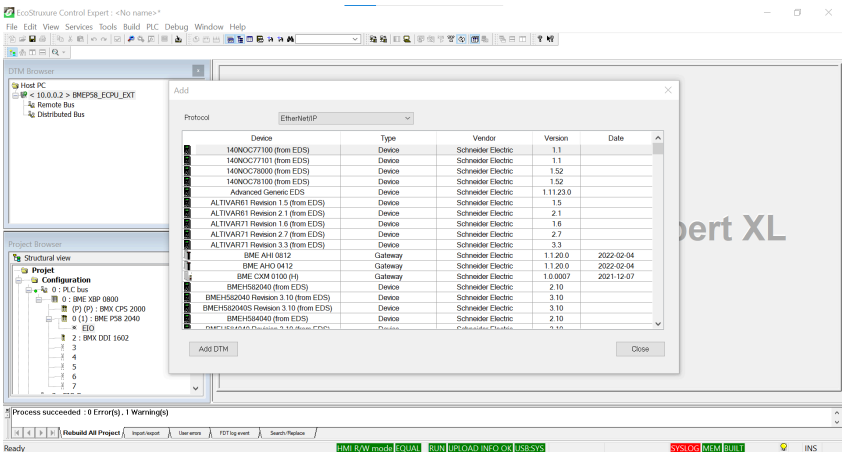
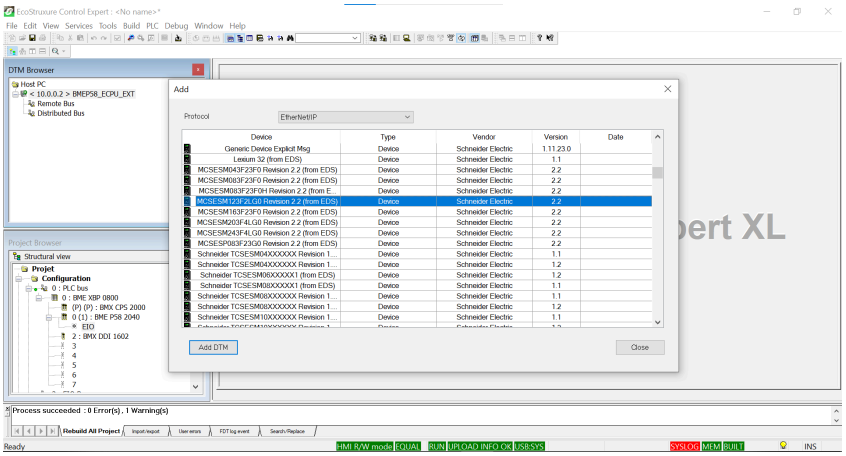
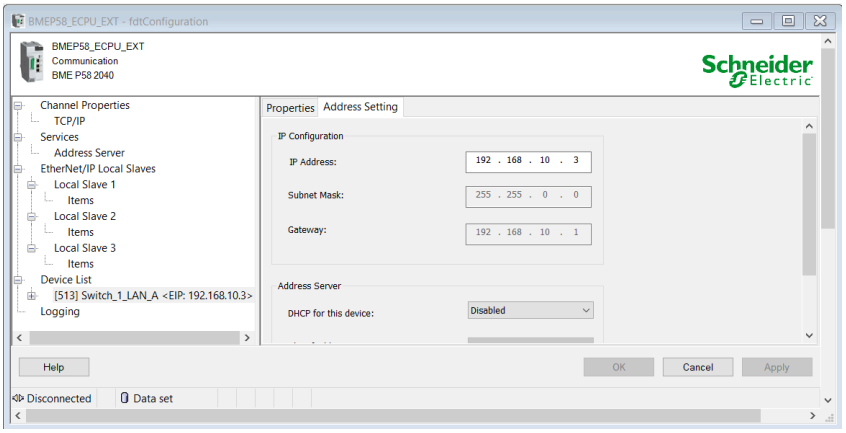
Accessing Ethernet Switch Data for Diagnostic

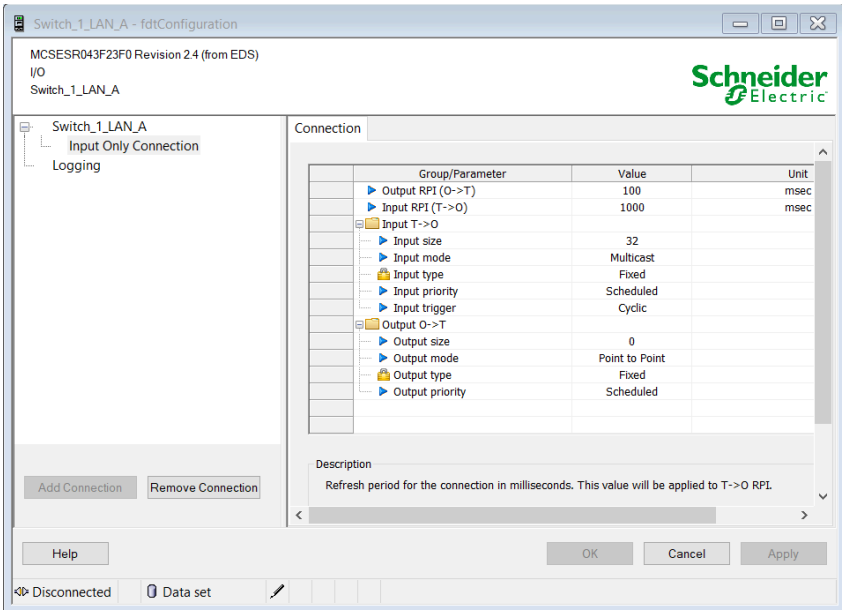
If you want to use an EtherNet/IP device for which no DTM is in the catalog, you need to import the EDS file into the catalog to create the corresponding DTM.

A Modicon switch is used for illustrating the steps of the following procedure:

Step	Action
1	To configure the Ethernet switch, open an Internet browser and enter the following URL: `https://[Switch IP address]` Use default username/password combination admin/private to log in. **NOTE:** On the first login you are required to change the password.
2	Verify that the EtherNet/IP function is enabled, page 45.
3	Exporting the EDS file of a EtherNet/IP device.  **1.** On the **Navigation** left pane, select **Advanced > Industrial Protocols > EtherNet/IP**. **2.** Click the  icon to display the submenu **Download EDS file**, and click it. **NOTE:** The EDS file is copied in a zip file onto the PC.
4	Add the EDS file to the Control Expert Hardware Catalog. **1.** In your Control Expert project, open the **DTM Browser** window (**Tool > DTM Browser**). **2.** In the **DTM Browser**, select the M580 Master DTM of the controller, right-click and scroll to **Device menu > Additional functions > Add EDS to library**. **3.** The **EDS Addition** wizard opens. **4.** You can now add the EDS file to the library. **NOTE:** For more detailed information, refer to chapter *Adding an EDS File to the Hardware Catalog* (see EcoStruxure™ Control Expert, Operating Modes).

The following procedure describes the steps for adding the DTM of the EtherNet/IP device(s) and accessing the implicit data for diagnostic purposes:

Step	Action
1	In the **DTM Browser**, select the M580 Master DTM of the controller, right-click and select **Add**. The following window opens: 
2	To limit the number of available devices, you can filter by selecting the **EtherNet/IP** protocol.  A. Select the DTM of the EtherNet/IP device you want to add. B. Click **Add DTM**
3	Configure the IP address of the EtherNet/IP device for communicating with the controller:  A. Open the M580 Master DTM of the controller. B. In the **Device List**, select the EtherNet/IP device to configure. C. In the **Address Setting** tab, enter the IP address of the device. D. Click **Apply** for validating the configuration.

Step	Action
4	Configure an EtherNet/IP connection (Target —> Originator) between the EtherNet/IP device and the controller. The following illustrates the configuration of the Modicon Redundancy Switch – MCSESR043F2•••(C):  A. Open the DTM of the EtherNet/IP device. B. Remove the exclusive owner connection by clicking the **Remove Connection** button. C. Add an input only connection by clicking the **Add Connection** button. D. Set the **Input RPI (T->O)** parameter to 1000 ms. E. Click **Apply** to save the new connection.
5	When the EtherNet/IP device DTM is added to the list of devices that are scanned by the Ethernet communication module (M580 controller), the respective EtherNet/IP device DDT is added in the **Data Editor**. You can add the variable to an Animation Table to read the status of the EtherNet/IP device for diagnosing and use the data in your application. Refer to chapter Modicon Switch Device DDT Structure, page 205 for the detailed description of the available data in implicit exchanges.

Module Diagnostic and Maintenance

What’s in This Part

Module Diagnostics

What's in This Chapter

Overview

This chapter describes the diagnostics for the BMECRA31310(H) modules:

- LED indicators on the module
- Control Expert diagnostic screens
- Implicit exchanges (device DDT):
  - TheBMECRA31310(H) device DDT.
  - For diagnostic provided by the M580 controller device DDT, refer to *Modicon M580, Hardware, Reference Manual*.
- Explicit exchanges for extended diagnostics using:
  - Modbus TCP explicit messages
  - EtherNet/IP explicit messages
- SNMP agent
- Syslog client

NOTE: System availability and monitoring single point of error are linked to continuously monitoring the overall high-availability I/O network architecture.

LED Diagnostics

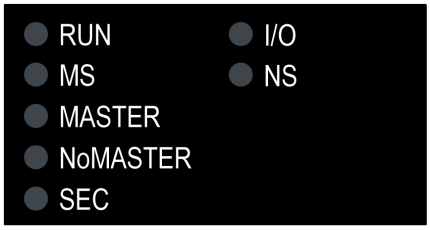
LED State and Flash Rate

This table describes the LED state used in the following tables for diagnosing the adapter module:

LED State	Flash Rate	State Symbol
LED is off	OFF	
LED is on	ON	
LED is flashing	• 200 ms OFF • 200 ms ON	
One of the possible pattern	–	

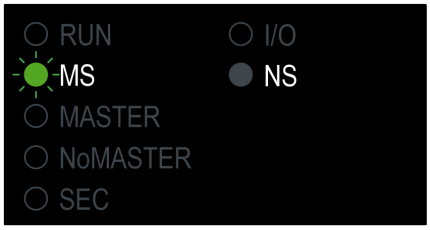
Module Power-Up Sequence

LED Status	Sequence
	**1.** Red LEDs are ON.
	**2.** LEDs are ON. **NOTE:** The color rendition for bicolor LEDs merges green with red.

LED Status	Sequence
	**3.**LEDs are OFF.
	**4.** RUN and I/O LEDs are ON and the other LEDs are OFF.

NOT CONFIGURED State Diagnostic

The LED MS when green flashing is characteristic of the *NOT CONFIGURED* state. The status of the LED NS complete the diagnostic of the adapter module.

LED Status	Condition
	The IP address is not valid.
	The IP address is valid but the configuration is not valid.

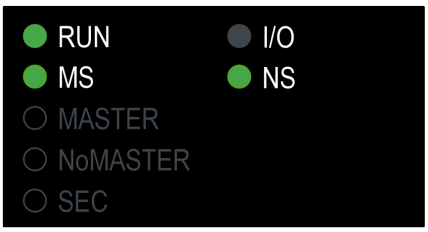
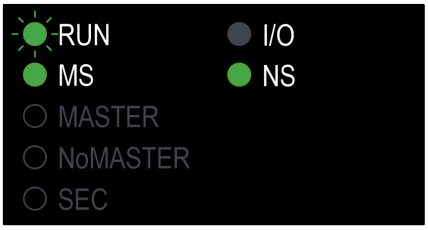
CONFIGURED State Diagnostic

The combination of the LEDs RUN and NS when green flashing is characteristic of the *CONFIGURED* state. The status of the LED I/O complete the diagnostic of the adapter module in this state.

LED Status	Condition
	No external error detected
	External error detected

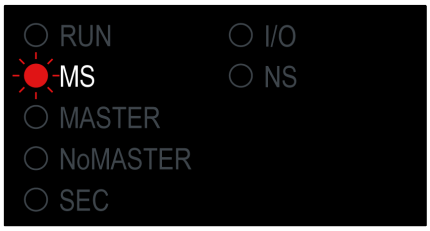
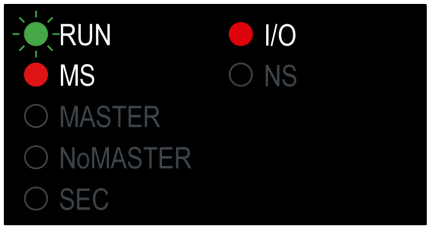
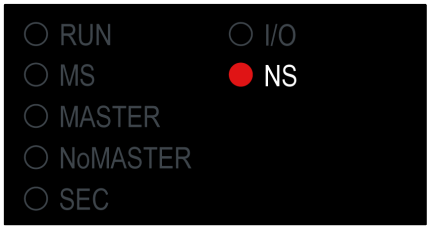
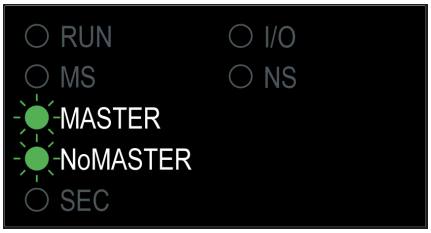
CONNECTED State Diagnostic

The combination of the LEDs MS and NS steady green is characteristic of the *CONNECTED* state. The status of the LEDs RUN and I/O complete the diagnostic of the module in this state.

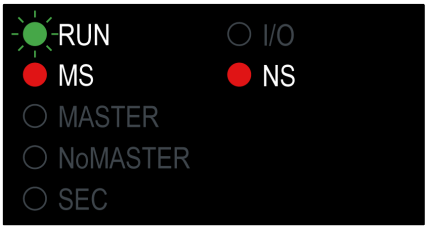
LED Status	Condition
	Controller/Task in RUN: normal operation
	Controller/Task in RUN: external detected error
	Controller/Task in STOP: normal operation

LED Status	Condition
	Controller/Task in STOP: • Input/output detected error(1), or • channel configuration detected error
(1)The detected error originates from a module or a channel configuration.	

ERROR State Diagnostic

LED Status	Condition
	Recoverable detected error
	Non-recoverable detected error
	One or more owner connections has timed out
	Duplicate IP address
	• Module inserted in incorrect slot of the rack, or • firmware or configuration mismatched (in redundant mode)

Firmware Download State Diagnostic

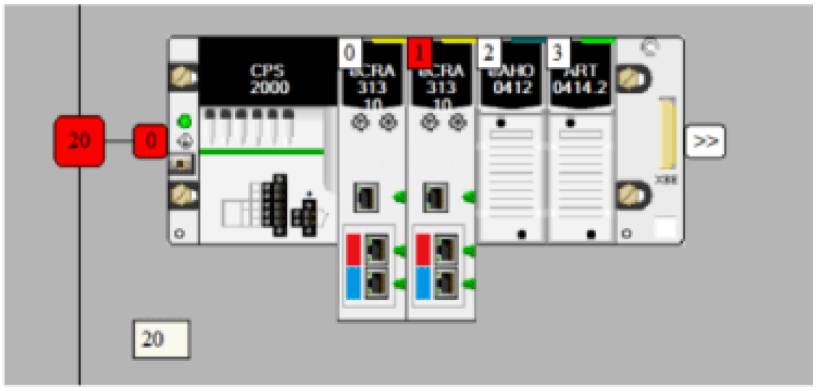
LED Status	Condition
	*Firmware Download* state

Viewing Diagnostics in Control Expert

The bus editor in Control Expert uses color animation to display the status of each drop, rack, or module on the **EIO Bus**.

The slot number of the drop/rack/module appears in red when a detected error is associated with that slot.

For a module, the red display indicates the module is missing, inoperable, or improperly configured.

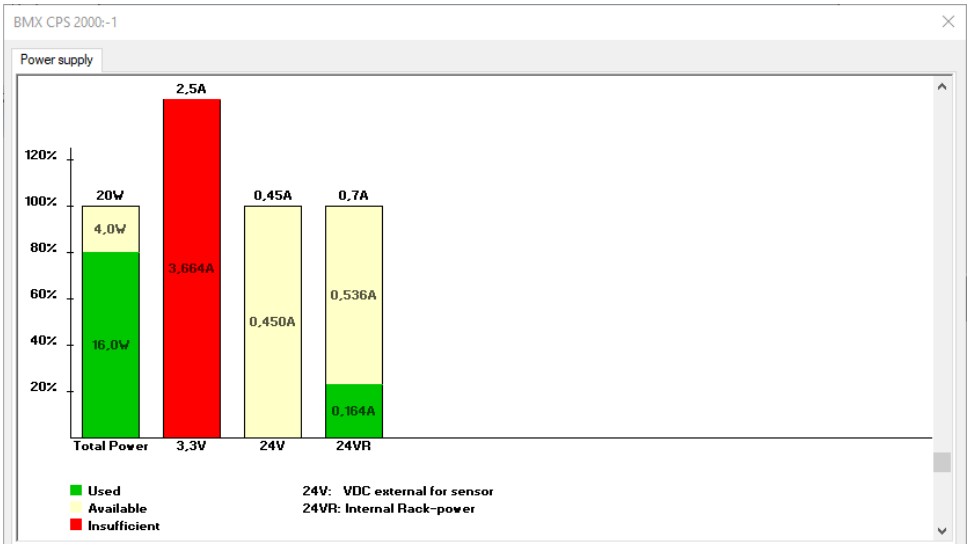


X80 Drop Power Consumption

In Control Expert you can monitor the power consumption budget for the main and/or extended rack of the X80 remote I/O drops:

Steps	Action
1	Open the **EIO Bus** window (In the **Project Browser**, double-click **Configuration > EIO Bus**)
2	Right-click the power supply module and select **Power Supply and IO Budget**. **Result:** The bar chart is displayed.
3	Click the **Power Supply** tab.

Budget example:



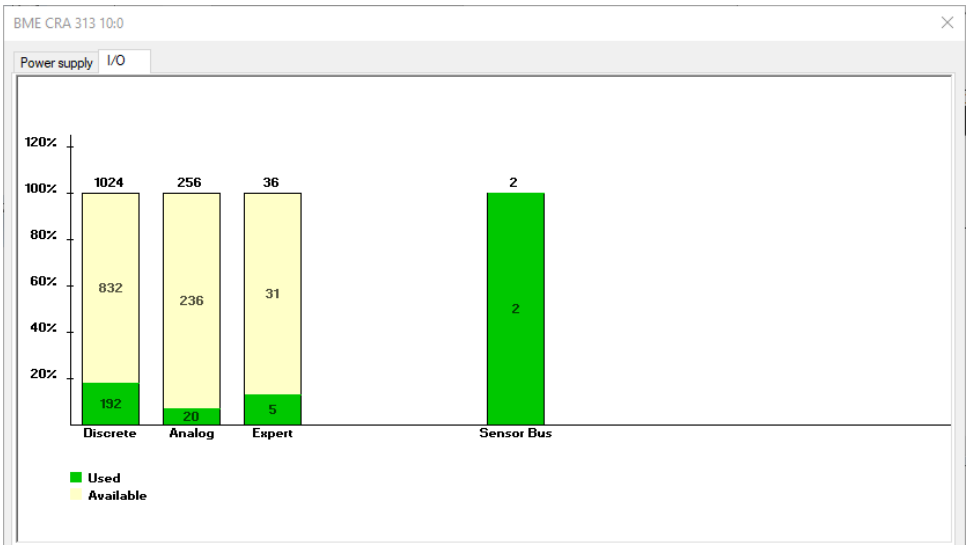
X80 Drop I/O Channel Consumption

In Control Expert you can monitor the number of channels configured in the X80 remote I/O drop:

Steps	Action
1	Open the **EIO Bus** window (In the **Project Browser**, double-click **Configuration > EIO Bus**)
2	Right-click the X80 redundant adapter module and select **Power Supply and IO Budget**. **Result:** The bar chart is displayed.
3	Click the **I/O** tab.

NOTE: In case of two adapter modules in the same drop (redundant mode), the adapter module located in the slot 0 provides the I/O channel budget.

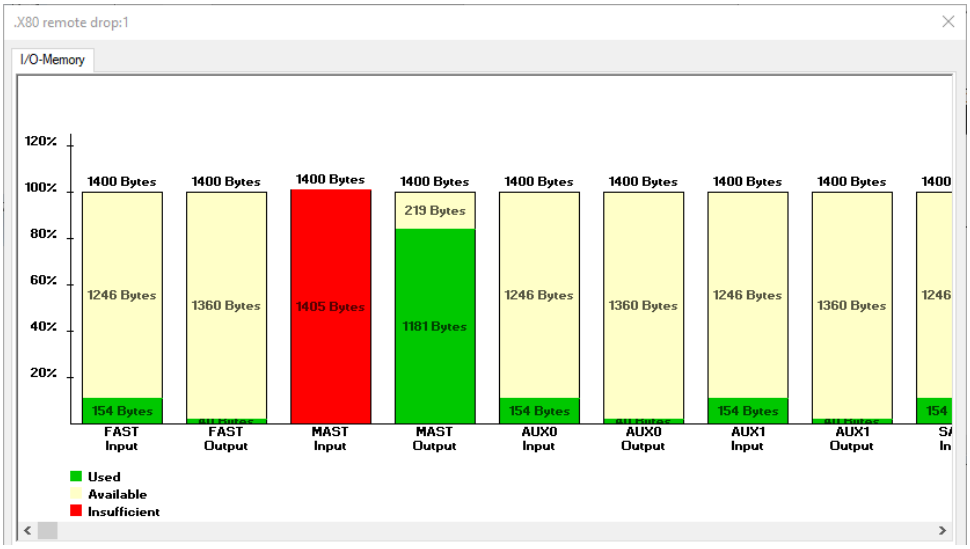
Budget example:



X80 Drop I/O Consumption Budget

In Control Expert you can monitor the I/O memory consumption by viewing the X80 remote I/O drop properties. In the **Project Browser**, double-click **Configuration > EIO Bus > .X80 remote drop**. Then right-click the X80 remote drop you want to monitor and select **Properties**.

This is an example of an **IO-Memory** tab:



NOTE: Exceeding the I/O memory capacity is also reported in the **Output Window**.

Device DDT Structure

T_M_CRA_EXT2_IN Structure

The following table describes the diagnostic parameters for the BMECRA31310 (H) adapter module in implicit exchanges:

Name	Type	Bit	Description
IO_HEALTH_RACK0	WORD	–	Health bits of rack 0: slots 0...15 (the Least Significant bit of the Word corresponding to slot 0). **NOTE:** In redundant mode, you cannot rely on this parameter in the device DDT instance of the adapter module with the *NOT MASTER* role.
IO_HEALTH_RACK1	WORD	–	Health bits of rack 1: slots 0...15 (the Least Significant bit of the Word corresponding to slot 0). **NOTE:** In redundant mode, you cannot rely on this parameter in the device DDT instance of the adapter module with the *NOT MASTER* role.
DEVICE_NAME	string [16]	–	Device name of the RIO drop.
VERSION	WORD	–	Firmware version (4 digits coded in BCD).
ROTARY_SWITCHES	BYTE	–	Rotary switch value at power up.
CRA_STATE	BYTE	–	1: adapter module is idle.
			2: adapter module is stopped.
			3: adapter module is running.

Name		Type	Bit	Description
CRA_ DIAGNOSTIC [WORD]	GLOBAL_IO_ HEALTH	BOOL	0	0: At least one I/O module in the drop is detected in error.
	CCOTF_IN_ PROGRESS	BOOL	1	CCOTF is in progress on the drop managed by the adapter module.
	CCOTF_INVALID_ CONF	BOOL	2	CCOTF is not valid on the drop managed by the adapter module.
	IOPL_MISMATCH	BOOL	3	The I/O configuration in the drop differs from that expected by the controller for the application.
	SWITCH_CHANGE	BOOL	4	The rotary switch settings have been modified since the last power up. This bit is reset if the rotary switch is returned to its original setting.
	DROP_COM_ HEALTH	BOOL	5	This bit indicates the drop communication health (set to 1 when communication is established between the RIO drop and the I/O scanner).
	REDUNDANT_ POWER_SUPPLY_ STATUS	BOOL	6	This bit indicates that redundant power is present (1) or not present (0).
	MASTER	BOOL	7	1 = the adapter module is assigned to the *MASTER* role. 0 = the adapter module is assigned to the *NOT MASTER* role. **NOTE:** During an adapter module swap, it might happen that for one MAST cycle the flag MASTER in the DDT is equal to 1 for the two adapter modules. If this happens, during that same cycle, there is 50% chance that the IN values of that drop keep the same values they had during the previous MAST cycle.
	SLOT	BOOL	8	1 = the adapter module is located in slot 1 of the rack. 0 = the adapter module is located in slot 0 of the rack.
	REDUNDANT	BOOL	9	1 = the adapter module redundancy is OK. 0 = the adapter module redundancy is not OK.
	SWAP	BOOL	—	1 = during the cycle where the adapter module is assigned to the*MASTER* role. 0 = the rest of the time.
	FW_ COMPATIBILITY_ ERROR	BOOL	—	1 = the peer adapter module has an incompatible version of the firmware (no HSBY synchronization).
	FW_MISMATCH	BOOL	—	1 = the peer adapter module has a different version of the firmware (the synchronization of the HSBY is not guaranteed).
CYCLE_CURR_TIME		UINT	—	This word indicates the execution time of the last adapter module cycle. It has values between [0.65535] with a resolution of 0.01 ms, therefore, the last cycle time is between [0.655] ms.

Name		Type	Bit	Description
CYCLE_MAX_TIME		UINT	—	This word indicates the longest adapter module cycle execution time since the last start. It has values between [0.65535] with a resolution of 0.01 ms, therefore, the longest cycle time is between [0,655] ms.
CYCLE_MIN_TIME		UINT	—	This word indicates the shortest adapter module cycle execution time since the last start. It has values between [0.65535] with a resolution of 0.01 ms, therefore, the shortest cycle time is between [0.655] ms.
TIME_STAMP_RECORDS		UINT	—	This word contains the number of records available in the local drop event buffer.
TS_ DIAGNOSTIC_ FLAGS (WORD)	TIME_VALID	BOOL	0	The time is valid and synchronized.
	CLOCK_FAILURE	BOOL	1	A clock error has been detected.
	CLOCK_NOT_SYNC	BOOL	2	The clock is not synchronized.
	BUFF_FULL	BOOL	3	The local drop event buffer is full.
TS_BUF_FILLED_PCTAGE		BYTE	—	This byte reports the percentage of the local drop event buffer filled (0...100).
TS_EVENTS_STATE		BYTE	—	Refer to Main States, page 138.
ETH_STATUS (BYTE)	PORT1_LINK	BOOL	0	0 = Service port (ETH1) link is down.
				1 = Service port (ETH1) link is up.
	PORT2_LINK	BOOL	1	0 = PRP port B (ETH2) link is down.
				1 = PRP port B (ETH2) link is up.
	PORT3_LINK	BOOL	2	0 = PRP port A (ETH3) link is down.
				1 = PRP port A (ETH3) link is up.
	ETH_BKP_PORT_ LINK	BOOL	3	0 = Ethernet backplane link is down.
				1 = Ethernet backplane link is up.
	RPI_CHANGE	BOOL	4	RPI change: EtherNet/IP RPI change is in progress (during CCOTF).
	REDUNDANCY_ OWNER	BOOL	6	1 = Redundant owner is present.
				0 = Redundant owner is not present.
	GLOBAL_STATUS **NOTE:** Refer to the **SERVICE_ STATUS** byte below.	BOOL	7	0 = At least 1 service is not operating normally.
				1 = All services are operating normally.

Name		Type	Bit	Description
SERVICE_ STATUS (BYTE)	PORT502_SERVICE	BOOL	2	0 = Port 502 service is not operating normally.
				1 = Port 502 service is operating normally or disabled.
	SNMP_SERVICE	BOOL	3	0 = SNMP service is not operating normally.
				1 = SNMP service is operating normally or disabled.
	EVENT_LOG_ STATUS	BOOL	4	0 = Event log service is not operating normally.
				1 = Event log service is operating normally or disabled.
	ETH_BKP_FAILURE	BOOL	5	0 = Ethernet backplane hardware status is not OK.
				1 = Ethernet backplane hardware status is OK.
	ETH_BKP_ERROR	BOOL	6	0 = An error is detected on the Ethernet backplane or the adapter module is assigned to the *NOT MASTER* role.
				1 = The adapter is assigned to the *MASTER* role and no errors are detected on the Ethernet backplane.
	LOG_SERVER_ NOT_REACHABLE	BOOL	7	0 = Acknowledgment received from syslog server.
				1 = No acknowledgment received from syslog server.
SERVICE_ STATUS2 (BYTE)	NTP_SYNC	BOOL	0	0 = Not synchronized to the NTP server.
				1 = Synchronized to the NTP server.
	NTP_SERVICE	BOOL	1	0 = NTP Daemon is down.
				1 = NTP Daemon is active.
	NTP_QUALITY_ WARNING	BOOL	2	0 = The quality of the clock conforms to what has been set in the configuration.
				1 = The quality of the clock is out of the range that has been set in the configuration.
ETH_PORT_STATUS (WORD) The combined 2-bit values indicate the port conditions.		WORD	0/1	Service port function: • 0 = Disabled • 1 = Access port • 2 = Mirror port

Name		Type	Bit	Description
ETH_PRP_STATUS (BYTE)	PRP_LAN_A_HEALTH	BOOL	—	0 = An error is detected or no activity on the PRP LAN A.
				1 = No errors are detected on the PRP LAN A.
	PRP_LAN_B_HEALTH	BOOL	—	0 = An error is detected or no activity on the PRP LAN B.
				1 = No errors are detected on the PRP LAN B.
	PRP_WRONG_LAN_A	BOOL	—	1 = PRP supervision frames received on PRP LAN A with an incorrect LAN ID. **NOTE:** If a PRP_WRONG_LAN_A is detected on a Redundant CRA, the other Redundant CRAs in the controller configuration have their PRP_WRONG_LAN information bit set to 1, even if their connections are good.
				0 = ok
	PRP_WRONG_LAN_B	BOOL	—	1 = PRP supervision frames received on PRP LAN B with an incorrect LAN ID. **NOTE:** If a PRP_WRONG_LAN_B is detected on a Redundant CRA, the other Redundant CRAs in the controller configuration have their PRP_WRONG_LAN information bit set to 1, even if their connections are good.
				0 = ok
ACCEPTED_PRP_COUNTER_LAN_A		UDINT	—	Accepted received PRP frames counter on LAN A.
ACCEPTED_PRP_COUNTER_LAN_B		UDINT	—	Accepted received PRP frames counter on LAN B.
DROPPED_DUPLICATE_PRP_COUNTER_LAN_A		UDINT	—	Dropped duplicate received PRP frames counter on LAN A.
DROPPED_DUPLICATE_PRP_COUNTER_LAN_B		UDINT	—	Dropped duplicate received PRP frames counter on LAN B.
NTP_WITHIN		UINT	—	Estimated accuracy of the clock, in milliseconds.
MAX_PACKET_INTERVAL		UINT	—	Maximum packet interval (ms) for output packets (from scanner to adapter).
IN_BYTES		UINT	—	Number of bytes (octets) received.
IN_ERRORS		UINT	—	Number of inbound packets containing detected errors.
OUT_BYTES		UINT	—	Number of bytes (octets) sent.
OUT_ERRORS		UINT	—	Number of outbound packets that contain detected errors.
EVENT_LOG_BUF_FREE_PCTAGE		WORD	—	Percentage of the buffer free [0..100]
NUMBER_OF_LOSTS_EVENTS		WORD	—	Number of events lost since last restart.
SOE_UNCERTAIN		BOOL	—	The sequence of events (SOE) in the local drop event buffer is indeterminable. The SOE_UNCERTAIN is reset when the sequence of events is OK.

Main States of the Time Stamp Source

The TS_EVENTS_STATE byte reports the main state of the source of the time stamp events:

Byte Value (hex)	Description
20	Wait for client
31	ValuesSynchro requested and waiting for buffer below the threshold.
32	ValuesSynchro started
40	Event Stamping

Ethernet Diagnostics Using Explicit Messages

Overview

The following Ethernet diagnostics are available by explicit messages:

- Data rate on the Ethernet TCP/IP network.
- Ethernet Activity information: This is the counter of Ethernet frames transmitted and received by the adapter module.
- Ethernet link status.
- Redundancy status.
- Port 502 Status: Modbus port
- Half / Full duplex mode: This is the mode of the RIO network.

EtherNet/IP CIP Requests

The BMECRA31310(H) adapter module supports the following CIP objects:

Required CIP objects	Identity (class code 01 Hex)
	Message Router (class code 02 Hex)
	Connection Manager (class code 06 Hex)
	Network specific object: • TCP/IP Interface (class code F5 Hex) • Ethernet Link (class code F6 Hex)
Application CIP objects	PRP Protocol (class code 56 Hex)
Schneider-specific CIP objects	EtherNet/IP Interface Diagnostics (class code 350 Hex)
	I/O Connection Diagnostics (class code 352 Hex)
	Service Port Control (class code 400 Hex)
Refer to chapter Diagnostics Available through EtherNet/IP CIP Objects, page 172 for details.	

EtherNet/IP explicit messages can be performed:

- Using the **EtherNet/IP Explicit Message** window in the Control Expert M580 DTM to send an explicit message to the adapter module on the network.
- Using the function block *DATA_EXCH*, *READ_VAR*, and *WRITE_VAR* in the application.

Modbus TCP Requests

You can use Modbus function code commands to perform diagnostics on the BMECRA31310(H) adapter module.

Modbus commands can reach the BMECRA31310(H) adapter module over its backplane port. It accepts the Modbus TCP/IP client data flow from a client that can access the backplane Ethernet network such as an M580 controller or a BMENOC0301.

The BMECRA31310(H) adapter module supports the following Modbus TCP requests:

Function code Dec (Hex)	Sub-function code Dec (Hex)	Function description
3 (3)	-	This Modbus function is used to read the content of contiguous block of holding registers in the adapter module (Modbus server). The module provides diagnostic data including: • Basic network diagnostics • Ethernet port diagnostics (internal port, service port, PRP LAN A port, PRP LAN B port, and backplane port) • Modbus port 502 diagnostics • Modbus port 502 connection table • NTPv4 diagnostics data • QoS diagnostics data • Identity data Refer to Modbus Function Code 3, page 151 for details on Modbus register mapping of the data.
8 (8)	22 (16)	This Modbus function is used to get/clear Ethernet statistics. Refer to Modbus Function Code 8, page 169 for details.
43 (2B)	14 (E)	This Modbus function is used to read device identification. Refer to Modbus Function Code 43, page 171 for details.

Modbus explicit message can be performed:

- Using the **Modbus Explicit Message** window in the Control Expert M580 DTM to send an explicit message to the adapter module on the network.
- Using the function block *DATA_EXCH* in the application.

SNMP Agent

Overview

The SNMP software agent provides access to a local MIB of objects that reflects the resources and activity of the BMECRA31310(H) adapter module. The agent responds to SNMP manager commands to retrieve values from the local MIB and to set values in the MIB.

To configure SNMP on the BMECRA31310(H) adapter module, you define the relationship between the manager and the agent.

MIB

The BMECRA31310(H) adapter module supports the standard MIB-II and the IEC-62439-3-MIB (PRP-MIB), page 200.

Example of standard MIB-II supported:

- system (OID 1.3.6.1.2.1.1)
- ip (OID 1.3.6.1.2.1.4)
- TCP (OID 1.3.6.1.2.1.6)
- snmp (OID 1.3.6.1.2.1.11)
- bridge (OID 1.3.6.1.2.1.17)

  NOTE: For detailed content of the standard MIB-II, refer to *RFC1213 - Management Information Base for Network Management of TCP/IP-based internets*.

Syslog Service

Introduction

The syslog service is used to log events regarding cybersecurity.

The BMECRA31310(H) adapter module acts as a syslog client to synchronize security events with a remote syslog server. You can access to the syslog server from a BMENUA0100 module or a router.

The TCP protocol is used for communication with the Syslog server. The Syslog messages respect the format described in RFC 5424 specification.

Syslog Server

The syslog service uses the same syslog server as the M580 controller.

To configure the syslog service in Control Expert, select **Tools > Project Settings > General > PLC diagnostics**

Select the **Event Logging** checkbox to edit the syslog server address and port number. The TCP protocol is used for transporting the syslog event messages and is non-modifiable.

Syslog Service Operation

Up to 2048 event messages are stored in the local buffer of the BMECRA31310 (H) adapter module. The buffer operates as a circular one with the most recent events overwriting and replacing the oldest events when it is full.

NOTE: Diagnosing prior events requires to record the syslog event in the syslog server.

The BMECRA31310(H) adapter module detects the following events:

- Successful and unsuccessful connections Modbus TCP and EIP Explicit TCP
- Successful and unsuccessful HTTPS login for firmware update
- Disconnection (HTTPS, Modbus TCP, EIP Explicit TCP)
- Configuration change
- Firmware update
- Invalid firmware
- Ethernet port link up/link down
- PRP topology change
- Program operating mode change (Run, Stop)
- Module reboot
- Product certificate modification
- Swap or switchover of the operating mode when using BMECRA31310(H) adapter module

For more detailed information on syslog event messages, refer to *Modicon Controller Platforms, Cyber Security, Reference Manual*

Syslog Service Diagnostics

The BMECRA31310(H) adapter module provides the following diagnostics for the syslog service in the device DDT:

- EVENT_LOG_STATUS bit

- LOG_SERVER_NOT_REACHABLE bit
- EVENT_LOG_BUF_FREE_PCTAGE
- NUMBER_OF_LOSTS_EVENTS

Module Maintenance

What's in This Chapter

This chapter describes the steps for updating the firmware for your adapter module. It also describes the procedure to follow when replacing a module.

Module Firmware Update

Firmware Update Tool

EcoStruxure™ Automation Device Maintenance (EADM) is required to update the module firmware. It is a standalone tool that allows you to download the firmware package on single or multiple devices simultaneously.

For downloading and installing the latest software version, refer to Schneider Electric web site in the section **Support > Products documents & Software > Software & Firmware**. To refine in the section **Software & Firmware**, you can use the **Search** box and type the word "EADM".

Firmware Version Compatibility

The firmware download is possible with a latest firmware version or a previous firmware version.

NOTE: The firmware in the module must be of the same version (or later) as the one declared in the Control Expert project configuration. Otherwise, one of the two adapter stays out of service, and if this X80 drop is reset both adapter modules will stay out of service. Adapter modules in this state can further be updated from EADM. You can diagnose a firmware mismatch with the LED status.

Firmware mismatch occurs when two devices on the same drop do not align with the expected or required version. Firmware incompatibility is a specific type of firmware mismatch where two devices are using different firmware versions that cannot work together, potentially impacting system redundancy.

NOTE: If the FW_COMPATIBILITY_ERROR bit is 1, ensure that all devices physically present on that drop are in service before performing the update of the adapter module with the MASTER role.

Download Procedure

Prerequisite:

- EADM is installed on the configuration PC you use to perform the firmware update.
- The BMECRA31310(H) adapter module is installed on a Modicon X80 rack and energized.

Do not interrupt the firmware download process by:

- Allowing an interruption to the power or communications.
- Closing the firmware update tool software.

If the firmware download process is interrupted, the new firmware is not installed and the module continues to use the previous firmware. If an interruption occurs, restart the process.

NOTE: If the download is not completed, there is a message saying that the update was unsuccessful.

Updating the Firmware in Single Mode

To update the firmware of the BMECRA31310(H) adapter module in single mode (there is one adapter module per drop):

Step	Action
1	Connect the configuration PC to the BMECRA31310(H) adapter module through service port or Ethernet ports. **NOTE:** The device discovery feature of the firmware update tool (EADM) is not available with BMECRA31310(H) adapter modules.
2	Start EcoStruxure™ Automation Device Maintenance software.
3	Select the adapter module in the device list, and add the device from the catalog and assign the IP address. **NOTE:** The adapter module receives its IP address from the controller at startup. If the controller is not configured or the firmware version of the adapter module is not compatible, the adapter module does not receive an IP address. Power cycle the adapter module and connect it through its service port to EADM using the IP address: 10.10.mac5.mac6.
4	Login by entering the credentials in the **Device login** dialog box. **Device User Name** is *loader* and the **Device password** is the firmware password set in Control Expert project.
5	Select the targeted firmware package and launch the download (**Update Firmware** button from EADM main window). **NOTE:** You may have to click the **trust** icon once if it is the first time you select the firmware package. If you perform any operations such as CCOTF, Hot Swap, Load New Application or manual controller changeover (Hot Standby Switchover) while the firmware update is in progress, these actions might force some I/O modules to re-initialize during the firmware update. **⚠WARNING** **UNINTENDED EQUIPMENT OPERATION** Do not to perform Configuration Change On The Fly (CCOTF), Hot Swap, Load New Application or manual controller changeover (Hot Standby Switchover) while the firmware update is in progress. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**
6	After the transfer is completed, close the EcoStruxure™ Automation Device Maintenance software tool.

NOTE: For a detailed description of the download procedure, refer to the EcoStruxure™ Automation Device Maintenance online help.

Updating the Firmware in Redundant Mode

To update the firmware of the BMECRA31310(H) adapter module in redundant mode (there are two adapter modules per drop):

Step	Action
1	Connect the configuration PC to the BMECRA31310(H) adapter module with the *NOT MASTER* role through any service port (including the controller port). **NOTE:** The device discovery feature of the firmware update tool (EADM) is not available with BMECRA31310(H) adapter modules.
2	Start EcoStruxure™ Automation Device Maintenance software.
3	Select the adapter module in the device list, and add the device from the catalog and assign the IP address. **NOTE:** The adapter module receives its IP address from the controller at startup. If the controller is not configured or the firmware version of the adapter module is not compatible, the adapter module does not receive an IP address. Power cycle the adapter module and connect it through its service port to EADM using the IP address: 10.10.mac5.mac6.
4	Login by entering the credentials in the **Device login** dialog box. **Device User Name** is *loader* and the **Device password** is the firmware password set in Control Expert project.

Step	Action
5	Select the targeted firmware package and launch the download (**Update Firmware** button from EADM main window). **NOTE:** You may have to click the **trust** icon once if it is the first time you select the firmware package. If you perform any operations such as CCOTF, Hot Swap, Load New Application or manual controller changeover (Hot Standby Switchover) while the firmware update is in progress, these actions might force some I/O modules to re-initialize during the firmware update. **⚠WARNING** **UNINTENDED EQUIPMENT OPERATION** Do not to perform Configuration Change On The Fly (CCOTF), Hot Swap, Load New Application or manual controller changeover (Hot Standby Switchover) while the firmware update is in progress. **Failure to follow these instructions can result in death, serious injury, or equipment damage.**
6	After the firmware update is completed and the BMECRA3110(H) adapter module with *NOT MASTER* role has rebooted, verify in Control Expert the status of the FW_MISMATCH and FW_COMPATIBILITY_ERROR bits within the CRA_DIAGNOSTIC word. **NOTE:** If the FW_COMPATIBILITY_ERROR bit is 1, ensure that all devices physically present on that drop are in service before performing the update of the adapter module with the *MASTER* role.
7	Repeat steps 1 to 5 for the adapter module with the *MASTER* role. **NOTE:** During the firmware update, the master role is transferred to the redundant BMECRA31310(H), which has the *NOT MASTER* role, so that I/Os continue to be controlled.

NOTE: For a detailed description of the download procedure, refer to the EcoStruxure™ Automation Device Maintenance online help.

Adapter Module Replacement

Overview

At any time and without turning off the power to the rack, a BMECRA31310(H) adapter module can be replaced by another BMECRA31310(H) adapter module with compatible firmware.

⚠⚠DANGER

EXPLOSION OR ELECTRIC SHOCK

- Only perform a hot swap operation in locations known and confirmed to be non-hazardous
- Use only your hands and suitable insulation equipment.
- Do not use metal tools.

Failure to follow these instructions will result in death or serious injury.

With FDR client functionality, the BMECRA31310(H) adapter module subscribes to the controller FDR service and obtains its operating parameters over Ethernet.

NOTE: You have to understand and plan for the consequences of hot-swapping a module.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Thoroughly identify and understand all implications and consequences of operating mode modifications before performing them.
- Take all necessary preventive measures before making operating mode modifications.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Single Mode Behavior

Disconnecting an adapter module in single mode interrupts communication to the devices located in the drop.

When the adapter module is removed, the I/O values go to fallback values. When the new adapter module is inserted, switched on and configured, the I/O values reset to their values before the hot swap.

To reduce the number of transitions after a hot swap, set the configured fallback state the same as the default fallback state (module powered-on but not configured) before performing the hot swap.

Redundant Mode Behavior

In normal operation, disconnecting an adapter module in redundant mode do not interrupt communication to the devices located on the drop. Hot swapping the adapter module with the *MASTER* role is similar to a switchover.

For detailed information on execution time and effect of a switchover on devices located on the drop, refer to the chapter Adapter Redundancy Operation, page 107.

Hot Swapping Procedure

⚠WARNING

ELECTRIC SHOCK

Positively confirm that the backplane is connected to the protective earth ground and that there is an equipotential grounding system in place before hot swapping a BMECRA31310 or BMECRA31310H module.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

To hot-swap a BMECRA31310(H) module, follow these steps:

Step	Action
1	Remove the Ethernet cable from the module.
2	Remove the module from the backplane.
3	Install the new module to the free slot of backplane. Tighten the retaining screw to hold the module in place on the rack: **NOTE:** The tightening torque is 0.4...1.5 N•m (0.30...1.10 lbf-ft).
4	Reconnect the PRP Ethernet network cables to the Redundant Device Network connector of the new module.

An incorrect module connection can lead to an unintended behavior of the system.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

Verify that the mounting screw is securely tightened to ensure the module is firmly attached to the rack.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Appendices

What's in This Part

Modbus Function Code 3 — Read Holding Register

What's in This Chapter

Overview

Modbus function code 3 provides access to a variety of diagnostic functions, including basic network diagnostics, Ethernet port diagnostics, and Modbus port 502 diagnostics.

To access the function code 3 diagnostics from the local device, set the **unit ID** to 100.

Type	Offset Modbus Address (starting address)	Size (Words)
Basic Networks Diagnostic Data	40001	39
Ethernet Port Diagnostics Data (**Internal port**)	40040	103
Ethernet Port Diagnostics Data (**Service port - ETH1**)	40143	103
Ethernet Port Diagnostics Data (**PRP LAN A - ETH 2**)	40246	103
Ethernet Port Diagnostics Data (**PRP LAN B - ETH 3**)	40349	103
Ethernet Port Diagnostics Data (**Backplane port**)	40452	103
Modbus TCP/Port 502 Diagnostic Data	40555	114
Modbus TCP/Port 502 Connection Table Data	40669	515
NTPv4 Diagnostics	41218	42
QoS Diagnostics	41275	11
Identify	42001	24

Here is an example of how to read registers 40018 and 40019, the *Ethernet receive frames OK* count registers. The request contains 7 bytes. The starting address, shown as a hex value in byte 2 below, is calculated as follows:

40018 – 40001 = 17 dec = (11 hex)

The number of registers to be diagnosed (2 hex) is shown in byte 4:

Byte Number	Value
0	Function code = 03 (hex)
1	Starting Address Hi = 00 (hex)
2	Starting Address Low = 11 (hex)
3	No. of Registers Hi = 00 (hex)
4	No. of Registers Low = 2 (hex)
5	CRC high byte (inserted by the Modbus sending application)
6	CRC low byte (inserted by the Modbus sending application)

The normal response is returned in 8 bytes. In this example, the expected response is 14229 hex; this value is shown in bytes 2 through 5 of the response:

Byte Number	Value
0	Function code = 03 (hex)
1	Byte count = 4 (hex)
2	1st register data, high byte = 00 (hex)
3	1st register data, low byte = 01 (01 hex)
4	2nd register data, high byte = 42 (hex)
5	2nd register data, low byte = 29 (hex)
6	CRC high byte
7	CRC low byte

Byte Number	Value
0	Original function code + 80 hex (= 83 hex)
1	Detected error code
2	CRC high byte
3	CRC low byte

For more information on Modbus function code 3 and other function codes, refer to the *Modicon Modbus Protocol Reference Guide* (PI-MBUS-300).

Basic Network Diagnostics Data

Modbus Registers Mapping

The format of basic network diagnostics data provided by the device is as follows:

Address	Length (Words)	Register Byte Order		Description
		MS BYTE	LS BYTE	
offset	2	MS Byte 00	Byte 01	Basic network diagnostic validity, page 154
		Byte 02	LS Byte	
offset + 2	1	MS Byte	LS Byte 03	**CGS**, page 154
offset + 3	1	MS Byte	LS Byte	**CS**, page 154
offset + 4	1	MS Byte	LS Byte	**CSS**, page 155
offset + 5	2	IP 1	IP 2	IP address (**IP**)
		IP 3	IP 4	Format: IP1.IP2.IP3.IP4
offset + 7	2	SM 1	SM 2	Subnet mask (**SM**)
		SM 3	SM 4	Format: SM1.SM2.SM3.SM4
offset + 9	2	GW 1	GW 2	Default gateway (**GIP**)
		GW 3	GW 4	Format : GW1.GW2.GW3.GW4
offset + 11	3	MAC 1	MAC 2	MAC address (**MAC**)
		MAC 3	MAC 4	Format: MAC1:MAC2:MAC3:MAC4:MAC5:MAC6
		MAC 5	MAC 6	
offset + 14	3	MS Byte 00	01	**EFF**, page 155
		02	03	
		04	LS Byte 05	
offset + 17	2	C00	C01	Ethernet receive frames OK (**ER**)
		C02	C03	
offset + 19	2	C00	C01	Ethernet transmit frames OK (**EX**)
		C02	C03	
offset + 21	1	MS Byte	LS Byte	Number of open client connections (**NOC**)
offset + 22	1	MS Byte	LS Byte	Number of open server connections (**NOS**)
offset + 23	2	C00	C01	Number of Modbus detected error messages sent (**MBE**)
		C02	C03	
offset + 25	2	C00	C01	Number of Modbus messages sent (**MBS**)
		C02	C03	
offset + 27	2	C00	C01	Number of Modbus messages received (**MBR**)
		C02	C03	
offset + 29	8			Device name: One byte per character (**FDN**)
offset + 37	2	MS Byte 00	Byte 01	**IAO**, page 155
		Byte 02	LS Byte 03	

Basic Network Diagnostic Validity: Detail

The Basic Network Diagnostic Validity fields indicate which fields in the Basic Network Diagnostic Data structure are valid:

Bit	Field	Description
31	Field Extended (FE)	0 = Not extended
30 - 18	Reserved	0
17	Communication Global Status (CGS)	0 = Not valid, 1 = Valid
16	Supported Communication Services (CS)	0 = Not valid, 1 = Valid
15	Field Extended (FE)	1 = Extended
14	Status of Communication Services (CSS)	0 = Not valid, 1 = Valid
13	IP Address (IP)	0 = Not valid, 1 = Valid
12	Subnet Mask (SM)	0 = Not valid, 1 = Valid
11	Default Gateway (GIP)	0 = Not valid, 1 = Valid
10	MAC Address (MAC)	0 = Not valid, 1 = Valid
9	Ether Frame Format Capability / Configuration / Operational (EFF)	0 = Not valid, 1 = Valid
8	Ether Rcv Frames OK (ER)	0 = Not valid, 1 = Valid
7	Ether Xmit Frames OK (EX)	0 = Not valid, 1 = Valid
6	Num MB Open Client Connections (NOC)	0 = Not valid, 1 = Valid
5	Num MB Open Server Connections (NOS)	0 = Not valid, 1 = Valid
4	Num MB Error Msgs Sent (MBE)	0 = Not valid, 1 = Valid
3	Num MB Msgs Sent (MBS)	0 = Not valid, 1 = Valid
2	Num MB Msgs Rcvd (MBR)	0 = Not valid, 1 = Valid
1	Device Name (FDN)	0 = Not valid, 1 = Valid
0	IP Assignment Mode Capability / Operational (IAO)	0 = Not valid, 1 = Valid

Communication Global Status (CGS): Detail

Bit	Field	Description
15 - 2	Reserved	0
1 - 0	Global Status (GS)	0 = Reserved, 1 = Not ok, 2 = ok, 3 = Reserved

Supported Communication Services (CS): Detail

Bit	Field	Description
15 - 1	Reserved	0
0	Port502Messaging (502)	0 = Not supported, 1 = Supported

Status of communication Services (CSS): Detail

Bit	Field	Description
15 - 3	Reserved	0
2 - 0	Port502Messaging (502)	1= IDLE, 2 = Operational

Ethernet Frame Format Capacity / Configuration / Operational (EFF): Detail

Bit	Field	Description
47 - 36	Reserved	0
35	Auto-detection capacity (ADC)	1= IDLE, 2 = Operational
34	802.3 Framing sender capacity (8SC)	0 = Not supported, 1 = supported
33	802.3 Framing receiver capacity (8RC)	0 = Not supported, 1 = supported
32	Ethernet II Framing capacity (E2C)	Always supported = 1
31 - 20	Reserved	0
19	Auto-detection configured (ADG)	0 = Not supported, 1 = supported
18	802.3 framing sender configured (8SG)	0 = Not supported, 1 = supported
17	802.3 frmaing receiver configured (8RG)	0 = Not supported, 1 = supported
16	Ethernet II framing configured (E2G)	Always configured = 1
15 - 4	Reserved	0
3	Auto detection operation (ADO)	0 = Not supported, 1 = supported
2	802.3 framing sender operation (8SO)	0 = Not supported, 1 = supported
1	802.3 framing receiver operation (8RO)	0 = Not supported, 1 = supported
0	Ethernet II framing operation (E2O)	0 = Not supported, 1 = supported

IP Assignment Mode Capacity / Operational (IAO): Detail

Bit	Field	Description
31 - 20	Reserved	0
19 - 16	IP Assignment Capacity	Values: 0 = Not available, 1 = available Available mode: Bit 16: SERVEDBYNAME Bit 17: SERVEDBYMAC using BOOTP Bit 18: SERVEDBYMAC using DHCP Bit 19: STORED assignment
15 - 4	Reserved	0
3 - 0	IP Assignment Mode Operational	Values: 0 = Not available, 1 = available Available mode: Bit 16: SERVEDBYNAME Bit 17: SERVEDBYMAC using BOOTP Bit 18: SERVEDBYMAC using DHCP Bit 19: STORED assignment

Ethernet Port Diagnostic Data

Modbus Registers Mapping

NOTE: There is as many contiguous Modbus registers as there are Ethernet ports on the device.

The format of an Ethernet port diagnostic data provided by the device is as follows:

Address	Length (Words)	Register Byte Order		Description
		MS BYTE	LS BYTE	
offset	1	MS Byte	LS Byte	Port Diagnostics Data Validity, page 159
offset + 1	1	MS Byte	LS Byte	Logical/Physical Port Number (**PN**) MS Byte = Logical port number LS Byte = Physical port number
offset + 2	1	MS Byte	LS Byte	Ethernet Control Capability (**ECC**), page 159
offset + 3	1	MS Byte	LS Byte	Internal port Link Speed Capability (**LSAC**) values (example): 100 = 10 Mbps, 1000 = 1 Gbps
offset + 4	1	MS Byte	LS Byte	Ethernet Control Configuration (**ECG**), page 159
offset + 5	1	MS Byte	LS Byte	Link Speed Configuration (**LSC**). Values (example) : 10 = 10 Mbps, 1000 = 1 Gbps
offset + 6	1	MS Byte	LS Byte	Ethernet Control Operational (**ECO**), page 160
offset + 7	1	MS Byte	LS Byte	Link Speed Operational (**LSO**) values (example): 10 = 10 Mbps, 1000 = 1 Gbps
offset + 8	3	MAC 1	MAC 2	Port MAC Address (**PMA**) Format: MAC1:MAC2:MAC3:MAC4:MAC5:MAC6
		MAC 3	MAC 4	
		MAC 5	MAC 6	
offset + 11	2	MSB C00	C01	Media Counters Data Validity, page 160
		C02	LSB C03	
offset + 13	2	MSB C00	C01	Num Frames Transmitted OK
		C02	LSB C03	
offset + 15	2	MSB C00	C01	Num Frames Received OK
		C02	LSB C03	
offset + 17	2	MSB C00	C01	Num Ether Collisions
		C02	LSB C03	
offset + 19	2	MSB C00	C01	Carrier Sense Errors detected
		C02	LSB C03	
offset + 21	2	MSB C00	C01	Num Ether Excessive Collisions
		C02	LSB C03	
offset + 23	2	MSB C00	C01	CRC Errors detected
		C02	LSB C03	
offset + 25	2	MSB C00	C01	FCS Errors detected
		C02	LSB C03	
offset + 27	2	MSB C00	C01	Alignment Errors detected
		C02	LSB C03	

Address	Length (Words)	Register Byte Order		Description
		MS BYTE	LS BYTE	
offset + 29	2	MSB C00	C01	Num Internal MAC Tx Errors detected
		C02	LSB C03	
offset + 31	2	MSB C00	C01	Late Collisions
		C02	LSB C03	
offset + 33	2	MSB C00	C01	Num Internal MAC Rx Errors detected
		C02	LSB C03	
offset + 35	2	MSB C00	C01	Multiple Collisions
		C02	LSB C03	
offset + 37	2	MSB C00	C01	Single Collisions
		C02	LSB C03	
offset + 39	2	MSB C00	C01	Deferred Transmissions
		C02	LSB C03	
offset + 41	2	MSB C00	C01	Frames Too Long
		C02	LSB C03	
offset + 43	2	MSB C00	C01	Frames Too Short
		C02	LSB C03	
offset + 45	2	MSB C00	C01	SQE Test Error detected
		C02	LSB C03	
offset + 47	1	MS Byte	LS Byte	Interface Label Length
offset + 48	32	IL char64	IL char63	Interface Label characters
		...	...	
		IL char02	IL char01	
offset + 80	1	MS Byte	LS Byte	Interface Counters Diagnostic Validity, page 161
offset + 81	2	MSB C00	C01	Num Octets Received
		C02	LSB C03	
offset + 83	2	MSB C00	C01	Num Unicast Packets Received
		C02	LSB C03	
offset + 85	2	MSB C00	C01	Num Non Unicast Packets Received
		C02	LSB C03	
offset + 87	2	MSB C00	C01	Num Inbound Packets Discarded
		C02	LSB C03	
offset + 89	2	MSB C00	C01	Num Inbound Packets Error detected
		C02	LSB C03	
offset + 91	2	MSB C00	C01	Num Inbound Packets Unknown
		C02	LSB C03	
offset + 93	2	MSB C00	C01	Num Octets Sent
		C02	LSB C03	
offset + 95	2	MSB C00	C01	Num Unicast Packets Sent
		C02	LSB C03	
offset + 97	2	MSB C00	C01	Num Non Unicast Packets Sent
		C02	LSB C03	
offset + 99	2	MSB C00	C01	Num Outbound Packets Discarded
		C02	LSB C03	

Address	Length (Words)	Register Byte Order		Description
		MS BYTE	LS BYTE	
offset + 101	2	MSB C00	C01	Num Outbound Packets Error detected
		C02	LSB C03	

Diagnostics Data Validity: Detail

Bit	Field	Description
15	Field Extended (FE)	0 = Not extended
14 - 11	Reserved	0
10	Logical/Physical Port Number (PN)	0 = Not valid, 1 = Valid
9	Ethernet Control Capability (ECC)	0 = Not valid, 1 = Valid
8	Link Speed Capability (LSAC)	0 = Not valid, 1 = Valid
7	Ethernet Control Configuration (ECG)	0 = Not valid, 1 = Valid
6	Link Speed Configuration (LSC)	0 = Not valid, 1 = Valid
5	Ethernet Control Operational (ECO)	0 = Not valid, 1 = Valid
4	Link Speed Operational (LSO)	0 = Not valid, 1 = Valid
3	Port MAC Address (PMA)	0 = Not valid, 1 = Valid
2	Media Counters (MC)	0 = Not valid, 1 = Valid
1	Interface Label (IL)	0 = Not valid, 1 = Valid
0	Interface Counters (IC)	0 = Not valid, 1 = Valid

Ethernet Control Capability (ECC): Detail

Bit	Field	Description
15 - 14	Reserved	0
13	Link	0 = Not supported, 1 = Supported
12 - 5	Reserved	0
4 - 3	Duplex (DP)	0 = None, 01 = Half-Duplex, 10 = Full-Duplex, 11 = Auto-Negociate
2	Reserved	0
1	Fiber Media Supported	0 = Not supported, 1 = Supported
0	Twisted pair Supported	0 = Not supported, 1 = Supported

Ethernet Control Configuration (ECG): Detail

Bit	Field	Description
15 - 14	Reserved	0
13	Link	0 = Link down, 1 = Link up
12 - 5	Reserved	0
4 - 3	Duplex (DP)	00 = None, 01 = Half-Duplex, 10 = Full-Duplex, 11 = Auto-Negociate
2	Reserved	0

Bit	Field	Description
1	Fiber Media Supported	0 = Disabled, 1 = Enabled
0	Twisted pair Supported	0 = Disabled, 1 = Enabled

Ethernet Control Operational (ECO): Detail

Bit	Field	Description
15 - 14	Reserved	0
13	Link	0 = Link down, 1 = Link up
12 - 5	Reserved	0
4 - 3	Duplex (DP)	00 = None, 01 = Half-Duplex, 10 = Full-Duplex, 11 = Auto-Negociate
2	Reserved	0
1	Fiber Media Supported	0 = Not operational, 1 = Operational
0	Twisted pair Supported	0 = Not operational, 1 = Operational

Media Counters Data Validity: Detail

Bit	Field	Description
31	Field Extended (FE)	0 = Not extended
30 - 18	Reserved	0
17	Num Frames Xmit OK (FX)	0 = Not valid, 1 = Valid
16	Num Frames Recv OK (FR)	0 = Not valid, 1 = Valid
15	Field Extended (FE)	0 = Not extended, 1 = Extended
14	Num Ether Collisions (EC)	0 = Not valid, 1 = Valid
13	Carrier Sense Errors (CSE)	0 = Not valid, 1 = Valid
12	Num Ether Excessive Collisions (EEC)	0 = Not valid, 1 = Valid
11	CRC Errors (CRE)	0 = Not valid, 1 = Valid
10	FCS Errors (FCS)	0 = Not valid, 1 = Valid
9	Alignment Errors (ALE)	0 = Not valid, 1 = Valid
8	Num Internal MAC Tx Errors (XM)	0 = Not valid, 1 = Valid
7	Late Collisions (LC)	0 = Not valid, 1 = Valid
6	Num Ether Receive MAC Errors (RM)	0 = Not valid, 1 = Valid
5	Multiple Collisions (MC)	0 = Not valid, 1 = Valid
4	Single Collisions (SC)	0 = Not valid, 1 = Valid
3	Deferred Transmissions (DT)	0 = Not valid, 1 = Valid
2	Frames Too Long (F2L)	0 = Not valid, 1 = Valid
1	Frames Too Short (Runt packets) (RP)	0 = Not valid, 1 = Valid
0	SQE Test Error (SQE)	0 = Not valid, 1 = Valid

Interface Counters Diagnostic Validity: Detail

Bit	Field	Description
15	Field Extended (FE)	0 = Not extended
14 - 11	Reserved	0
10	Num Octets Received (OR)	0 = Not valid, 1 = Valid
9	Num Unicast Packets Received (UR)	0 = Not valid, 1 = Valid
8	Num Non Unicast Packets Received (NUR)	0 = Not valid, 1 = Valid
7	Num Inbound Packets Discard (ID)	0 = Not valid, 1 = Valid
6	Num Inbound Packets Error (IE)	0 = Not valid, 1 = Valid
5	Num Inbound Packets Unknown (IU)	0 = Not valid, 1 = Valid
4	Num Octets Sent (OS)	0 = Not valid, 1 = Valid
3	Num Unicast Packets Sent (US)	0 = Not valid, 1 = Valid
2	Num Non Unicast Packets Sent (NUS)	0 = Not valid, 1 = Valid
1	Num Outbound Packets Discard (OD)	0 = Not valid, 1 = Valid
0	Num Outbound Packets Error (OE)	0 = Not valid, 1 = Valid

Modbus TCP Port 502 Diagnostics Data

Modbus Regiters Mapping

The format of Modbus TCP Port 502 diagnostics data provided by the device is as follows:

Address	Length (Words)	Register Byte Order		Description
		MS BYTE	LS BYTE	
offset	2	MS Byte 00	Byte 01	Modbus TCP/Port 502 Diagnostic Data Validity, page 162
		Byte 02	LS Byte 03	
offset + 2	1	MS Byte	LS Byte	Port 502 Status (**502**)
offset + 3	1	MS Byte	LS Byte	Num Open Connections (**OC**)
offset + 4	2	MSB C00	C01	Num MB Messages Sent (**MBS**)
		C02	LSB C03	
offset + 6	2	MSB C00	C01	Num MB Messages Received (**MBR**)
		C02	LSB C03	
offset + 8	1	MS Byte	LS Byte	Num MB Open Client Connections (**OCC**)
offset + 9	1	MS Byte	LS Byte	Num MB Open Server Connections (**OSC**)
offset + 10	1	MS Byte	LS Byte	Max Num Connections (**MNC**)
offset + 11	1	MS Byte	LS Byte	Max Num Client Connections (**MCC**)
offset + 12	1	MS Byte	LS Byte	Max Num Server Connections (**MSC**)
offset + 13	2	MSB C00	C01	Num MB Detected Error Messages Sent (**MBE**)
		C02	LSB C03	
offset + 15	1	MS Byte	LS Byte	Num Open Priority Connections (**OPC**)
offset + 16	1	MS Byte	LS Byte	Max Num Priority Connections (**MPC**)
offset + 17	1	MS Byte	LS Byte	Num Entries in Unauthorized Table (**NUT**)
offset + 18	2	MSB - IP1	IP2	**Connection 1**: Remote IP Address
		IP3	LSB - IP4	
offset + 20	1	MS Byte	LS Byte	**Connection 1**: Num Attempts to Open Unauthorized
...	...	...	...	...
offset + 39	2	MSB - IP1	IP2	**Connection 8**: Remote IP Address
		IP3	LSB - IP4	
offset + 41	1	MS Byte	LS Byte	**Connection 8**: Num Attempts to Open Unauthorized

Modbus TCP/Port 502 Diagnostic Data Validity: Detail

Bit	Field	Description
15	Field Extended (FE)	0 = Not extended
14 - 13	Reserved	0
12	Port 502 Status (502)	0 = Not valid, 1 = Valid
11	Num MB Open Connections (OC)	0 = Not valid, 1 = Valid
10	Num MB Msgs Sent (MBS)	0 = Not valid, 1 = Valid

Bit	Field	Description
9	Num MB Msgs Rcvd (MBR)	0 = Not valid, 1 = Valid
8	Num MB Open Client Connections (OCC)	0 = Not valid, 1 = Valid
7	Num MB Open Server Connections (OSC)	0 = Not valid, 1 = Valid
6	Max Num Connections (MNC)	0 = Not valid, 1 = Valid
5	Max Num Client Connections (MCC)	0 = Not valid, 1 = Valid
4	Max Num Server Connections (MSC)	0 = Not valid, 1 = Valid
3	Num MB Error Messages Sent (MBE)	0 = Not valid, 1 = Valid
2	Num Open Priority Connections (OPC)	0 = Not valid, 1 = Valid
1	Max Num Priority Connections (MPC)	0 = Not valid, 1 = Valid
0	Num Attempts to Open Unauthorized TCP Connections (NUT)	0 = Not valid, 1 = Valid

Modbus TCP Port 502 Connection Table Data

Modbus Registers Mapping

The format of Modbus TCP port 502 connection table provided by the device is as follows:

Address	Length (Words)	Register Byte Order		Description
		MS BYTE	LS BYTE	
offset	1	MS Byte	LS Byte	Connection Table Validity, page 164
offset + 1	1	MS Byte	LS Byte	Number of Entries (**NE**)
offset + 2	1	MS Byte	LS Byte	Starting Entry Index (**SE**)
offset + 3	1	MS Byte	LS Byte	Connection 1: Index
offset + 4	2	IP1	IP2	Connection 1: Remote IP Address
		IP3	IP4	
offset + 6	1	MS Byte	LS Byte	Connection 1 : Remote Port Number
offset + 7	1	MS Byte	LS Byte	Connection 1: Local Port Number
offset + 8	1	MS Byte	LS Byte	Num MB Messages Sent on connection 1
offset + 9	1	MS Byte	LS Byte	Num MB Messages Received on connection 1
offset + 10	1	MS Byte	LS Byte	Num MB Detected Error Messages Sent on connection 1
...	...	...	...	...
offset + 59	1	MS Byte	LS Byte	Connection 8: Index
offset + 60	2	IP1	IP2	Connection 8: Remote IP Address
		IP3	IP4	
offset + 62	1	MS Byte	LS Byte	Connection 8: Remote Port Number
offset + 63	1	MS Byte	LS Byte	Connection 8: Local Port Number
offset + 64	1	MS Byte	LS Byte	Num MB Messages Sent on connection 8
offset + 65	1	MS Byte	LS Byte	Num MB Messages Received on connection 8
offset + 66	1	MS Byte	LS Byte	Num MB Detected Error Messages Sent on connection 8

Modbus TCP/Port 502 Connection Table Validity: Detail

Bit	Field	Description
15	Field Extended (FE)	0 = Not extended
14 - 3	Reserved	0
2	Number of Entries (NE)	0 = Not valid, 1 = Valid
1	Starting Entry Index (SE)	0 = Not valid, 1 = Valid
0	Connections Table Entries (CTE)	0 = Not valid, 1 = Valid

NTPv4 Diagnostic Data

Modbus Register Mapping

The format of the NTPv4 diagnostic data provided by the device is as follows:

Address	Length (Words)	Register Byte Order		Description
		MS Byte	LS Byte	
offset	2	MSW - MSB	MSW - LSB	Enabled/disabled
		LSW - MSB	LSW - LSB	
offset + 2	2	MSW - MSB	MSW - LSB	Primary NTP Server IP Address
		LSW - MSB	LSW - LSB	
offset + 4	2	MSW - MSB	MSW - LSB	Secondary NTP Server IP Address
		LSW - MSB	LSW - LSB	
offset + 6	1	Unused	LS Byte	Polling Period
offset + 7	1	Unused	LS Byte	Daylight Saving Auto Adjustment
offset + 8	1	Unused	LS Byte	Update controller with Module Time
offset + 9	1	Unused	LS Byte	Reserved
offset + 10	2	MSW - MSB	MSW - LSB	Time Zone
		LSW - MSB	LSW - LSB	
offset + 12	1	MS Byte	LS Byte	Time Zone Offset
offset + 13	1	Unused	Unused	Reserved
offset + 14	1	Unused	Unused	Reserved
offset + 15	1	Unused	LS Byte	Daylight Saving Start Date - Month
offset + 16	1	Unused	LS Byte	Daylight Saving Start Date - week # day of week
offset + 17	1	Unused	LS Byte	Daylight Saving End Date - Month
offset + 18	1	Unused	LS Byte	Daylight Saving End Date - week # day of week
offset + 19	1	MSW - MSB	MSW - LSB	Network Time Service Status
offset + 20	1	LSW - MSB	LSW - LSB	
offset + 21	2	MSW - MSB	MSW - LSB	Link to NTP Server Status
		LSW - MSB	LSW - LSB	
offset + 23	2	MSW - MSB	MSW - LSB	NTP Server IP Address
		LSW - MSB	LSW - LSB	
offset + 25	2	MSW - MSB	MSW - LSB	NTP Server Type
		LSW - MSB	LSW - LSB	
offset + 27	2	MSW - MSB	MSW - LSB	NTP Server Time Quality
		LSW - MSB	LSW - LSB	
offset + 29	2	MSW - MSB	MSW - LSB	Number of NTP Requests Sent
		LSW - MSB	LSW - LSB	
offset + 31	2	MSW - MSB	MSW - LSB	Number of Communication Errors
		LSW - MSB	LSW - LSB	
offset + 33	2	MSW - MSB	MSW - LSB	Number of NTP Reponses Received
		LSW - MSB	LSW - LSB	
offset + 35	1	MS Byte	LS Byte	Last Error

Address	Length (Words)	Register Byte Order		Description
		MS Byte	LS Byte	
offset + 36	2	MSW - MSB	MSW - LSB	Present Time
		LSW - MSB	LSW - LSB	
offset + 38	1	MS Byte	LS Byte	Present Date
offset + 39	2	MSW - MSB	MSW - LSB	Daylight Saving Status
		LSW - MSB	LSW - LSB	
offset + 41	2	MSW - MSB	MSW - LSB	Time Since Last Update
		LSW - MSB	LSW - LSB	

QoS Diagnostics Data

Modbus Register Mapping

The format of the QoS diagnostic data provided by the device is as follows:

Address	Length (Words)	Register Byte Order		Description
		MS Byte	LS Byte	
offset	1	MS Byte	LS Byte	802.1Q Tag enable / disable
offset + 1	1	MS Byte	LS Byte	DSCP PTP Event
offset + 2	1	MS Byte	LS Byte	DSCP PTP General
offset + 3	1	MS Byte	LS Byte	DSCP EIP Urgent
offset + 4	1	MS Byte	LS Byte	DSCP EIP Scheduled
offset + 5	1	MS Byte	LS Byte	DSCP EIP High
offset + 6	1	MS Byte	LS Byte	DSCP EIP Low
offset + 7	1	MS Byte	LS Byte	DSCP EIP Explicit
offset + 8	1	MS Byte	LS Byte	DSCP Modbus IO Scanner (same as DSCP EIP High)
offset + 9	1	MS Byte	LS Byte	DSCP Modbus Client/Server (same EIP Explicit)
offset + 10	1	MS Byte	LS Byte	DSCP NTPv4

Identity Data

Modbus Registers Mapping

The format of identity data provided by the device is as follows:

Address	Length (Words)	Register Byte Order		Description
		MS BYTE	LS BYTE	
offset	1	MS Byte	LS Byte	Vendor ID Value = 0xF3 (Schneider Electric)
offset + 1	1	MS Byte	LS Byte	Device type Value = 0x0C (Communication adapter device)
offset + 2	1	MS Byte	LS Byte	Product code
offset + 3	1	Unused	LS Byte	Revision - Major revision
offset + 4	1	Unused	LS Byte	Revision - Minor revision
offset + 5	1	MS Byte	LS Byte	Status of the device
offset + 6	2	SN 1	SN 2	Serial number of the device
		SN 3	SN 4	
offset + 8	1	Unused	LS Byte	Length of the product name Value = 0x0B (11 dec)
offset + 9	16	-	-	Device name: One byte per character. Value = BMECRA31310

Modbus Function Code 8 — Get/Clear Ethernet Statistics

What's in This Chapter

Modbus Request Format

You can get or clear a variety of diagnostic data using the function code 8, and subcode 22 in a Modbus request.

The Modbus request format is as follows:

Definition	Number of Bytes	Value
Device Modbus Server number	1 byte	FF hex
Function code	2 bytes	08 (08 hex)
Sub-function code	2 bytes	22 (0016 hex)
Operation code	2 bytes	Example: 0001 hex to read diagnostic data. See below list for operation code values.
Diagnostic control	2 bytes	Example: 0102 hex to read Ethernet port ETH1 diagnostic data. See below list for diagnostic control values.
Starting entry index	1 byte	00 (0 to 255)

The operation code field is used to select the diagnostic and the statistic data to be read from the adapter module:

Bit	Field	Description
15...12	Reserved	Must be zero
11...8	Protocol Version (PV)	Indicates version of the protocol of the client (requestor) Values are: 00 hex (initial version)
7...0	Operation Code	Indicates function to be performed by the command. Values are: • 01 hex = Read diagnostic data • 02 hex = Clear diagnostic data • 03 hex = Clear all diagnostic data • 04 hex = List ports

The diagnostic control field provides the data selection information for this protocol as well as specifies the logical port from which, the data is to be retrieved (if applicable). The diagnostic control field is defined as shown in the following table:

<table>
<tr><th>Bit</th><th>Field</th><th>Description</th></tr>
<tr><td>15...8</td><td>Data Selection Code (DS)</td><td>Indicates the diagnostic data to retrieve or to clear from the logical port.
<table>
<tr><th>Data Selection Code</th><th>Diagnostic Data Retrieved</th><th>Port Select Needed</th></tr>
<tr><td>01 hex</td><td>Basic network diagnostics</td><td>No</td></tr>
<tr><td>02 hex</td><td>Ethernet port diagnostics</td><td>Yes</td></tr>
<tr><td>03 hex</td><td>Modbus TCP port 502 diagnostics</td><td>No</td></tr>
<tr><td>04 hex</td><td>Modbus TCP port 502 connection table</td><td>No</td></tr>
<tr><td>7F hex</td><td>Data structure offsets</td><td>No</td></tr>
</table></td></tr>
<tr><td>7...0</td><td>Port Select (PS)</td><td>Indicates the logical port number to retrieve the selected data when Data Selection Code requires a valid port select value.
• 00 hex = the internal port of the adapter.
• 01 hex to 04 hex = logical number of the desired port.
• FF hex = the port the request came in.
NOTE: This value should be FF hex if the requested data is not port specific.</td></tr>
</table>

Modbus Function Code 43 — Read Device Identification

What's in This Chapter

Modbus Request Format

You can get basic device identification data using the function code 43 and subcode 14 in a Modbus request.

Modbus request format:

Definition	Number of Bytes	Value
Device Modbus Server number	1 byte	FF hex
Function code	1byte	43 (2B hex)
Sub-function code	1 byte	14 (0E hex)
Operation code	1 byte	01 hex to get all basic device identification data 04 hex to get one specific basic device identification data
Object ID	1 byte	See below list for object ID values

Object ID	Object Name	Type	Response
0x00	VendorName (vendor name)	ASCII string	Schneider Electric
0x01	ProductCode (product code)	ASCII string	BME CRA 313 10
0x02	MajorMinorRevision (version number)	ASCII string	Example: V01.01.24

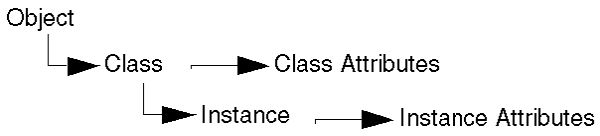
Diagnostics Available through EtherNet/IP CIP Objects

What's in This Chapter

M580 applications use CIP within a producer/consumer model to provide communication services in an industrial environment. This section describes the available CIP objects for diagnosing the X80 RIO drop redundant communication adapter module in an M580 system.

About CIP Objects

The CIP object data and content are exposed and accessed hierarchically in the following nested levels:



NOTE: You can use explicit messaging to access these items:

- Access a collection of instance attributes by including the class and instance values for the object in the explicit message.
- Access a single attribute by adding a specific attribute value to the explicit message with the class and instance values for the object.

The CIP objects and their content depend on the design of each device.

For more detailed information about CIP objects, refer to the ODVA standard documents:

- The CIP Networks Library, Volume 1, Common Industrial Protocol (CIP™) - Publication Number: PUB00001
- The CIP Networks Library, Volume 2, EtherNet/IP Adaptation of CIP - Publication Number: PUB00002

Identity Object

Overview

The Identity object provides identification and general information about the device.

Class ID

01 (hex), 01 (decimal)

Instance IDs

The Identity object presents 2 instances:

- 0: class
- 1: instance

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device Value = 1
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device Value = 1
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device Value = 7

The supported instance attributes (Instance ID = 1) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Vendor ID	UINT	Value =F3 hex (Schneider Electric)
2	Get	Device type	UINT	Value = 0C hex (Communication adapter device)
3	Get	Product code	UINT	Value = 0812 hex

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
4	Get	Revision	STRUCT of:	Product revision number
			USINT	Major revision
			USINT	Minor revision
5	Get	Status	WORD	Status of the adapter bit 2: • 01 hex = the module is configured bits 4 - 7: • 03 hex = no I/O connections established • 06 hex = at least 1 I/O connection in run mode • 07 hex = at least 1 I/O connection established, all in IDLE mode
6	Get	Serial number	UDINT	Serial number of the adapter
7	Get	Product name	STRING	Character string: 1 byte per character, 1 byte length indicator. Value = BMECRA31310

Services

The Identity object supports the following services:

Service Code	Description	Class	Instance	Notes
0x01	Get_Attributes_All	X	X	Returns: • all class attributes (instance = 0) • instance attributes 1 to 7 (instance = 1)
0x0E	Get_Attribute_Single	X	X	Returns the value of the specified attribute.
X = supported — = not supported				

Connection Manager Object

Overview

The Connection Manager Class allocates and manages the internal resources associated with both I/ O and Explicit Messaging Connections.

Class ID

06 (hex), 06 (decimal)

Instance IDs

The Connection Manager object presents 2 instance values:

- 0: class
- 1: instance

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device. Value = 1
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. Value = 1
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device. Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device. Value = 8

The supported instance attributes (Instance ID = 1) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Open Requests	UINT	Number of Forward Open service requests received.
2	Get	Open Format Rejects	UINT	Number of Forward Open service requests that were rejected due to an incorrect format.
3	Get	Open Resource Rejects	UINT	Number of Forward Open service requests that were rejected due to lack of resources.
4	Get	Open Other Rejects	UINT	Number of Forward Open service requests that were rejected for reasons other than an incorrect format or lack of resources.

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
5	Get	Close Requests	UINT	Number of Forward Close service requests received.
6	Get	Close Format Rejects	UINT	Number of Forward Close service requests that were rejected due to an incorrect format.
7	Get	Close Other Rejects	UINT	Number of Forward Close service requests that were rejected for reasons other than an incorrect format.
8	Get	Connection Timeouts	UINT	Total number of connection timeouts that occurred in connections controlled by this connections manager

Services

The Connection Manager object supports the following services:

Service Code	Description	Class	Instance	Notes
0x01	Get_Attributes_All	X	X	Returns: • all class attributes (instance = 0) • instance attributes 1 to 8 (instance = 1)
0x0E	Get_Attribute_ Single	X	X	Returns the value of the specified attribute.
X = supported — = not supported				

TCP/IP Interface Object

Overview

The TCP/IP Interface Object provides the mechanism to configure the TCP/IP network interface of the device. Examples of configurable items include IP Address, Network Mask, and Gateway Address of the device.

Class ID

F5 (hex), 245 (decimal)

Instance IDs

The TCP/IP interface object presents 2 instance values:

- 0: class
- 1: instance

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device. Value = 1
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device. Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device. Value = 11

The supported instance attributes (Instance ID = 1) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Status	DWORD	Interface status (bits 0–3): • 0 = The interface configuration attribute has not been configured. • 1 = The interface configuration attribute contains valid configuration obtain from DHCP.
2	Get	Configuration capability	DWORD	Device network configuration capability (bits 0–3): • 4 = The device is capable of obtaining its network configuration through DHCP.
3	Get Set	Configuration control	DWORD	Configuration method (bits 0–3): • 2 = The device obtains its network configuration through DHCP upon start-up.

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
4	Get	Physical Link Object	STRUCT of:	Path to physical link object
		Path size	UINT	Size of the path
		Path	Padded EPATH	Logical segments identifying the physical link object
5	Get Set	Interface Configuration	STRUCT of:	TCP/IP network interface configuration
		IP address	UDINT	IP adress of the device
		Network mask	UDINT	Network mask of the device
		Gateway address	UDINT	Default gateway address
		Name server	UDINT	Primary name server
		Name server 2	UDINT	Secondary name server
		Domain name	STRING	Default domain name
6	Get	Host name	STRING	The host name corresponds to the **Identifier** in Control Expert. For example `PCRA_001_0`.
10	Set(1)	selectAcd	BOOL	Activate the use of ACD: • 1 = ACD is enabled (default value) • 0 = ACD is disabled
11	Set(2)	LastConflictDetected	STRUCT of:	ACD diagnostic parameters Refer to chapter 5 - 4 in The CIP Networks Library, Volume 2, EtherNet/IP Adaptation of CIP for details.
		AcdActivity	USINT	State of ACD activity when last conflict detected
		RemoteMAC	ARRAY of 6 USINT	MAC address of remote node from the ARP PDU in which a conflict was detected
		ArpPdu	ARRAY of 28 USINT	Copy of the raw ARP PDU in which a conflict was detected

(1) The new value of the attribute is applied after a restart of the device.

(2) Set_Attribute_Single service is invoked with an attribute value of all 0 to reset this attribute. Other values returns an error code.

Services

The TCP/IP interface object supports the following services:

Service Code	Description	Class	Instance	Notes
0x01	Get_Attributes_All	X	X	Returns: • All class attributes (instance = 0) • Instance attributes 1 to 11 (instance = 1)
0x0E	Get_Attribute_ Single	X	X	Returns the value of the specified attribute.
0x10	Set_Attribute_Single (1)	—	X	Sets the value of the specified attribute.
X = supported — = not supported				
(1) The Set_Attribute_Single service can execute when these preconditions are satisfied: • Configure the Ethernet communication module to obtain its IP address from flash memory. • Confirm that the controller is in stop mode.				

Ethernet Link Object

Overview

The Ethernet Link object maintains link-specific status information for the Ethernet communications interface.

Class ID

F6 (hex), 246 (decimal)

Instance IDs

The Ethernet Link object presents the following instance values:

- 0: class
- 1: ETH 1 (Service port)
- 2: ETH 2 (LAN A port)
- 3: ETH 3 (LAN B port)
- 4: Ethernet backplane port
- 255: internal port
- 101: Ethernet port on backplane slot 0
- ....
- 112: Ethernet port on backplane slot 11

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device. Value = 255
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. Value = 0x11 (17 dec)
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device. Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device. Value = 10

The supported instance attributes (Instance ID = 1, 2, 3, 4, 101, ..., 112, or 255) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Interface Speed	UDINT	Valid values: 0, 10, 100.
2	Get	Interface Flags	DWORD	• Bit 0: link status 0 = Inactive 1 = Active • Bit 1: duplex mode 0 = half duplex 1 = full duplex • Bits 2...4: negotiation status 3 = successfully negotiated speed and duplex 4 = forced speed and link • Bit 5: manual setting requires reset 0 = automatic 1 = device need reset • Bit 6: local hardware detected error 0 = no event 1 = event detected
3	Get	Physical Address	ARRAY of 6 USINT	Module MAC address.
4	Get	Interface Counters	STRUCT of:	–
		In octets	UDINT	Octets received on the interface.
		In Ucast Packets	UDINT	Unicast packets received on the interface.
		In NUcast Packets	UDINT	Non-unicast packets received on the interface.
		In Discards	UDINT	Inbound packets received on the interface, but discarded.
		In Errors	UDINT	Inbound packets with detected errors (does not include in discards).
		In Unknown Protos	UDINT	Inbound packets with indeterminable protocol.
		Out Octets	UDINT	Octets sent on the interface.
		Out Ucast Packets	UDINT	Unicast packets sent on the interface.
		Out NUcast Packets	UDINT	Non-unicast packets sent on the interface.
		Out Discards	UDINT	Outbound packets discarded.
		Out Errors	UDINT	Outbound packets with detected errors.

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
5	Get	Media Counters	STRUCT of:	–
		Alignment Errors	UDINT	Frames that are not an integral number of octets in length.
		FCS Errors	UDINT	Incorrect CRC – frames received do not pass the FCS verification.
		Single Collisions	UDINT	Successfully transmitted frames that experienced exactly 1 collision.
		Multiple Collisions	UDINT	Successfully transmitted frames that experienced more than 1 collision.
		SQE Test Errors	UDINT	Number of times the detected SQE test error is generated.
		Deferred Transmissions	UDINT	Frames for which first transmission attempt is delayed because the medium is busy.
		Late Collisions	UDINT	Number of times a collision is detected later than 512 bit times into the transmission of a packet.
		Excessive Collisions	UDINT	Frames that do not transmit due to excessive number of collisions.
		MAC Transmit Errors	UDINT	Frames that do not transmit due to a detected internal MAC sub layer transmit error.
		Carrier Sense Errors	UDINT	Times that the carrier sense condition was lost or not asserted when attempting to transmit a frame.
		Frame Too Long	UDINT	Frames received that exceed the maximum permitted frame size.
		MAC Receive Errors	UDINT	Frames not received on an interface due to a detected internal MAC sub layer receive error.
6	Get Set	Interface Control	STRUCT of:	API of the connection.
		Control Bits	WORD	• Bit 0: Auto-negotiation disabled (0) or enabled (1). **NOTE:** When auto-negotiation is enabled, 0C hex (object state conflict) is returned when attempting to set either: ◦ forced interface speed ◦ forced duplex mode • Bit 1: forced duplex mode (if auto-negotiation bit = 0) 0 = half duplex 1 = full duplex
		Forced Interface Speed	UINT	Valid values include 10000000 and 100000000. **NOTE:** Attempting to set any other value returns the detected error 0x09 (invalid attribute value).
10	Get	Interface Label	SHORT_ STRING	A textual string identifying the interface. It includes 'internal' for internal interfaces. Maximum number of characters is 64.

Services

The Ethernet Link object supports the following services:

Service Code	Description	Class	In-stan-ce	Notes
0x01	Get_Attributes_All	X	X	Returns: • All class attributes (instance = 0) • Instance attributes 1 to 10 (instance = 1, 2, 3, 4, 101, ...112, or 255)
0x0E	Get_Attribute_ Single	X	X	Returns the value of the specified attribute.
0x10	Set_Attribute_ Single	—	X	Sets the value of the specified attribute.
0x4C	Get_And_Clear	—	X	Returns the value of the specified attribute then after the response the service set the value of the attribute to zero if the attribute is a counter (Interface counters #4 and Media counters # 5).
X = supported — = not supported				

PRP Protocol Object

Overview

The PRP Protocol object provides a configuration and diagnostic interface to the PRP protocol.

Class ID

56 (hex), 86 (decimal)

Instance IDs

The PRP Protocol object presents these instance values:

- 0: class
- 1: instance

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device. Value = 1
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. Value = 1
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device. Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device. Value = 20 (0x14)

The supported instance attributes (Instance ID = 1) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	LRE enable	BOOL	LRE (link redundancy entity) enable flag. Value = `TRUE`
2	Get	Node Type	UINT	Operating mode of the node. Value = `1` (PRP mode)
3	Get	Node Name	SHORT_STRING	Name of the LRE. Value = `PRP node`

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
4	Get	Version Name	SHORT_STRING	Version name of the LRE. Value = `version 1.0`
5	Get	LRE MAC Address	ETH_MAC_ADDR	Specify the MAC Address used by the LRE.
6	Get	Duplicate Discard	UINT	Specifies whether the duplicate discard algorithm is used at reception. Value = `1` (default) means the duplicate discard algorithm is used at reception.
7	Get	Transparent Reception	UINT	Specifies if the RCT is removed or passed from the frame by the LRE before forwarding to the upper layers. Value = `0` means the RCT is removed.
8	Get	LRE Interface Counters	STRUCT of:	—
		Transmit Count A	UDINT	Not applicable. Value = `0`
		Transmit Count B	UDINT	Not applicable. Value = `0`
		Transmit Count C	UDINT	Not applicable. Value = `0`
		Receive Count A	UDINT	Number of frames received on port A that are RCT (redundancy control trailer) appended with matching LAN-ID and PRP port. This counter is the sum of accepted and dropped frames.
		Receive Count B	UDINT	Number of frames received on port B that are RCT (redundancy control trailer) appended with matching LAN-ID and PRP port. This counter is the sum of accepted and dropped frames.
		Receive Count C	UDINT	Not applicable. Value = `0`
		Wrong LAN A Count	UDINT	Not applicable. Value = `0`
		Wrong LAN B Count	UINT	Not applicable. Value = `0`
		Wrong LAN C Count	UINT	Not applicable. Value = `0`

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
9	Get	LRE Duplicate Detection Counters	STRUCT of:	—
		Entries Unique Count A	UDINT	Not applicable. Value = 0
		Entries Unique Count B	UDINT	Not applicable. Value = 0
		Entries Duplicate Count A	UDINT	Number of frames in the duplicate detection mechanism on port A for which one single duplicate was received.
		Entries Duplicate Count B	UDINT	Number of frames in the duplicate detection mechanism on port B for which one single duplicate was received.
		Entries Multiple Count A	UDINT	Not applicable. Value = 0
		Entries Multiple Count B	UDINT	Not applicable. Value = 0
10	Get	Proxy Nodes Count	UDINT	Not applicable. Value = 0
11	Get	Proxy Nodes Table	ARRAY of:	—
		Proxy Node MAC Address	ETH_MAC_ADDR	Not applicable. The Proxy node table is empty.
12	Get	PRP Nodes Table Path	STRUCT of:	—
			UINT	Not applicable. Path size. Value = 0
			Padded EPATH	Not applicable. Path: Logical segments identifying the Nodes Table object Value = 0
13	Get	Switching Mode	UINT	Shows the feature implemented in the device Value = 3 (PRP node).
14	Get	HSR Mode	UINT	Not applicable Value = 0
15	Get	RedBox ID	UINT	Not applicable Value = 0
16	Get	Evaluate Supervision	BOOL	Module evaluates received supervision frames. Value = TRUE
17	Get	Warning LAN A	BOOL	Value = 1 means PRP supervision frames received on PRP LAN A with an incorrect LAN ID Value = 0 for else.
18	Get	Warning LAN B	BOOL	Value = 1 means PRP supervision frames received on PRP LAN B with an incorrect LAN ID Value = 0 for else.

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
19	Get	Warning Count LAN A	UINT	Not applicable Value = 0
20	Get	Warning Count LAN B	UINT	Not applicable Value = 0

Services

The PRP protocol object supports the following services:

Service Code	Description	Class	Instance	Notes
0x01	Get_Attributes_All	X	X	Returns: • All class attributes (instance = 0) • Instance attributes 1 to 20 (instance = 1)
0x0E	Get_Attribute_ Single	X	X	Returns the value of the specified attribute.
X = supported — = not supported				

EtherNet/IP Interface Diagnostics Object

Overview

The EtherNet/IP Interface Diagnostics object provides an overall diagnostic of the EIP communication of the EIP interface.

Class ID

350 (hex), 848 (decimal)

Instance IDs

The EtherNet/IP Interface object presents 2 instance values:

- 0: class
- 1: instance

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device. Value = 1
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. Value = 1
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device. Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device. Value = 7

The supported instance attributes (Instance ID = 1) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Protocols Supported	UINT	Protocol(s) supported (0 = not supported, 1 = supported) • Bit 0: EtherNet/IP • Bit 1: Modbus TCP/IP • Bit 2: Modbus SL • Bits 3...15: Reserved
2	Get	Connection Diagnostics	STRUCT of:	–
		Max CIP I/O connections opened	UINT	Number of CIP I/O connections opened since the last reset
		Current CIP I/O connections	UINT	Number of CIP I/O connections currently opened.
		Max CIP explicit connections opened	UINT	Number of CIP explicit connections opened since the last reset.
		Current CIP explicit connections	UINT	Number of CIP explicit connections currently opened.
		CIP connections opening detected errors	UINT	Increments each time a Forward Open is not successful (Originator and Target).
		CIP connections timeout detected errors	UINT	Increments when a connection times out (Originator and Target).
		Max EIP TCP connections opened	UINT	Number of TCP connections (used for EIP as client or server) opened since the last reset.
		Current EIP TCP connections	UINT	Number of TCP connections (used for EIP as client or server) currently open.
3	Get Clear	I/O Messaging Diagnostics	STRUCT of:	–
		I/O production counter	UDINT	Increments each time a Class 0/1 message is sent.
		I/O consumption counter	UDINT	Increments each time a Class 0/1 message is received.
		I/O productions send detected error counter	UINT	Increments each time a Class 0/1 message is not sent.
		I/O consumptions receive detected error counter	UINT	Increments each time a consumption is received with a detected error.
4	Get Clear	Explicit Messaging Diagnostics	STRUCT of:	–
		Class 3 message sent counter	UDINT	Increments each time a Class 3 message is sent (client and server).
		Class 3 message received counter	UDINT	Increments each time a Class 3 message is received (client and server).
		UCMM message received counter	UDINT	Increments each time an UCMM message is sent (client and server).
		UCMM message received counter	UDINT	Increments each time an UCMM message is received (client and server).

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
5	Get	Communication Capacity	STRUCT of:	–
		Max CIP I/O connections	UINT	Max supported CIP connections.
		Max TCP connections	UINT	Max supported TCP connections.
		Max Urgent priority rate	UINT	Max CIP transport Class 0/1 Urgent priority messages packets/s.
		Max Scheduled priority rate	UINT	Max CIP transport Class 0/1 Scheduled priority messages packets/s.
		Max High priority rate	UINT	Max CIP transport Class 0/1 High priority messages packets/s.
		Max Low priority rate	UINT	Max CIP transport Class 0/1 Low priority messages packets/s.
		Max Explicit Messaging rate	UINT	Max CIP transport Class 2/3 or other EIP messages packets/s.
6	Get	Bandwidth diagnostic	STRUCT of:	–
		Current sending Urgent priority rate	UINT	CIP transport Class 0/1 Urgent priority messages packets/s sent.
		Current reception Urgent priority rate	UINT	CIP transport Class 0/1 Urgent priority messages packets/s received.
		Current sending Scheduled priority rate	UINT	CIP transport Class 0/1 Scheduled priority messages packets/s sent.
		Current reception Scheduled priority rate	UINT	CIP transport Class 0/1 Scheduled priority messages packets/s received.
		Current sending High priority rate	UINT	CIP transport Class 0/1 High priority messages packets/s sent.
		Current reception High priority rate	UINT	CIP transport Class 0/1 High priority messages packets/s received.
		Current sending Low priority rate	UINT	CIP transport Class 0/1 Low priority messages packets/s sent.
		Current reception Low priority rate	UINT	CIP transport Class 0/1 Low priority messages packets/s received.
		Current sending Explicit rate	UINT	CIP transport Class 2/3 or other EIP messages packets/s sent.
		Current reception Explicit rate	UINT	CIP transport Class 2/3 or other EIP messages packets/s received.
7	Get	Modbus diagnostic	STRUCT of:	–
		Max Modbus TCP connections opened	UINT	Maximum number of TCP connection opened and used for Modbus communication.
		Current Modbus TCP connections	UINT	Number of TCP connections currently opened and used for Modbus communication.
		Modbus TCP message send counter	UDINT	Incremented each time a Modbus TCP/IP message is sent.
		Modbus TCP message received counter	UDINT	Incremented each time a Modbus TCP/IP message is received.

Services

The EtherNet/IP Interface Diagnostics object supports the following services:

Service Code	Description	Class	In-stan-ce	Notes
0x01	Get_Attributes_All	X	X	Returns: • all class attributes (instance = 0) • instance attributes 1 to 7 (instance = 1)
0x0E	Get_Attribute_ Single	X	X	Returns the value of the specified attribute.
0x4C	Get_and_Clear	—	X	Returns the value of the specified attribute then after the response the service set the value of the attribute to zero if it is a counter.
X = supported — = not supported				

I/O Connection Diagnostics Object

Overview

The I/O Connection Diagnostics object provides a detailed diagnostic of each opened CIP IO connection.

Class ID

352 (hex), 850 (decimal)

Instance IDs

The I/O Connection Diagnostics object presents the following instance values:

- 0: class
- 1...N: instances

  where N is the maximum number of CIP IO connection.

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device. Example value = 3
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. Example value = 2
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device. Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device. Value = 2

The supported instance attributes (Instance ID = 1 to N) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get Clear	I/O Communication Diagnostics	STRUCT of:	—
		I/O production counter	UDINT	Increments at each production.
		I/O consumption counter	UDINT	Increments at each consumption.
		I/O production sent detected error counter	UINT	Increments each time a production is not sent.
		I/O consumption received detected errors counter	UINT	Increments each time a consumption is received with a detected error.
		CIP connection timeout detected errors	UINT	Increments when a connection times out.
		CIP connection opening detected errors	UINT	Increments each time a connection is unable to open.
		CIP connection state	UINT	State of the CIP IO connection(1).
		CIP last detected error general status	UINT	General status of the last error detected on the connection
		CIP last detected error extended status	UINT	Extended status of the last error detected on the connection
		Input communication status	UINT	Communication status of the inputs (see table, below)
		Output communication status	UINT	Communication status of the outputs (see table, below)

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
2	Get	Connection Diagnostics	STRUCT of:	–
		Production connection ID	UDINT	Connection ID for production
		Consumption connection ID	UDINT	Connection ID for consumption
		Production RPI	UDINT	RPI for production (µs)
		Production API	UDINT	API for production (µs)
		Consumption RPI	UDINT	RPI for consumption (µs)
		Consumption API	UDINT	API for consumption (µs)
		Production connection parameters	UDINT	Connection parameters for production(2).
		Consumption connection parameters	UDINT	Connection parameters for consumption(2).
		Local IP	UDINT	–
		Local UDP port	UINT	–
		Remote IP	UDINT	–
		Remote UDP port	UINT	–
		Production multicast IP	UDINT	Multicast IP address used for production. If not used, it is 0.
		Consumption multicast IP	UDINT	Multicast IP address used for consumption. If not used, it is 0.
		Protocols supported	UDINT	Protocol(s) supported on the I/O connection (0 = not supported, 1 = supported) • Bit 0: EtherNet/IP • Bit 1: Modbus TCP/IP • Bit 2: Modbus SL • Bits 3...15: Reserved

Refer to The CIP Networks Library, Volume 1, Common Industrial Protocol (CIP™) - Publication Number: PUB00001 for:

(1) The description is provided in the chapter **3-4.4.1 State Attribute**.

(2) The description is provided in the chapter **3-5.5.1.1 Network Connection Parameters**.

The following values describe the structure of the instance attributes *Input Communication status*, and *Output communication status*:

Bit Number	Description	Values
15...3	*Reserved*	0
2	Idle	0 = no idle notification 1 = idle notification
1	Consumption inhibited	0 = consumption started 1 = no consumption
0	Production inhibited	0 = production started 1 = no production

Services

The I/O connection Diagnostics object supports the following services:

Service Code	Description	Class	Instance	Notes
0x01	Get_Attributes_All	X	X	Returns: • All class attributes (instance = 0) • Instance attributes 1 to 2 (instance = 1...N)
0x0E	Get_Attribute_ Single	X	X	Returns the value of the specified attribute.
0x4C	Get_and_Clear	—	X	Returns the value of the specified attribute then after the response the service set the value of the attribute to zero if it is a counter.
X = supported — = not supported				

Service Port Control Object

Overview

The BMECRA31310(H) adapter module supports the Schneider vendor specific Service Port Control Object. This CIP object includes status information and can also be used for configuring the service port through explicit messaging.

Class ID

400 (hex), 1024 (decimal)

Instance IDs

The Service Port Control object presents these instance values:

- 0: class
- 1: instance

Attributes

The supported class attributes (Instance ID = 0) are as follows:

Class attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get	Revision	UINT	Revision of the object
2	Get	Max Instance	UINT	Maximum instance number of the object currently created in this class level of the device. Value = 1
3	Get	Number of Instances	UINT	Number of object instances currently created at this class level of the device. Value = 1
6	Get	Maximum ID Number Class Attributes	UINT	The attribute ID number of the last class attribute of the class definition implemented in the device. Value = 7
7	Get	Maximum ID Number Instance Attributes	UINT	The attribute ID number of the last instance attribute of the class definition implemented in the device. Value = 2

The supported instance attributes (Instance ID = 1) are as follows:

Instance attribute				
ID	**Access**	**Name**	**Type**	**Description / Value**
1	Get Set	Port control	UINT	0: disabled 1: access port 2: port mirroring
2	Get Set	Mirror	UINT	bit 0: ETH2 port (PRP LAN A port) bit 1: ETH3 port (PRP LAN B port) bit 2: backplane port bit 3: internal port

NOTE:

- If the SERVICE port is not configured for port mirroring, the mirror attribute is ignored. If the value of a parameter request is outside the valid range, the service request is ignored.
- In port mirroring mode, the SERVICE port acts like a read-only port. That is, you cannot access devices (ping, connection to Control Expert, and so on) through the SERVICE port.

Services

The Service Port Control object supports these services:

Service Code	Description	Class	Instance	Notes
0x01	Get_Attributes_All	X	X	Returns: • all class attributes (instance = 0) • instance attributes 1 to 2(instance = 1)
0x0E	Get_Attribute_ Single	X	X	Returns the value of the specified attribute.
0x02	Set_Attributes_All	—	X	Set all attributes in a single message.
0x10	Set_Attribute_Single	—	X	Set a single specified attribute.
X = supported — = not supported				

MIB-II

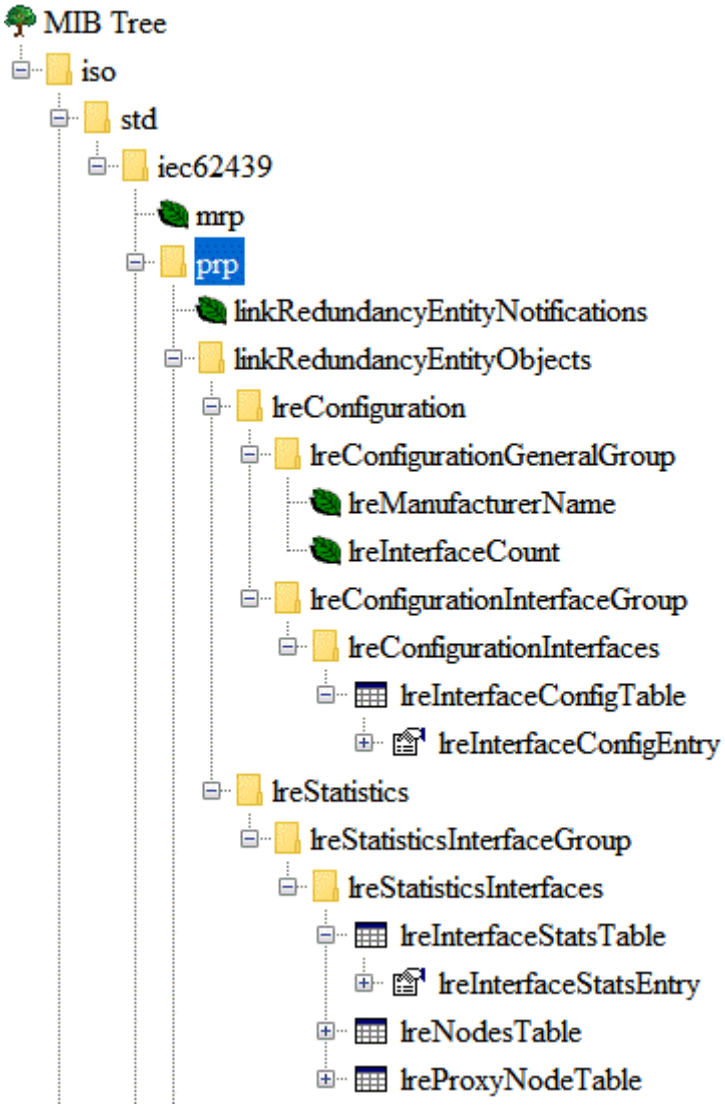
What's in This Chapter

This chapter provides the detailed tree structure of the PRP— MIB as defined in IEC 62439–3.

PRP-MIB Description

Introduction

The PRP-MIB supported by the BMECRA31310(H) adapter module presents the following tree structure:



The BMECRA31310(H) adapter module has one LRE (representing a pair of LAN ports A and B). So there is one entry in the interface configuration table and one entry in the interface statistics table.

NOTE: As the BMECRA31310(H) adapter module do not support the node table nor the proxy node table, the objects in the lreNodesTable and lreProxyNodeTable are not supported.

lreConfiguration Objects

The configuration objects in the PRP-MIB are divided into two groups:

- lreConfigurationGeneralGroup
- lreConfigurationInterfaceGroup

The following table presents the objects available in the lreConfigurationGeneralGroup

Object Name / OID	Access	Syntax	Description / Value
lreManufacturerName OID: 1.0.62439.2.21.0.0.1	Read Only	STRING	Specifies the name of the LRE device manufacturer. Value = Schneider Electric
lreInterfaceCount OID: 1.0.62439.2.21.0.0.2	Read Only	INTEGER	Total number of LREs present in this system. Value = 1

In the lreConfigurationInterfaceGroup, you can access the available objects under the following subtree:
lreConfigurationInterfaceGroup (OID: 1.0.62439.2.21.0.1)
— lreConfigurationInterfaces (OID: 1.0.62439.2.21.0.1.0)
— — lreInterfaceConfigTable (OID: 1.0.62439.2.21.0.1.0.1)
— — — lreInterfaceConfigEntry (OID: 1.0.62439.2.21.0.1.0.1.1)

Object Name / OID	Data access	Syntax	Description / Value
lreInterfaceConfigIndex OID: 1.0.62439.2.21.0.1.0.1.1.-1	No access	Unsigned32	Unique value for each LRE.
lreRowStatus OID: 1.0.62439.2.21.0.1.0.1.1.-2	Read create	INTEGER	Indicates the status of the LRE table entry. Value = 1
lreNodeType OID: 1.0.62439.2.21.0.1.0.1.1.-3	Read Write	INTEGER	Specifies the operation mode of the LRE. Value = 1 (PRP mode)
lreNodeName OID: 1.0.62439.2.21.0.1.0.1.1.-4	Read Write	STRING	Specifies this LRE's node name. Value = BMECRA31310
lreVersionName OID: 1.0.62439.2.21.0.1.0.1.1.-5	Read Only	OCTET STRING	Specifies the version of this LRE's software. Example value = FwID:01.01
lreMacAddress OID: 1.0.62439.2.21.0.1.0.1.1.-6	Read Write	OCTET STRING	Specifies the MAC address in hexadecimal to be used by this LRE. MAC addresses are identical for all ports of a single LRE. Example value = 00 80 F4 01 F3 47
lrePortAdminStateA OID: 1.0.62439.2.21.0.1.0.1.1.-7	Read Write	INTEGER	Specifies whether the port A shall be active or not Active through administrative action. Value = 2 (default = active)
lrePortAdminStateB OID: 1.0.62439.2.21.0.1.0.1.1.-8	Read Write	INTEGER	Specifies whether the port B shall be active or not Active through administrative action. Value = 2 (default = active)
lreLinkStatusA OID: 1.0.62439.2.21.0.1.0.1.1.-9	Read Only	INTEGER	Shows the link status of the LRE's port A. Value = 1 (up)
lreLinkStatusB OID: 1.0.62439.2.21.0.1.0.1.1.-10	Read Only	INTEGER	Shows the link status of the LRE's port B. Value = 1 (up)

Object Name / OID	Data access	Syntax	Description / Value
lreDuplicateDiscard OID: 1.0.62439.2.21.0.1.0.1.1.-11	Read Write	INTEGER	Specifies whether a duplicate discard algorithm is used at reception. Value = 2 (default = discard)
lreTransparentReception OID: 1.0.62439.2.21.0.1.0.1.1.-12	Read Write	INTEGER	If removeRCT is configured, the RCT is removed when forwarding to the upper layers. Value = 1 (default = removeRCT)
lreHsrLREMode OID: 1.0.62439.2.21.0.1.0.1.1.-13	Read Write	INTEGER	This enumeration is applicable if the LRE is an HSR bridging node or RedBox. Value = 1 (default mode)
lreSwitchingEndNode OID: 1.0.62439.2.21.0.1.0.1.1.-14	Read Write	INTEGER	This enumeration shows which feature is enabled in this particular LRE. Value = 3 (prpmode)
lreRedBoxIdentity OID: 1.0.62439.2.21.0.1.0.1.1.-15	Read Write	INTEGER	The integer value states the value of the path field a Modicon Redundancy switch inserts into each frame it receives from its interlink and injects into the HSR ring. When interpreted as binary values, the LSB denotes the configuration of the RedBox (A or B), and the following 3 bits denote the identifier of a Modicon Redundancy switch pair. Value = 2 (id1a)
lreEvaluateSupervision OID: 1.0.62439.2.21.0.1.0.1.1.-16	Read Write	INTEGER (TruthValue)	TRUE if the LRE evaluates received supervision frames. FALSE if it drops the supervision frames without evaluating. **NOTE:** LREs are required to send supervision frames, but reception is optional. Default value is dependent on implementation. Value = 1 (TRUE)
lreNodesTableClear OID: 1.0.62439.2.21.0.1.0.1.1.-17	Read Write	INTEGER	Specifies that the Node table is to be cleared. Value = 0 **NOTE:** Node table is not supported.
lreProxyNodeTableClear OID: 1.0.62439.2.21.0.1.0.1.1.-18	Read Write	INTEGER	Specifies that the Proxy Node table is to be cleared. Value = 0 **NOTE:** Proxy Node table is not supported.

lreStatistics Objects

In the lreStatisticsInterfacesGroup, you can access the available objects under the following subtree:
lreStatisticsInterfacesGroup (OID: 1.0.62439.2.21.1.1)
— lreStatisticsInterfaces (OID: 1.0.62439.2.21.1.1.0)
— — lreInterfaceStatsTable (OID: 1.0.62439.2.21.1.1.0.1)
— — — lreInterfaceStatsEntry (OID: 1.0.62439.2.21.1.1.0.1.1)

Object Name / OID	Access	Syntax	Description / Value
lreInterfaceStatsIndex OID: 1.0.62439.2.21.1.1.0.1.1.-1	No access	Unsigned32	Unique value for each LRE.
lreCntTxA OID: 1.0.62439.2.21.1.1.0.1.1.-2	Read Only	Counter32	Not supported Value = 0
lreCntTxB OID: 1.0.62439.2.21.1.1.0.1.1.-3	Read Only	Counter32	Not supported Value = 0
lreCntTxC OID: 1.0.62439.2.21.1.1.0.1.1.-4	Read Only	Counter32	Not supported Value = 0
lreCntErrWrongLanA OID: 1.0.62439.2.21.1.1.0.1.1.-5	Read Only	Counter32	Number of frames with the incorrect LAN identifier received on port A. Initial value = 0
lreCntErrWrongLanB OID: 1.0.62439.2.21.1.1.0.1.1.-6	Read Only	Counter32	Number of frames with the incorrect LAN identifier received on port B. Initial value = 0.
lreCntErrWrongLanC OID: 1.0.62439.2.21.1.1.0.1.1.-7	Read Only	Counter32	Not supported Value = 0
lreCntRxA OID: 1.0.62439.2.21.1.1.0.1.1.-8	Read Only	Counter32	Number of frames received on port A. Only frames fitted with a PRP Redundancy Control Trailer are counted. Frames that are not forwarded anywhere (for example, because the sender of the frame is in the proxy node table) are counted, too. Only frames received completely and without error are counted. Initial value = 0.
lreCntRxB OID: 1.0.62439.2.21.1.1.0.1.1.-9	Read Only	Counter32	Number of frames received on port B. Only frames fitted with a PRP Redundancy Control Trailer are counted. Frames that are not forwarded anywhere (for example, because the sender of the frame is in the proxy node table) are counted, too. Only frames received completely and without error are counted. Initial value = 0.
lreCntRxC OID: 1.0.62439.2.21.1.1.0.1.1.-10	Read Only	Counter32	Not supported Value = 0
lreCntErrorsA OID: 1.0.62439.2.21.1.1.0.1.1.-11	Read Only	Counter32	Not supported Value = 0
lreCntErrorsB OID: 1.0.62439.2.21.1.1.0.1.1.-12	Read Only	Counter32	Not supported Value = 0

Object Name / OID	Access	Syntax	Description / Value
lreCntErrorsC OID: 1.0.62439.2.21.1.1.0.1.1.-13	Read Only	Counter32	Not supported Value = 0
lreCntNodes OID: 1.0.62439.2.21.1.1.0.1.1.-14	Read Only	INTEGER	Not supported Value = 0
lreCntProxyNodes OID: 1.0.62439.2.21.1.1.0.1.1.-15	Read Only	INTEGER	Not supported Value = 0
lreCntUniqueA OID: 1.0.62439.2.21.1.1.0.1.1.-16	Read Only	Counter32	Not supported Value = 0
lreCntUniqueB OID: 1.0.62439.2.21.1.1.0.1.1.-17	Read Only	Counter32	Not supported Value = 0
lreCntUniqueC OID: 1.0.62439.2.21.1.1.0.1.1.-18	Read Only	Counter32	Not supported Value = 0
lreCntDuplicateA OID: 1.0.62439.2.21.1.1.0.1.1.-19	Read Only	Counter32	Number of entries in the duplicate detection mechanism on port A for which one single duplicate was received. Initial value = 0.
lreCntDuplicateB OID: 1.0.62439.2.21.1.1.0.1.1.-20	Read Only	Counter32	Number of entries in the duplicate detection mechanism on port B for which one single duplicate was received. Initial value = 0.
lreCntDuplicateC OID: 1.0.62439.2.21.1.1.0.1.1.-21	Read Only	Counter32	Not supported Value = 0
lreCntMultiA OID: 1.0.62439.2.21.1.1.0.1.1.-22	Read Only	Counter32	Not supported Value = 0
lreCntMultiB OID: 1.0.62439.2.21.1.1.0.1.1.-23	Read Only	Counter32	Not supported Value = 0
lreCntMultiC OID: 1.0.62439.2.21.1.1.0.1.1.-24	Read Only	Counter32	Not supported Value = 0
lreCntOwnRxA OID: 1.0.62439.2.21.1.1.0.1.1.-25	Read Only	Counter32	Not supported Value = 0
lreCntOwnRxB OID: 1.0.62439.2.21.1.1.0.1.1.-26	Read Only	Counter32	Not supported Value = 0

Modicon Switch Device DDT Structure

The following table describes the diagnostic parameters in implicit exchanges for :

- MCSESR043F2•••(C): Modicon Redundancy switch
- MCSESM•••
- MCSESP•••

Name	Type	Description
Freshness	BOOL	This is a global bit: • **1**: All input objects below (Freshness_1, ...) for the associated device are true (1) and provide up-to-date data. • **0**: One or more inputs (below) is not connected and does not provide up-to-date data.
Freshness_1	BOOL	This bit represents individual input objects for the connection: • **1**: The input object is connected and provides up-to-date data. • **0**: The input object is not connected and does not provide up-to-date data.

Name		Type	Description
Inputs	Free0	BYTE	–
	Device_Error	BOOL	Like the signal contact, the value indicates the device overall state (0 = OK, 1 = error).
	Device_Security_Error	BOOL	Device security state (0 = OK, 1 = error)
	Power_Supply_1_Error	BOOL	Power supply 1 error (0 = OK, 1 = error or not existing)
	Power_Supply_2_Error	BOOL	Power supply 2 error (0 = OK, 1 = error or not existing)
	RESERVED_BIT_0	BOOL	Reserved Data
	RESERVED_BIT_1	BOOL	Reserved Data
	Signal_Contact_1_Open	BOOL	Signal contact 1 state (0 = closed, 1 = opened)
	Signal_Contact_2_Open	BOOL	Signal contact 2 state (0 = closed, 1 = open or not existing)
	Free1	BYTE	-
	RESERVED	BOOL	Reserved Data
	Temperature_Error	BOOL	Temperature status (0 = OK, 1 = error)
	Module_Removed	BOOL	Module removed status (1 = removed)
	ACA22_USB_C_ Removed	BOOL	ACA22 USB-C removed (1 = removed)
	ACA31_Removed	BOOL	ACA31 removed (1 = removed)
	Free2	BYTE	Reserved Data
	RESERVEDA	BOOL	Reserved Data
	RESERVEDB	BOOL	Reserved Data
	MRP_Enabled	BOOL	MRP enabled
	Free3	BYTE	–
	PRP_Enabled	BOOL	PRP enabled
	HSR_Enabled	BOOL	HSR enabled
	RSTP_Enabled	BOOL	RSTP enabled
	LAG_Enabled	BOOL	LAG enabled
	DLR_Enabled	BOOL	DLR enabled
	RESERVEDC	BOOL	Reserved Data
	RESERVEDG	BOOL	Reserved Data
	Connection_Error	BOOL	Connection error
	Link_States	DWORD	Ethernet Port Link States - Bitmask (1 Bit per port), 0 = LinkDown, 1 = LinkUp
	Output_Links_Admin_ State_Appl	DWORD	Port Link Admin States (acknowledge to output data) - Bitmask (1 Bit per port) to acknowledge output, 0 = Port enabled, 1 = Port disabled
	Utilization_Alarm	DWORD	Ethernet Port Utilization Alarm Status (bitmask per port) - Bitmask (1 Bit per port), 0 = No alarm, 1 = alarm
	Access_Violation	DWORD	Ethernet Port Access Violation Status (bit mask per port) - Bitmask (1 Bit per port), 0 = No alarm, 1 = alarm
	Multicast_Connections	DINT	Number of Multicast (I/O, Class1) Connections currently opened
	TCP/IP_Connections	DINT	Number of Class 3 Connections currently opened
	Quick_Connect_Mask	DWORD	Quick Connect Port Status - Bitmask (1 Bit per port), 0 = Quick Connect is disabled, 1 = Quick Connect is enabled

Glossary

A

adapter:

An adapter is the target of real-time I/O data connection requests from scanners. It cannot send or receive real-time I/O data unless it is configured to do so by a scanner, and it does not store or originate the data communications parameters necessary to establish the connection. An adapter accepts explicit message requests (connected and unconnected) from other devices.

AUX:

An (AUX) task is an optional, periodic processor task that is run through its programming software. The AUX task is used to execute a part of the application requiring a low priority. This task is executed only if the MAST and FAST tasks have nothing to execute. The AUX task has two sections:

- IN: Inputs are copied to the IN section before execution of the AUX task.
- OUT: Outputs are copied to the OUT section after execution of the AUX task.

B

broadcast:

A message sent to all devices in a broadcast domain.

C

CCOTF:

(*change configuration on the fly*) A feature of Control Expert that allows a module hardware change in the system configuration while the system is operating. This change does not impact active operations.

CIP™:

(*common industrial protocol*) A comprehensive suite of messages and services for the collection of manufacturing automation applications (control, safety, synchronization, motion, configuration and information). CIP allows users to integrate these manufacturing applications with enterprise-level Ethernet networks and the internet. CIP is the core protocol of EtherNet/IP.

CPU:

(*central processing unit*) The CPU, also known as the processor or controller, is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. CPUs are computers suited to survive the harsh conditions of an industrial environment.

D

DDT:

(*derived data type*) A derived data type is a set of elements with the same type (`ARRAY`) or with different types (structure).

determinism:

For a defined application and architecture, you can predict that the delay between an event (change of value of an input) and the corresponding change of a controller output is a finite time *t*, smaller than the deadline required by your process.

DHCP:

(*dynamic host configuration protocol*) An extension of the BOOTP communications protocol that provides for the automatic assignment of IP addressing settings, including IP address, subnet mask, gateway IP address, and DNS server names. DHCP does not require the maintenance of a table identifying each network device. The client identifies itself to the DHCP server using either its MAC address, or a uniquely assigned device identifier. The DHCP service utilizes UDP ports 67 and 68.

DRS:

(*dual-ring switch*) A ConneXium extended managed switch that has been configured to operate on an Ethernet network. Predefined configuration files are provided by Schneider Electric to downloaded to a DRS to support the special features of the main ring / sub-ring architecture.

DSCP:

(*differentiated service code points*) This 6-bit field is in the header of an IP packet to classify and prioritize traffic.

E

EtherNet/IP™:

A network communication protocol for industrial automation applications that combines the standard internet transmission protocols of TCP/IP and UDP with the application layer common industrial protocol (CIP) to support both high speed data exchange and industrial control. EtherNet/IP employs electronic data sheets (EDS) to classify each network device and its functionality.

Ethernet:

A 10 Mb/s, 100 Mb/s, or 1 Gb/s, CSMA/CD, frame-based LAN that can run over copper twisted pair or fiber optic cable, or wireless. The IEEE standard 802.3 defines the rules for configuring a wired Ethernet network; the IEEE standard 802.11 defines the rules for configuring a wireless Ethernet network. Common forms include 10BASE-T, 100BASE-TX, and 1000BASE-T, which can utilize category 5e copper twisted pair cables and RJ45 modular connectors.

explicit messaging:

TCP/IP-based messaging for Modbus TCP and EtherNet/IP. It is used for point-to-point, client/server messages that include both data, typically unscheduled information between a client and a server, and routing information. In EtherNet/IP, explicit messaging is considered class 3 type messaging, and can be connection-based or connectionless.

F

FAST:

A FAST task is an optional, periodic processor task that identifies high priority, multiple scan requests, which is run through its programming software. A FAST task can schedule selected I/O modules to have their logic solved more than once per scan. The FAST task has two sections:

- IN: Inputs are copied to the IN section before execution of the FAST task.
- OUT: Outputs are copied to the OUT section after execution of the FAST task.

I

implicit messaging:

UDP/IP-based class 1 connected messaging for EtherNet/IP. Implicit messaging maintains an open connection for the scheduled transfer of control data between a producer and consumer. Because an open connection is maintained, each message contains primarily data, without the overhead of object information, plus a connection identifier.

IP address:

The 32-bit identifier, consisting of both a network address and a host address assigned to a device connected to a TCP/IP network.

L

LRE:

(*Link Redundancy Entity*) Component of a DAN, it handles duplication of packets and management of the redundancy.

M

MAST:

A master (MAST) task is a deterministic processor task that is run through its programming software. The MAST task schedules the RIO module logic to be solved in every I/O scan. The MAST task has two sections:

- IN: Inputs are copied to the IN section before execution of the MAST task.
- OUT: Outputs are copied to the OUT section after execution of the MAST task.

MIB:

(*management information base*) A virtual database used for managing the objects in a communications network. See SNMP.

MTU:

(*Maximum Transmission Unit*) It defines the largest size of Ethernet frames that an interface can send or receive in a network transaction.

multicast:

A special form of broadcast where copies of the packet are delivered to only a specified subset of network destinations. Implicit messaging typically uses multicast format for communications in an EtherNet/IP network.

N

NTP:

(*network time protocol*) Protocol for synchronizing computer system clocks. The protocol uses a jitter buffer to resist the effects of variable latency.

P

PAC:

programmable automation controller. The PAC is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. PACs are computers suited to survive the harsh conditions of an industrial environment.

port 502:

Port 502 of the TCP/IP stack is the well-known port that is reserved for Modbus TCP communications.

port mirroring:

In this mode, data traffic that is related to the source port on a network switch is copied to another destination port. This allows a connected management tool to monitor and analyze the traffic.

PRP: A parallel redundancy protocol (PRP) is a network protocol standard that provides redundancy by duplicating the network infrastructure and by monitoringe the simultaneous data transmitted in both independent network.

R

RCT:

(*Redundancy Control Trailer*) A 6-bytes sequence number appended to the Ethernet frame by the LRE. It contains a sequence number, the LAN identifier, the frame data size, and the PRP suffix that identifies the trailer type as PRP.

RedBox:

(*Redundancy Box*) It is a switch that enables non-PRP nodes to connect to the PRP network. M580 CPU, DIO, X80 RIO drops manages by a BM•CRA312•0 adapter module are examples of non-PRP nodes.

RIO drop:

One of the three types of RIO modules in an Ethernet RIO network. An RIO drop is an M580 rack of I/O modules that are connected to an Ethernet RIO network and managed by an Ethernet RIO adapter module. A drop can be a single rack or a main rack with an extended rack.

RIO network:

An Ethernet-based network that contains 3 types of RIO devices: a local rack, an RIO drop, and a ConneXium extended dual-ring switch (DRS). Distributed equipment may also participate in an RIO network via connection to DRSs or BMENOS0300 network option switch modules.

RSTP:

(*rapid spanning tree protocol*) Allows a network design to include spare (redundant) links to provide automatic backup paths if an active link stops working, without the need for loops or manual enabling/disabling of backup links.

S

service port:

A dedicated Ethernet port on the M580 RIO modules. The port may support these major functions (depending on the module type):

- port mirroring: for diagnostic use
- access: for connecting HMI/Control Expert/ConneXview to the CPU
- extended: to extend the device network to another subnet
- disabled: disables the port, no traffic is forwarded in this mode

T

TCP/IP:

Also known as *internet protocol suite*, TCP/IP is a collection of protocols used to conduct transactions on a network. The suite takes its name from two commonly used protocols: transmission control protocol and internet protocol. TCP/IP is a connection-oriented protocol that is used by Modbus TCP and EtherNet/IP for explicit messaging.

TCP:

(*transmission control protocol*) A key protocol of the internet protocol suite that supports connection-oriented communications, by establishing the connection necessary to transmit an ordered sequence of data over the same communication path.

trap:

A trap is an event directed by an SNMP agent that indicates one of these events:

- A change has occurred in the status of an agent.
- An unauthorized SNMP manager device has attempted to get data from (or change data on) an SNMP agent.

U

UDP:

(*user datagram protocol*) A transport layer protocol that supports connectionless communications. Applications running on networked nodes can use UDP to send datagrams to one another. Unlike TCP, UDP does not include preliminary communication to establish data paths or provide data ordering and checking. However, by avoiding the overhead required to provide these features, UDP is faster than TCP. UDP may be the preferred protocol for time-sensitive applications, where dropped datagrams are preferable to delayed datagrams. UDP is the primary transport for implicit messaging in EtherNet/IP.

Index

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

EIO0000004532.01