

Altivar HVAC ATH200

Variable Speed Drives for Asynchronous and Synchronous Motors

BACnet MS/TP Embedded - BACnet IP VW3A3726 Manual

JPS43216.01
12/2025



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.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

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.....	5
About the document	7
Hardware Setup	14
BACnet MSTP Network Configurations	15
BACnet IP Network Configurations	18
Cyber Security.....	21
Overview	22
Defense in depth measures expected in the environment	23
Security Policy.....	25
Potential Risks and Compensating Controls	26
Account Management Guidelines	28
Software Setup.....	29
Software Overview	30
BACnet MS/TP parameters	33
BACnet IP parameters	37
[User authentication] SEC- menu.....	44
Software Setup with SpaceLogic™ AS-P Automation Server.....	46
Introduction.....	47
How to Configure SpaceLogic Ready-Server using Configuration Wizard	48
Command and communication configuration	49
Connect the drive and the controller with EcoStruxure™ Building Operation.....	50
Diagnostics and Troubleshooting	53
Configuring Communication Error Response	54
Communication troubleshooting	56
Control-Signal Diagnostics	57
Communication error codes.....	58
Annex.....	61
Firmware Update.....	62
Operation.....	63
Profile	64
Functional Profiles Supported by the Drive.....	65
Functional Description.....	66
CIA402 Operating State Diagram.....	67
Description of Operating States.....	68
Device Status Summary	69
Command Register $C \ N \ d$	70
Stop Commands.....	71
Assigning Control Word Bits	71
[CIA402 State Reg] $E \ L \ R$	72
Extended Control Word	73
Internal State register.....	74
Starting Sequence	75
Starting Sequence for a Drive Powered by the Power Stage Supply	76
Starting Sequence for a Drive with Separate Control Stage	78

Starting Sequence for a Drive with Mains Contactor Control	81
Operating Modes	83
Configuring the Control Channel	84
Configuration of the Drive for Operation with CiA 402 Profile in Combined Mode	84
Configuration of the Drive for Operation with CiA 402 Profile in Separate Mode	85
BACnet Basics	86
BACnet Devices	87
Monitoring of communication channel / Bacnet timeout	88
BACnet Device Profiles and BIBBs.....	89
BACnet Object.....	91
Binary input object.....	91
Binary output object.....	91
Analog input object.....	91
Analog output object.....	91
Binary value object.....	92
Analog value object.....	93
Device object.....	96
Port object.....	98
Additional Functions.....	100
Glossary	101

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.

Qualification of Personnel

Only appropriately trained persons who are familiar with and understand the contents of this manual and all other pertinent product documentation are authorized to work on and with this product. In addition, these persons must have received safety training to recognize and avoid hazards involved. These persons must have sufficient technical training, knowledge and experience and be able to foresee and detect potential hazards that may be caused by using the product, by changing the settings and by the mechanical, electrical and electronic equipment of the entire system in which the product is used. All persons working on and with the product must be fully familiar with all applicable standards, directives, and accident prevention regulations when performing such work.

Intended Use

This product is intended for industrial use according to this manual.

The product may only be used in compliance with all applicable safety standard and local regulations and directives, the specified requirements and the technical data. The product must be installed outside the hazardous ATEX zone. Prior to using the product, you must perform a risk assessment in view of the planned application. Based on the results, the appropriate safety measures must be implemented. Since the product is used as a component in an entire system, you must ensure the safety of persons by means of the design of this entire system (for example, machine design). Any use other than the use explicitly permitted is prohibited and can result in hazards.

About the document

Document Scope

The purpose of this document is to show you how to configure the Altivar HVAC ATH230 and ATH250 to use BACnet for monitoring and control.

NOTE: Read and understand this document and all related documents (see below) before installing, operating, or maintaining your drive.

Validity Note

Original instructions and information given in the present document have been written in English (before optional translation).

This documentation is valid for the Altivar HVAC ATH200 drives.

Product Related Information

Read and understand these instructions before performing any procedure with this device.

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Only appropriately trained persons who are familiar with and fully understand the contents of the present manual and all other pertinent product documentation and who have received all necessary training to recognize and avoid hazards involved are authorized to work on and with this device system.
- Installation, adjustment, repair and maintenance must be performed by qualified personnel.
- Verify compliance with all local and national electrical code requirements as well as all other applicable regulations with respect to grounding of all equipment.
- Only use properly rated, electrically insulated tools and measuring equipment.
- Do not touch unshielded components or terminals with voltage present.
- Prior to performing any type of work on the device system, block the motor shaft to prevent rotation.
- Insulate both ends of unused conductors of the motor cable.
- Do not short across the DC bus terminals or the DC bus capacitors or the braking resistor terminals.

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

Damaged products or accessories may cause electric shock or unanticipated equipment operation.

⚡⚠ DANGER

ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION

Do not use damaged products or accessories.

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

Contact your local Schneider Electric sales office if you detect any damage whatsoever.

Your application consists of a whole range of different interrelated mechanical, electrical, and electronic components, the device being just one part of the application. The device by itself is neither intended to nor capable of providing the entire functionality to meet all safety-related requirements that apply to your application. Depending on the application and the corresponding risk assessment to be conducted by you, a whole variety of additional equipment is required such as, but not limited to, external encoders, external brakes, external monitoring devices, guards, etc.

As a designer/manufacturer of machines, you must be familiar with and observe all standards that apply to your machine. You must conduct a risk assessment and determine the appropriate Performance Level (PL) and/or Safety Integrity Level (SIL) and design and build your machine in compliance with all applicable standards. In doing so, you must consider the interrelation of all components of the machine. In addition, you must provide instructions for use that enable the user of your machine to perform any type of work on and with the machine such as operation and maintenance in a safe manner.

The present document assumes that you are fully aware of all normative standards and requirements that apply to your application. Since the device cannot provide all safety-related functionality for your entire application, you must ensure that the required Performance Level and/or Safety Integrity Level is reached by installing all necessary additional equipment.

⚠ WARNING

INSUFFICIENT PERFORMANCE LEVEL/SAFETY INTEGRITY LEVEL AND/OR UNINTENDED EQUIPMENT OPERATION

- Conduct a risk assessment according to EN ISO 12100 and all other standards that apply to your application.
- Use redundant components and/or control paths for all critical control functions identified in your risk assessment.
- Implement all monitoring functions required to avoid any type of hazard identified in your risk assessment, for example, slipping or falling loads.
- Verify that the service life of all individual components used in your application is sufficient for the intended service life of your overall application.
- Perform extensive commissioning tests for all potential error situations to verify the effectiveness of the safety-related functions and monitoring functions implemented, for example, but not limited to, speed monitoring by means of encoders, short circuit monitoring for all connected equipment, correct operation of brakes and guards.
- Perform extensive commissioning tests for all potential error situations to verify that the load can be brought to a safe stop under all conditions.

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

Product may perform unexpected movements because of incorrect wiring, incorrect settings, incorrect data or other errors.

▲ WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Carefully install the wiring in accordance with the EMC requirements.
- Do not operate the product with unknown or unsuitable settings or data.
- Perform a comprehensive commissioning test.

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

▲ WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop, overtravel stop, power outage and restart.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Observe all accident prevention regulations and local safety guidelines (1).
- Each implementation of the product must be individually and thoroughly tested for proper operation before being placed into service.

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

(1) For USA: 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.

Machines, controllers, and related equipment are usually integrated into networks. Unauthorized persons and malware may gain access to the machine as well as to other devices on the network/fieldbus of the machine and connected networks via insufficiently secure access to software and networks.

⚠ WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

- In your hazard and risk analysis, consider all hazards that result from access to and operation on the network/fieldbus and develop an appropriate cybersecurity concept.
- Verify that the hardware infrastructure and the software infrastructure into which the machine is integrated as well as all organizational measures and rules covering access to this infrastructure consider the results of the hazard and risk analysis and are implemented according to best practices and standards covering IT security and cybersecurity (such as: ISO/IEC 27000 series, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, IEC 62351, ISA/IEC 62443, NIST Cybersecurity Framework, Information Security Forum - Standard of Good Practice for Information Security, SE recommended Cybersecurity Best Practices*).
- Verify the effectiveness of your IT security and cybersecurity systems using appropriate, proven methods.

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

(*) : SE Recommended Cybersecurity Best Practices can be downloaded on SE.com.

⚠ WARNING

LOSS OF CONTROL

Perform a comprehensive commissioning test to verify that communication monitoring properly detects communication interruptions.

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

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the [Cybersecurity Best Practices](#) document.

Schneider Electric provides additional information and assistance:

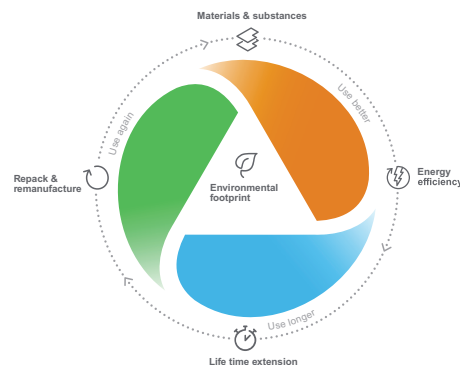
- Subscribe to the [Schneider Electric security newsletter](#).
- Visit the [Cybersecurity Support Portal](#) web page to:
 - Find Security Notifications.
 - Report vulnerabilities and incidents.
- Visit the [Schneider Electric Cybersecurity and Data Protection Posture](#) web page to:
 - Access the cybersecurity posture.
 - Learn more about cybersecurity in the cybersecurity academy.
 - Explore the cybersecurity services from Schneider Electric.

Environmental Data

The Environmental Data Program is a framework for how we measure, categorize, and compare the environmental attributes and footprint of our products.

Using a rigorous, fact-based methodology, the program provides environmental data from across the product lifecycle.

Five data categories across the product lifecycle



Use Better: How sustainable a product is, including environmental footprint, materials and substances, packaging, and energy efficiency.

Use Longer: How a product's life time can be effectively extended in terms of reparability and updatability.

Use Again: How a product can be reused, from dismantling and remanufacturing to recyclability and manufacturer take back.

With this transparent, verified data, customers and partners are empowered to make conscious environmental choices and accurately evaluate and report on sustainability performance.

All our hardware offers have an associated environmental data available on [se.com](#) product pages.

Refer to [Environmental Data Program](#) for more information.

Related Documents

Use your tablet or your PC to quickly access detailed and comprehensive information on all our products on [www.se.com](#).

The internet site provides the information you need for products and solutions:

- The whole catalog for detailed characteristics and selection guides,
- The CAD files to help design your installation, available in over 20 different file formats,
- All software and firmware to maintain your installation up to date,

- A large quantity of White Papers, Environment documents, Application solutions, Specifications... to gain a better understanding of our electrical systems and equipment or automation,
- And finally all the User Guides related to your drive, listed below:

Title of Documentation	Reference Number
Catalog: Altivar Building ATH200	DIA2ED2250901EN (English) DIA2ED2250901FR (French)
ATH200 Getting Started	JPS43191 (English), JPS43192 (French), JPS43193 (German), JPS43194 (Spanish) JPS43198 (Italian), JPS43199 (Chinese), JPS43197 (Portuguese), JPS43195 (Turkish)
ATH200 Getting Started Annex (SCCR)	JPS43196 (English)
ATH200 Installation manual	JPS43203 (English), JPS43204 (French), JPS43202 (German), JPS43201 (Spanish), JPS43200 (Italian), JPS43208 (Chinese), JPS43205 (Portuguese), JPS43209 (Turkish)
ATH200 Programming manual	JPS43207 (English), JPS43206 (French), JPS43212 (German), JPS43211 (Spanish), JPS43210 (Italian), JPS43213 (Chinese), JPS43214 (Portuguese), JPS43215 (Turkish)
ATH200 ATEX manual	JPS43218 (English)
ATH200 Modbus manual	JPS43217 (English)
ATH200 BACnet manual	JPS43216 (English)
ATH200 Communication Parameters	JPS43219 (English)
ATH200 Safety Functions manual	JPS43226 (English), JPS43227 (French), JPS43229 (German), JPS43233 (Spanish), JPS43231 (Italian), JPS43232 (Chinese)
ATH200 - ATV Logic manual	JPS43234 (English), JPS43230 (French), JPS43236 (German), JPS43238 (Spanish), JPS43237 (Italian), JPS43235 (Chinese)
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)
ATH200: DTM	ATH200 DTM Library EN (English – to be installed first) ATH200 DTM Lang IT (Italian) ATH200 DTM Lang FR (French) ATH200 DTM Lang DE (German) ATH200 DTM Lang SP (Spanish) ATH200 DTM Lang CN (Chinese)
Recommended Cybersecurity Best Practices	CS-Best-Practices-2019-340 (English)

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

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Terminology used in this document

The technical terms, terminology, and the corresponding descriptions in this manual normally use the terms or definitions in the relevant standards.

Among others, these standards include:

- ISO 13849: The Foundation of Functional Safety in the Machinery
- IEC 60204-1: Safety of machinery - Electrical equipment of machines – Part 1: General requirements.
- IEC 61010: Safety requirements for electrical equipment for measurement, control, and laboratory use.
- IEC 61158 series: Industrial communication networks - Fieldbus specifications
- IEC 61508 Ed.2 series: Functional safety of electrical/electronic/programmable electronic safety-related.
- IEC 61784 series: Industrial communication networks - Profiles.
- IEC 61784-5-3: Industrial communication networks - Profiles - Part 5-3: Installation of fieldbuses - Installation profiles for CPF 3
- IEC 61800 series: Adjustable speed electrical power drive systems.
- IEC 61918: Industrial communication networks - Installation of communication networks in industrial premises.
- IEC 62443: Security for industrial automation and control systems.

In the area of drive systems this includes, but is not limited to, terms such as **error**, **error message**, **failure**, **fault**, **fault reset**, **protection**, **safe state**, **safety function**, **warning**, **warning message**, and so on.

In addition, the term **zone of operation** is used in conjunction with the description of specific hazards, and is defined as it is for a **hazard zone** or **danger zone** in the EC Machinery Directive (2006/42/EC) and in ISO 12100-1.

Contact us

Select your country on www.se.com/contact.

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

Hardware Setup

What's in This Part

BACnet MSTP Network Configurations	15
BACnet IP Network Configurations	18

BACnet MSTP Network Configurations

Modbus VP12S / BACnet MSTP Port usage

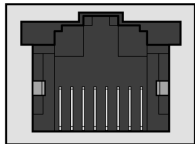
To use the port with the BACnet MSTP configuration, use the parameter

[Embedded Protocol] `C o n` ([Communication] `C o n` → [Emb Serial Line] `S P C -`) and select [Bacnet MS/TP] `E b n`, then reboot the product.

NOTE: The product needs to be rebooted to take the modification into account.

RJ45 connector

The table describes the pin out of the RJ45 connector of the device:



8 7 6 5 4 3 2 1

Pin	Signal
1	Reserved
2	
3	
4	D1 ⁽¹⁾
5	D0 ⁽¹⁾
6	Reserved
7	VP, 10 Vdc ⁽²⁾
8	Common ⁽¹⁾
⁽¹⁾ Modbus signals	
⁽²⁾ Supply for RS232 / RS485 converter or a remote terminal	

Modbus adaptor cable — LV434211

Use the cable Modbus adaptor cable LV434211.



RS485 Bus Schematic

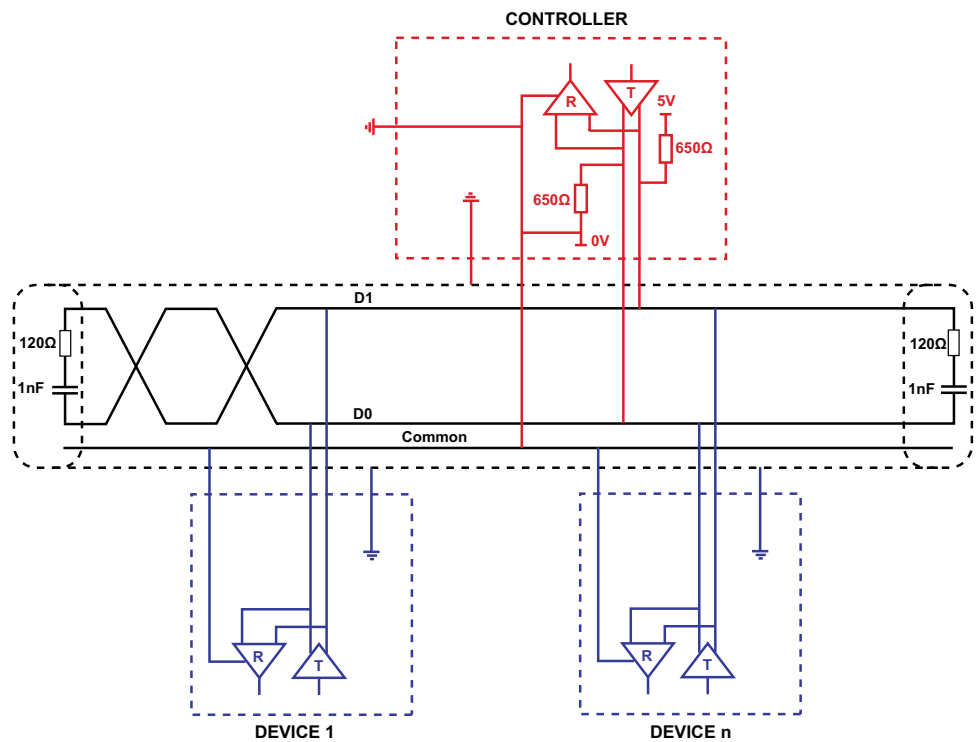
The RS485 standard allows variants of different characteristics:

- Polarization
- Line terminator
- Distribution of a reference potential
- Number of devices
- Length of bus

The Modbus specification published on the Modbus.org site contains precise details of all these characteristics. They are also summarized in standard schematic section. The new Schneider Electric devices conform to this specification.

Schematic Diagram

The following is the RS485 bus schematic diagram:



Characteristic	Definition
Type of cable	Twisted-pair, copper wire, tinned
Shield	Braid
Maximum length of bus	1000 m at 19200 bps
Maximum number of stations (without repeater)	32 stations that are 31 devices
Maximum length of tap links	<ul style="list-style-type: none"> • 20 m for 1 tape link • 40 m divided by the number of tape links on a multiple junction box
Bus polarization	<ul style="list-style-type: none"> • One 450...650 Ω pull-up resistor at 5 V (650 Ω recommended) • One 450...650 Ω pull-down resistor at the common (650 Ω recommended) <p>This polarization is recommended for the controller.</p>
Velocity of propagation	78%
Capacitance	<p>< 41.0105 pF/m (12.5 pF/ft) between conductors</p> <p>< 72.1784 pF/m (22 pF/ft) between the conductor connected to ground and the next conductor</p>
Line termination	<p>Two polarization of the pair are available with a R or RC circuit as line termination:</p> <ul style="list-style-type: none"> • R circuit: One 150Ω resistor. • RC circuit: One 120Ω 0.25W resistor in series with 1nF 10V capacitor. <p>NOTE: An analysis is to be carried out to determine which solution is best suited for the network topology.</p>
Common polarity	<p>The Common circuit (Signal and optional Power Supply Common) must be connected directly to protective ground, at one point only for the entire bus on the controller side.</p>

BACnet IP Network Configurations

BACnet Fieldbus Module

The following figure shows the VW3A3726 BACnet module:



Firmware version

The VW3A3726 BACnet IP module is compatible with, at least, V1.0 software version.

Modbus TCP Requests

⚠ WARNING

LOSS OF CONTROL

Do not control the drive via Modbus TCP when using the VW3A3726 BACnet IP module.

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

Before Starting

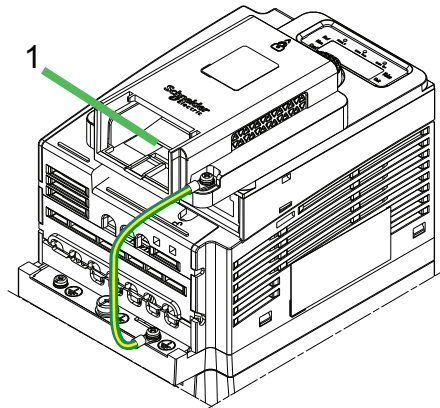
Check that the module catalog number marked on the label is the same as that on the delivery note corresponding to the purchase order.

Remove the fieldbus module from its packaging and check that it has not been damaged in transit.

Insertion of the Fieldbus Module

The table provides the procedure for insertion of the VW3A3726 BACnet module in the drive:

Step	Action
1	Ensure that the power is off.
2	Locate the fieldbus module slot (1).
3	Insert the module.
4	Check that the module is correctly inserted and locked mechanically in the drive.



1 Slot A

Removal of the Fieldbus Module

The table provides the procedure for removal of the VW3A3726 BACnet module from the drive:

Step	Action
1	Ensure that the power is off.
2	Press the strip.
3	Remove the module while maintaining the strip pressed,

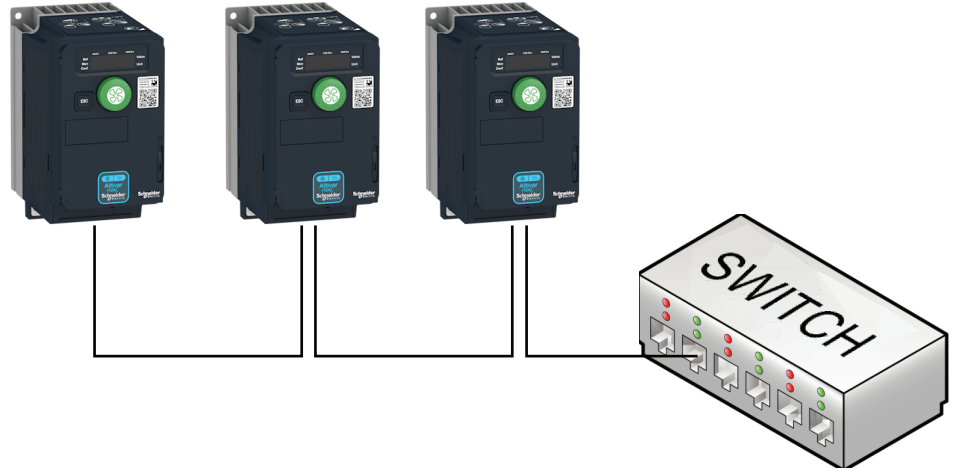
Cable Specifications

Cables used to should conform to a network cable Cat 5e (UTP/FTP) with shielded.

Installation Topology

Daisy chain topology is the recommended topology to use on BACnet IP networks. Star and ring networks are not supported.

Daisy chain configurations consist of a single cable that is routed to the first BACnet IP device, the next device, and so on, in the sequence.



Cyber Security

What's in This Part

Overview	22
Defense in depth measures expected in the environment	23
Security Policy	25
Potential Risks and Compensating Controls	26
Account Management Guidelines	28

Overview

Cyber Security is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions.

The objective of Cyber Security is to help provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.

No single Cyber Security approach is adequate. Schneider Electric recommends a defense-in-depth approach. Conceived by the **National Security Agency (NSA)**, this approach layers the network with security features, appliances, and processes.

The basic components of this approach are:

- Risk assessment
- A security plan built on the results of the risk assessment
- A multi-phase training campaign
- Physical separation of the industrial networks from enterprise networks using a demilitarized zone (DMZ) and the use of firewalls and routing to establish other security zones
- System access control
- Device hardening
- Network monitoring and maintenance

This chapter defines the elements that help you configure a system that is less susceptible to cyber attacks.

For detailed information on the defense-in-depth approach, refer to the TVDA: **How Can I Reduce Vulnerability to Cyber Attacks in the Control Room (STN V2)** on the Schneider Electric website.

To submit a Cyber Security question, report security issues, or get the latest news from Schneider Electric, visit the Schneider Electric website.

Defense in depth measures expected in the environment

Machines, controllers, and related equipment are usually integrated into networks. Unauthorized persons and malware may gain access to the machine as well as to other devices on the network/fieldbus of the machine and connected networks via insufficiently secure access to software and networks.

▲ WARNING
<p>UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS</p> <ul style="list-style-type: none"> • In your hazard and risk analysis, consider all hazards that result from access to and operation on the network/fieldbus and develop an appropriate cybersecurity concept. • Verify that the hardware infrastructure and the software infrastructure into which the machine is integrated as well as all organizational measures and rules covering access to this infrastructure consider the results of the hazard and risk analysis and are implemented according to best practices and standards covering IT security and cybersecurity (such as: ISO/IEC 27000 series, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, IEC 62351, ISA/IEC 62443, NIST Cybersecurity Framework, Information Security Forum - Standard of Good Practice for Information Security, SE recommended Cybersecurity Best Practices*). • Verify the effectiveness of your IT security and cybersecurity systems using appropriate, proven methods. <p>Failure to follow these instructions can result in death, serious injury, or equipment damage.</p>

(*) : SE Recommended Cybersecurity Best Practices can be downloaded on SE.com.

Additionally, use a layered network approach with multiple security and defense controls in your IT and control system to minimize data protection gaps, reduce single-points of failure and create a strong cybersecurity posture. The more layers of security in your network, the harder it is to breach defenses, take digital assets or cause disruption.

Control System - Cybersecurity policy

- Cybersecurity governance – available and up-to-date guidance on governing the use of information and technology assets in your company that is matching with a dedicated risk analysis about the control system
- The access control policy defined in the cybersecurity governance is strictly applied. In particular, it guarantees the authenticity of privileged operations. For example operations that can alter the critical assets.
- The instructions and procedures should structure the roles and responsibilities in terms of security within the organization; in other words, who is authorized to perform what and when. These should be known by the users.
- Define information security continuous monitoring (ISCM) to maintain the awareness of information security, vulnerabilities and threats to your organization.
- Perform patch management by applying security patches from vendor to ensure stability and completeness.

Physical perimeter security

- Set up the devices in an enclosed area with physical access control to prevent unauthorized access to the device, with dedicated monitoring

Physical network segmentation

Independence from non-control system networks – the control system provides network services to control system networks, critical or non-critical, without a connection to non-control system networks

- Physically segment control system networks from non-control system network
- Physically segment critical control system networks from non-critical control system networks

Logical isolation of critical networks

The control system provides the capability to logically and physically isolate critical control system networks from non-critical control system networks. For example, using VLANs.

Zone boundary protection – the control system provides the capability to:

- Manage connections through managed interfaces consisting of appropriate boundary protection devices, such as: proxies, gateways, routers, firewalls, and encrypted tunnels
- Use an effective architecture, for example, firewalls protecting application gateways residing in a DMZ
- Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site, for example, data centers

No public internet connectivity – access from the control system to the internet is not recommended

Information disclosure prevention

- Encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution
- Reduce access to control system information by distributing permissions according to predefined access control with least privilege practices

Control against malware

- Detection, prevention, and recovery controls to help protect against malware are implemented and combined with appropriate user awareness
- Any computer in use on the control system either on premise or temporarily connected, should have an updated anti-virus, anti-malware, anti-ransomware application activated during the use

Resource & control system availability

- Help to ensure continuity of service – ability to break the connections between different network segments or use duplicate devices in response to an incident, redundancy of controllers or network device like switches or similar solution.
- Manage communication loads – the control system provides the capability to manage communication loads to mitigate the effects of information flooding types of DoS (Denial of Service) events
- Manage the retention cycles of data and programs with the retention periods determined as appropriate.

Security Policy

The device does not have the capability to transmit data encrypted using the following protocols: Modbus serial, Modbus TCP, Bacnet IP and Bacnet MS/TP. If other users gained access to your network, transmitted information can be disclosed or subject to tampering.

▲ WARNING

CYBERSECURITY HAZARD

- For transmitting data over an internal network, physically or logically segment the network, the access to the internal network needs to be restricted by using standard controls such as firewalls.
- For transmitting data over an external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.

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

Any computer using SoMove/DTM should have an updated anti-virus, anti-malware, anti-ransomware application activated during the use.

The ATH230 has the capability to export its settings and files manually or automatically. It is recommended to archive any settings and files (device configuration) in a secure area.

Potential Risks and Compensating Controls

Address potential risks using these compensating controls:

Area	Issue	Risk	Compensating controls
User accounts.	Default account settings are often the source of unauthorized access by malicious users.	If you do not change default password or disable the user access control, unauthorized access can occur.	Help to ensure user access control is enabled on all the communication ports and change the default passwords to help reduce unauthorized access to your device.
Secure protocols.	The device does not have the capability to transmit data encrypted using these protocols: <ul style="list-style-type: none"> • Bacnet MS/TP • Bacnet IP • Modbus TCP • Modbus serial 	If a malicious user gained access to your network, they could intercept communication.	For transmitting data over internal network, physically or logically segment your network. For transmitting data over external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.

Data Flow Restriction

To secure the access to the drive and limit the data flow, the use of a firewall device is required.

Firewall Product

The Firewall is a security appliance that provides levels of protection against cyber threats for industrial networks, automation systems, SCADA systems, and process control systems.

This Firewall is designed to permit or deny communications between devices connected to the external network connection of the Firewall and the protected devices connected to the internal network connection.

The Firewall can restrict network traffic based on user defined rules that would permit only authorized devices, communication types and services.

The Firewall includes built-in security modules and an off-line configuration tool for creating secure zones within an industrial automation environment.

Backing-up and Restoring the Software Configuration

To protect your data, Schneider Electric recommends backing-up the device configuration and keeping your backup file in a secure place. The backup is available in the device DTM, using **load from device** and **store to device** functions.

Remote Access to the Drive

When remote access is used between a device and the drive, help to ensure your network is secure (VPN, Firewall...).

Machines, controllers, and related equipment are usually integrated into networks. Unauthorized persons and malware may gain access to the machine as well as to other devices on the network/fieldbus of the machine and connected networks via insufficiently secure access to software and networks.

▲ WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

- In your hazard and risk analysis, consider all hazards that result from access to and operation on the network/fieldbus and develop an appropriate cybersecurity concept.
- Verify that the hardware infrastructure and the software infrastructure into which the machine is integrated as well as all organizational measures and rules covering access to this infrastructure consider the results of the hazard and risk analysis and are implemented according to best practices and standards covering IT security and cybersecurity (such as: ISO/IEC 27000 series, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, IEC 62351, ISA/IEC 62443, NIST Cybersecurity Framework, Information Security Forum - Standard of Good Practice for Information Security, SE recommended Cybersecurity Best Practices*).
- Verify the effectiveness of your IT security and cybersecurity systems using appropriate, proven methods.

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

(*) : SE Recommended Cybersecurity Best Practices can be downloaded on SE.com.

Deactivation of Unused Functions

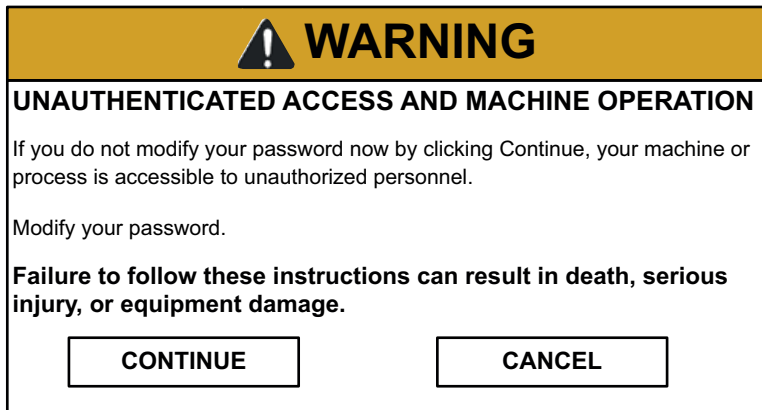
To avoid unauthorized access, it is advisable to deactivate unused functions.

Account Management Guidelines

The ATH200 password must contain:

- A total of eight characters
- At least one upper-case letter
- At least one lower-case letter
- At least one special character (for example, @, #, \$)
- No blank character

The figure below displays the first connection a dialog box requiring the modification of the default password. This dialog box continues to be displayed until a password is defined.



Schneider Electric recommends to:

- Modify the password every 90 days
- Use a dedicated password (not related to your personal password)

NOTE: No responsibility is assumed by Schneider Electric for any consequences if anyone hacks your product password and if you use the same password for personal usage.

Software Setup

What's in This Part

Software Overview	30
BACnet MS/TP parameters	33
BACnet IP parameters	37
[User authentication] SEC- menu	44

Software Overview

About BACnet

BACnet fieldbus was developed by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers, INC. (ASHRAE).

This fieldbus allows integration of devices from different manufacturers in building automation control systems.

Within BACnet, it is possible to display and configure device properties in the same way.

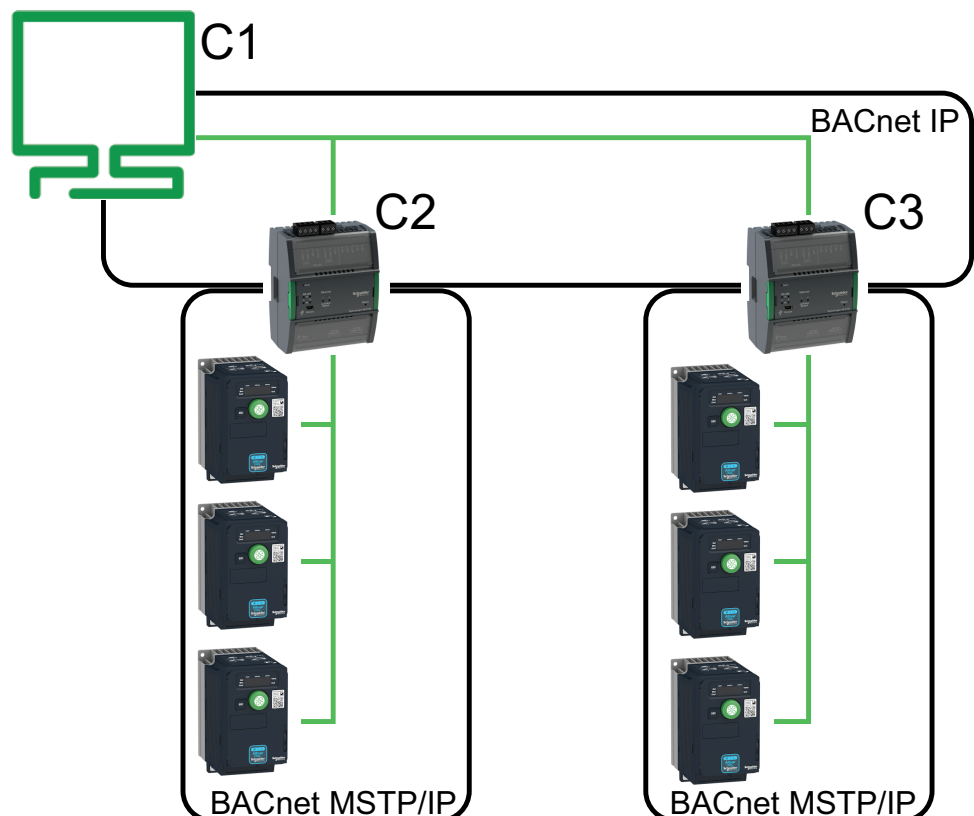
What Is a BACnet Network

A BACnet network is a transport (LAN or WAN) that carries data from device to device, within a network and between networks. A BACnet network can be a high-speed backbone network:

- Ethernet
- BACnet/IP

It can also be a fieldbus network

- Manager-Subordinate/Token-Passing (BACnet MS/TP)
- ARCNET
- LonTalk

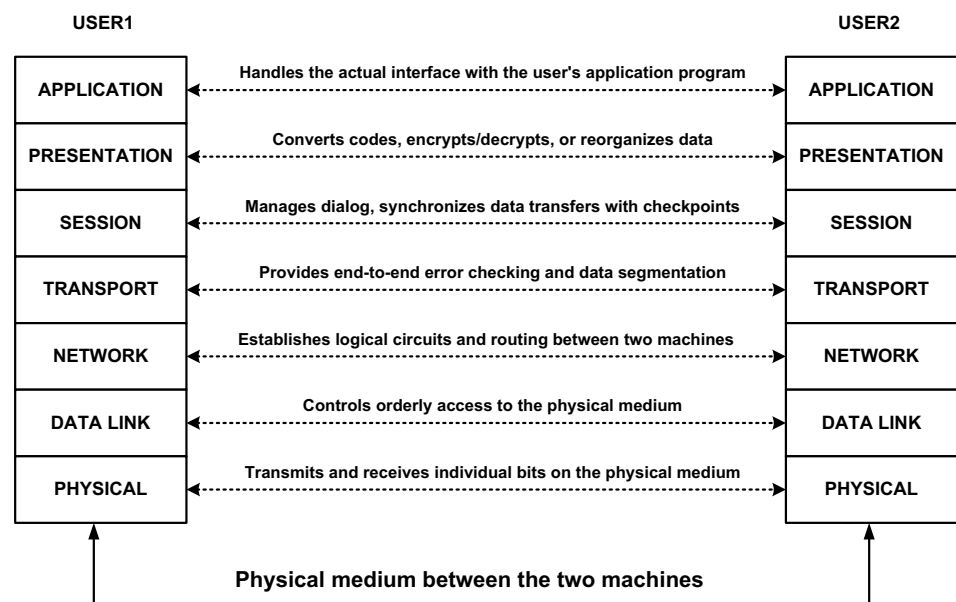


BACnet protocol architecture — following ISO 16484-5

The Open System Interconnection (OSI) - Basic Reference Model (ISO 7498) is an international standard that defines a model for developing multi-vendor computer communication protocol standards. The OSI model addresses the general problem of computer-to-computer communication and breaks this very complex problem into seven smaller, more manageable sub-problems, each of which concerns itself with a specific communication function. Each of these subproblems forms a "layer" in the protocol architecture.

The seven layers are arranged in a hierarchical fashion as shown in Figure "The ISO Open Systems Interconnection Basic Reference Model". A given layer provides services to the layers above and relies on services provided to it by the layers below. Each layer can be thought of as a black box with carefully defined interfaces on the top and bottom. An application process connects to the OSI application layer and communicates with a second, remote application process. This communication appears to take place between the two processes as if they were connected directly through their application layer interfaces. Minimal knowledge or understanding of the other layers is required. In a similar manner, each layer of the protocol relies on lower layers to provide communication services and establishes a virtual peer-to-peer communication with its companion layer on the other system. The only real connection takes place at the physical layer.

The ISO Open Systems Interconnection Basic Reference Model



The OSI model addresses computer-to-computer communication from a very general perspective. It was designed to deal with the problems associated with computers in large, complex networks communicating with other computers in networks anywhere in the world. In this environment, computers can be separated by long distances and the messages might pass through several intermediate points, each of which may have to make routing decisions or perform some type of translation. Complex synchronization and error recovery schemes may also be needed.

The cost of implementing such a protocol today is prohibitively high for most building automation applications and is not generally required. Nevertheless, the OSI model is a good one to use for a building automation protocol if consideration is given to including only the OSI functionality that is actually needed, thereby collapsing the seven-layer architecture. In a collapsed architecture, only selected layers of the OSI model are included. The other layers are effectively null, thus reducing message length and communication processing overhead. Such a collapsed architecture permits the building automation industry to take advantage of lower cost, mass-produced processor and local area network technologies such

as have been developed for the process control and office automation industries. The use of readily available, widespread technologies, such as Ethernet, ARCNET, and LonTalk, will lower the cost, increase performance, and open new doors to system integration.

The BACnet Collapsed Architecture — following ISO 16484-5

BACnet is based on a four-layer collapsed architecture that corresponds to the physical, data link, network, and application layers of the OSI model as shown in table “BACnet collapsed architecture”. The application layer and a simple network layer are defined in the BACnet standard. BACnet provides the following options that correspond to the OSI data link and physical layers.

Collectively these options provide a manager/subordinate MAC, deterministic token-passing MAC, high-speed contention MAC, dial-up access, Internet access, star and bus topologies, and a choice of twisted-pair, coax, or fiber optic media, in addition to wireless connectivity.

A four-layer collapsed architecture was chosen after careful consideration of the particular features and requirements of BAC networks, including a constraint that protocol overhead needed to be as small as possible. The reasoning behind the selection of the physical, data link, network, and application layers for inclusion in the BACnet architecture is outlined in this clause.

BAC networks function as local area networks, either physically, as with MS/TP, or logically, as with BACnet/IP. This is true even though in some applications it is necessary to exchange information with devices in a building that is very far away. This long-distance communication is done through the telephone networks or across the Internet. The routing, relaying, and guaranteed delivery issues are handled by the telephone and Internet systems and can be considered external to the BAC network. BAC devices are static. They don't move from place to place and the functions that they are asked to perform do not change in the sense that a manufacturing device may make one kind of part today and some very different part tomorrow. These are among the features of BAC networks that can be used to evaluate the appropriateness of the layers in the OSI model.

BACnet collapsed architecture

BACnet Layers								Equivalent OSI Layers
BACnet Application Layer								Application
BACnet Network Layer								Network
ISO 8802-2 (IEEE 802.3)	MS/TP	PTP	LonTalk	BACnet Virtual Link Layer	BACnet Data Link Layer	Secure Connect	BACnet Virtual Link Layer	Data Link
ISO 8802-3 (IEEE 802.3)	ARCNET	EIA-485	EIA-232	IPv4	IPv6	Zigbee	Web-Socket	Physical
VW3A3726		MSTP Embedded						

BACnet MS/TP parameters

Switch mode between Modbus and BACnet MS/TP

The parameters are accessible in the **[Communication] C o n -**  **[Emb Serial Line] S P C -**.

The parameter **[Embedded Protocol] C o n** defines the Serial fieldbus switch mode.

The list presents the parameter settings:

- **[Bacnet MS/TP] E b n**
- **[Modbus] n d b**

To be take into account, apply a power cycle of the product.

Access

The parameters are accessible in the **[Communication] C o n -**  **[Bacnet MS/TP] E b n -** menu.

Note

- When BACnet MS/TP is enabled, the keypad is unavailable and SoMove cannot connect.

[MS/TP Address] b A d r

This parameter defines the BACnet MS/TP subordinates address of the drive.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
0...127	0... 1 2 7	0	R/W	16#7210 = 29200

[MS/TP Baudrate] b b d r

This parameter defines the BACnet MS/TP baud rate.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[Automatic]	<i>A u t o</i>	[Automatic]	R/W	16#7211 = 29201
[9600 bsp]	<i>9 6 0 0</i>			
[19200 bps]	<i>1 9 2 0 0</i>			
[38.4 Kbps]	<i>3 8 4 0 0</i>			
[76.8 Kbps]	<i>7 6 8 0 0</i>			

[MS/TP Frame Format] *b F o r*

This parameter displays the BACnet MS/TP frame format.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[8-N-1]	<i>B n l</i>	[8-N-1]	R	16#7212 = 29202

[MS/TP Timeout] *b t L P*

This parameter defines the BACnet MS/TP fieldbus timeout.

NOTE: A [Mdb Com Interrupt] *5 L F l* error is triggered if the fieldbus module does not received any BACnet messages at its address within a defined time period defined by [MS/TP Timeout] *b t L P* parameter.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0.1...60.0 s]	<i>l ... 6 0 0</i>	4.0 s	R/W	16#7213 = 29203

[MS/TP Inst Nb High] *b i n H*

This parameter defines the BACnet MS/TP device instance number.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...4194]	<i>0 ... 4 1 9 4</i>	1	R/W	16#7214 = 29204

[MS/TP Inst Nb Low] *b i n L*

This parameter defines the BACnet MS/TP device instance number.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...999]	<i>0 ... 9 9 9</i>	1	R/W	16#7215 = 29205

[MS/TP Max Master Nb] *b n n n*

This parameter defines the max manager device address on the BACnet MS/TP subnetwork.

NOTE: It is recommended to set [MS/TP Max Master Nb] to [MS/TP Address] + 1.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...127]	<i>l ... 1 2 7</i>	1	R/W	16#7217 = 29207

[MS/TP Max info frame] *b P , F*

This parameter defines the maximum number of frames that can be send before passing token to the next manager.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...100]	<i>1... 100</i>	10	R/W	16#7218 = 29208

[MS/TP APDU Retries] *R P d r*

This parameter displays the number of retries on APDU packets.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...10]	<i>1... 10</i>	3	R	16#7228 = 29224

[MS/TP APDU Timeout] *R P d t*

This parameter displays the timeout on APDU send before a resend is executed.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...100 s]	<i>1... 100</i>	60 s	R	16#7229 = 29225

[MS/TP Rx frame count] *b t F r*

This parameter displays the total number of received frames.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...65535]	<i>0... 65535</i>	–	R	16#7219 = 29209

[MS/TP Tx frame count] *b t F S*

This parameter displays the total number of transmitted frames.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...65535]	<i>0... 65535</i>	–	R	16#721A = 29210

[MS/TP Error Frames] 𐀀 𐀁 𐀂 𐀃

This parameter displays the total number of incorrect frames received.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...65535]	𐀀 ... 𐀁 𐀂 𐀃 𐀄 𐀅 𐀆 𐀇 𐀈 𐀉	–	R	16#721B = 29211

BACnet IP parameters

Access

The parameters are accessible in the **[Communication] C o n -**  **[Comm module] C b d -** menu.

[Device Name] P A n n

This parameter is used to set the device name.

[MAC @] n n c

This parameter displays the MAC address of the BACnet IP port in the format **[MM-MM-MM-XX-XXXX]**.

[IP mode] , P n

This parameter is used to select the IP address assignment method.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
<ul style="list-style-type: none"> [Fixed] : Manually set the IP address. [DHCP] : Automatically gets the IP address from the DHCP server using the device name. 	<ul style="list-style-type: none"> n n n n d H C P 	[DHCP]	R/W	16#FBC2 = 64250

[IP address] , P c 1, , P c 2, , P c 3, , P c 4

This parameter is used to set the IP address and can be edited only when the IP mode is set to fixed address.

The modification of this parameter setting is only effective when you restart the drive if **[IP mode] , P n** is set to **[Fixed] n n n n**.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R/W	, P c 1: 16#FAD4 = 64212 , P c 2: 16#FAD5 = 64213 , P c 3: 16#FAD6 = 64214 , P c 4: 16#FAD7 = 64215

[Mask] ,P01, ,P02, ,P03, ,P04

This parameter can be edited only when the IP mode is set to fixed address.

The modification of this parameter setting is only effective when you restart the drive if **[IP mode] ,P0** is set to **[Fixed] 0000**.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R/W	,P01 : 16#FAD8 = 64216 ,P02 : 16#FAD9 = 64217 ,P03 : 16#FADA = 64218 ,P04 : 16#FADB = 64219

[Gateway] ,PG1, ,PG2, ,PG3, ,PG4

This parameter can be edited only when the IP mode is set to fixed address.

The modification of this parameter setting is only effective when you restart the drive if **[IP mode] ,P0** is set to **[Fixed] 0000**.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R/W	,PG1 : 16#FADC = 64220 ,PG2 : 16#FADD = 64221 ,PG3 : 16#FADE = 64222 ,PG4 : 16#FADF = 64223

[MonitorIPAddress] IPA1, IPA2, IPA3, IPA4

This parameter can be accessed only when **[IP mode] ,P0** is set to fixed address.

This is the current IP setting taken into account by the drive.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R/W	IPA1 : 16#FAFC = 64252 IPA2 : 16#FAFD = 64253 IPA3 : 16#FAFE = 64254 IPA4 : 16#FAFF = 64255

[MonitorIPMask] IPS1, IPS2, IPS3, IPS4

This parameter can be accessed only when [IP mode] *IP* is set to fixed address.

This is the current IP Mask.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R	IPS1: 16#FB00 = 64256 IPS2: 16#FB01 = 64257 IPS3: 16#FB02 = 64258 IPS4: 16#FB03 = 64259

[MonitorIPGateway] IPT1, IPT2, IPT3, IPT4

This parameter can be accessed only when [IP mode] *IP* is set to fixed address.

This is the current IP Gateway obtained from the network.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R	IPT1: 16#FB04 = 64260 IPT2: 16#FB05 = 64261 IPT3: 16#FB06 = 64262 IPT4: 16#FB07 = 64263

[Bacnet IP Mode] *BAIP*

This parameter defines the BACnet IP manager mode.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[Bacnet Normal]	<i>norIP</i>	[Bacnet Normal]	R/W	16#FB23 = 64291
[Bacnet Foreign]	<i>ForE</i>			

[Bacnet IP UDP port] *BAIPU*

This parameter defines the BACnet IP UDP port.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...65535]	<i>1...65535</i>	[47808]	R/W	16#FB24 = 64292

[Bacnet IP Time-Out] *b A t t*

This parameter defines the BACnet IP fieldbus timeout.

NOTE: A [Fdbus Com Interrupt] *L n F* error is triggered if the fieldbus module does not received any BACnet messages at its address within a defined time period defined by [Bacnet IP Time-Out] *b A t t* parameter.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...60.0 s]	<i>l... 6 0 0</i>	4.0 s	R/W	16#FB26 = 64294

[Bacnet Instance High] *b A o H*

This parameter defines the BACnet IP device instance number.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...4194]	<i>0... 4 1 9 4</i>	1	R/W	16#FB22 = 64290

[Bacnet Instance Low] *b A o L*

This parameter defines the BACnet IP device instance number.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...999]	<i>0... 9 9 9</i>	1	R/W	16#FB21 = 64289

[IP APDU Retries] *A P r ,*

This parameter displays the number of retries on APDU packets.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...10]	<i>l... 1 0</i>	3	R	16#FB27 = 64295

[IP APDU Timeout] *A P t ,*

This parameter displays the timeout on APDU send before a resend is executed.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...100 s]	<i>l... 1 0 0</i>	60 s	R	16#FB2A = 64298

[APDU Seg Timeout] *RP5* ,

This parameter displays the segment timeout on APDU send before a resend is executed.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1...100 s]	<i>1... 100</i>	50 s	R	16#FB2A = 64298

Monitoring of Communication Channel

Communication channels are monitored if they are involved in one of the following parameters:

- The control word (**[Cmd Register] CMD**) from the active command channel
- The control word containing the command switch (bit configured on **[Command Switching] CCS**)
- The control word containing the switch for reference value 1'1B (bit configured on **[Ref 1B switching]**).
- The control word containing the switch for reference value 1'2 (bit configured on **[Freq Switch Assign]**).
- The reference frequency or reference speed (**[Ref Frequency]** or **[Speed Setpoint]**: Nominal speed value) from the active channel for reference value.
- Summing reference frequency or reference speed (**[Ref Frequency]** or **[Speed Setpoint]**: Nominal speed value) 2 (assigned to **[Summing Input 2]**).
- Summing reference frequency or reference speed (**[Ref Frequency]** or **[Speed Setpoint]**: Nominal speed value) 3 (assigned to **[Summing Input 3]**).
- Subtracting reference frequency or reference speed (**[Ref Frequency]** or **[Speed Setpoint]**: Nominal speed value) 2 (assigned to **[Subtract Ref Freq 2]**).
- Subtracting reference frequency or reference speed (**[Ref Frequency]** or **[Speed Setpoint]**: Nominal speed value) 3 (assigned to **[Subtract Ref Freq 3]**).
- The reference value given by the PID controller (**[PID Set Point]**).
- The PID controller feedback (**[AI Virtual 1]**).
- The multiplication coefficient of the reference values (**[Multiplying coeff.]** 2 (assigned to **[Ref Freq 2 Multiply]**).
- The multiplication coefficient of the reference values (**[Multiplying coeff.]** 3 (assigned to **[Ref Freq 3 Multiply]**).
-

As soon as one of these parameters has been written once to a communication channel, it activates monitoring for that channel.

If a communication warning is sent (in accordance with the protocol criteria) by a monitored port or fieldbus module, the drive triggers a communication interruption.

The drive reacts according to the communication interruption configuration (operating state Fault, maintenance, fallback, and so on).

If a communication warning occurs on a channel that is not being monitored, the drive does not trigger a communication interruption.

Enabling of Communication Channels

A communication channel is enabled once one parameter involved has been written at least one time. The drive is only able to start if the channel involved in command and reference value are enabled.

Example:

A drive in CIA DSP402 profile is connected to an active communication channel.

It is mandatory to write at least one time the reference value and the command in order to switch from *4-Switched on* to *5-Operation enabled* state.

A communication channel is disabled in *forced local* mode.

On exiting *forced local* mode:

- The drive copies the `run` commands, the direction, and the forced local reference value to the active channel (maintained).
- Monitoring of the active channels for the command and reference value resumes following a time delay [**Time-out forc. local**]. After this time if command channel not valid, [**Mdb Com Interrupt**] `SLF1` or [**Fdbus Com Interrupt**] `CNF` is trigger.
- Drive control only takes effect once the drive has received the reference and the command from the active channels.

Command and Reference Channels

All the drive command and reference parameters are managed on a channel-by-channel basis.

Parameter Name	Parameter Code		
	Taken Into Account by the Drive	Embedded	BACnet IP
Control word	<code>CNd</code>	<code>CNdI</code>	<code>CNdE</code>
Extended control word	<code>CNi</code>	<code>CNiI</code>	<code>CNiE</code>
Reference speed (rpm)	<code>LFr d</code>	<code>LFr I</code>	<code>LFr E</code>
Reference frequency (0.1 Hz)	<code>LFr</code>	<code>LFr I</code>	<code>LFr E</code>
Reference for torque control mode (0.1% of the normal torque)	<code>LEr</code>	<code>LEr I</code>	<code>LEr E</code>
Reference value supplied by PI controller	<code>PiSP</code>	<code>PiRI</code>	<code>PiRE</code>
Reference value supplied by analog multiplier function	<code>PFr</code>	<code>PFr I</code>	<code>PFr E</code>

[User authentication] SEC- menu

About This Menu

This menu is accessible in **[Communication]** COM- → **[Comm module]** CBD- menu via the graphic display terminal if the BACnet IP module has been inserted. The content of this menu can also be accessed via the commissioning software.

The following parameter is used to enable or disable the user authentication to access your drive through PC software tools.

NOTE: The user authentication is a feature provided to help prevent unauthorized and malicious connection to the device. The access to the connected device via a software tool provided by Schneider Electric (such as SoMove) is restricted. For more information, refer to the DTM online help.

Possible Settings – [User Authentication] SPOL

This parameter is used to enable or disable the user authentication feature.

Disabling this feature, no credentials will be required to access your process or machine. This setting is saved with the configuration and will be active if a configuration is loaded or copied.

⚠ WARNING

UNAUTHENTICATED ACCESS AND MACHINE OPERATION

Do not disable the feature if your machine or process is accessible to unauthorized personnel either directly or via a network.

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

Set **[User Authentication]** SPOL to:

- **[No]** NO to disable User authentication.
Connection to PC software tools provided by Schneider-Electric (such as SoMove FDT / DTM) is unlocked.
- **[Yes]** YES to enable User authentication.
Connection to PC software tools provided by Schneider-Electric (such as SoMove FDT / DTM) is locked by a password.

Possible Settings – [Reset Option Pwd] RPWD

Reset option password (used for user authentication).

It resets the user authentication password to the default value. Once reset, the default password can be read using **[Option default password]** DPW.

If **[Reset Option Pwd]** RPWD is set to:

- **[No]** NO: Password reset not requested. (**Factory Setting**)
- **[Yes]** YES: Password reset requested.

The parameter switches back to **[No]** NO when the operation is done.

Possible Settings – [Option default password] DPW

It provides the eight characters default password linked to the inserted option module.

This password must be entered at the first connection of the PC software tool in order to have access to the drive configuration.

This default password is also available on the sticker of the option module.

At the first connection, a dialog box is displayed (see figure below) requiring the modification of the default password. This dialog box will continue to be displayed until a password is defined.



The default password must not be used. A new password must be defined after a password reset or at the first connection to the drive.

Software Setup with SpaceLogic™ AS-P Automation Server

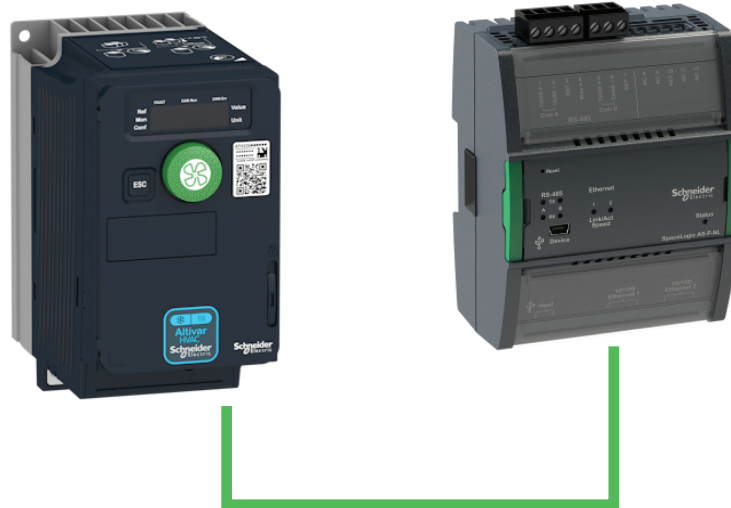
What's in This Part

Introduction.....	47
How to Configure SpaceLogic Ready-Server using Configuration Wizard.....	48
Command and communication configuration	49
Connect the drive and the controller with EcoStruxure™ Building Operation	50

Introduction

In the following example

- Drive is connected to the AS-P Automation Server equipped with BACnet MS/TP or IP port.
- Drive can be controlled through the EBO software.



How to Configure SpaceLogic Ready-Server using Configuration Wizard

Go to www.se.com to configure the SpaceLogic Automation server.

Command and communication configuration

Command Configuration

To control the drive with a AS-P Automation Server, select the communication module as the active command channel. Go to:

[Drive menu] *d r i* → [Configuration] *C o n F* → [Full] *F u L L* → [Command] *C t L*

Then configure [Ref Freq 1 Config] *F r 1* parameter to:

- [Ref. Freq-Modbus] *n d b* for BACnet MSTP
- [Ref. Freq-Com. Module] *n E t* for BACnet IP.

Communication Configuration with BACnet MSTP

Select the BACnet MS/TP address in the menu:

[Communication] *C o n* → [Bacnet MS/TP] *E b n*

Then configure:

- [MS/TP Address] *b A d r* to [2] *2*.

NOTE: Ensure that the addresses follow the previous one on the network.

In this example, the following drive parameters remain to their factory settings:

- [MS/TP Baudrate] *b b d r* to [Automatic] *A u t o*,
- [MS/TP Max info frame] *b n i f* to 10 maximum information frames,
- [MS/TP Max Master Nb] *b n n n* to 3.

NOTE: It is recommended to set [MS/TP Max Master Nb] to [MS/TP Address] + 1.

- [MS/TP Timeout] *b t L P* to (4 s in our example).

Communication Configuration with BACnet IP

Select the BACnet IP address in the menu:

[Communication] *C o n* → [Comm module] *C b d*


Then configure [IP address].

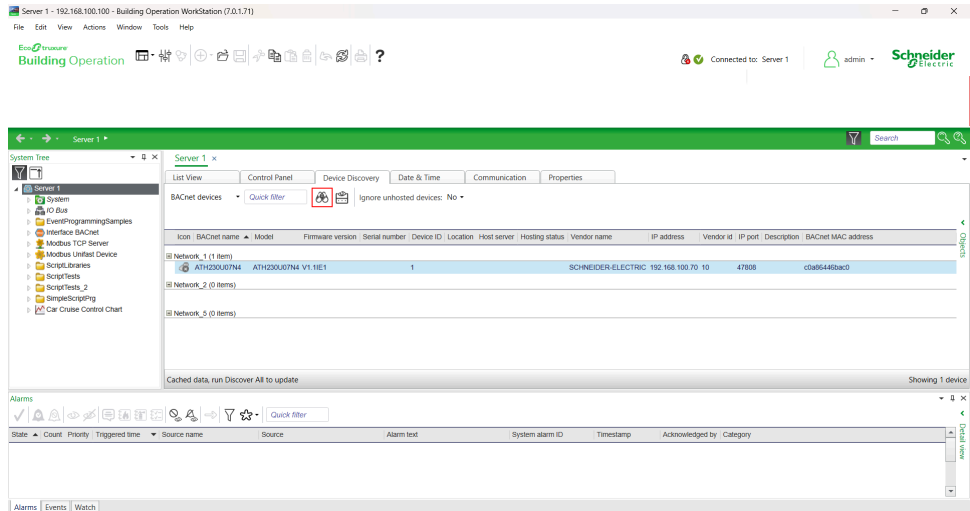
In this example, the following drive parameters remain to their factory settings:

- [Bacnet Instance High] *b A o H* to 1,
- [Bacnet Instance Low] *b A o L* to 1,
- [IP mode] *i P n* to [DCP] *d C P*,
- [Bacnet IP Time-Out] *b A t t* to 4 s.

Connect the drive and the controller with EcoStruxure™ Building Operation

Add the drive in a network

Click on .

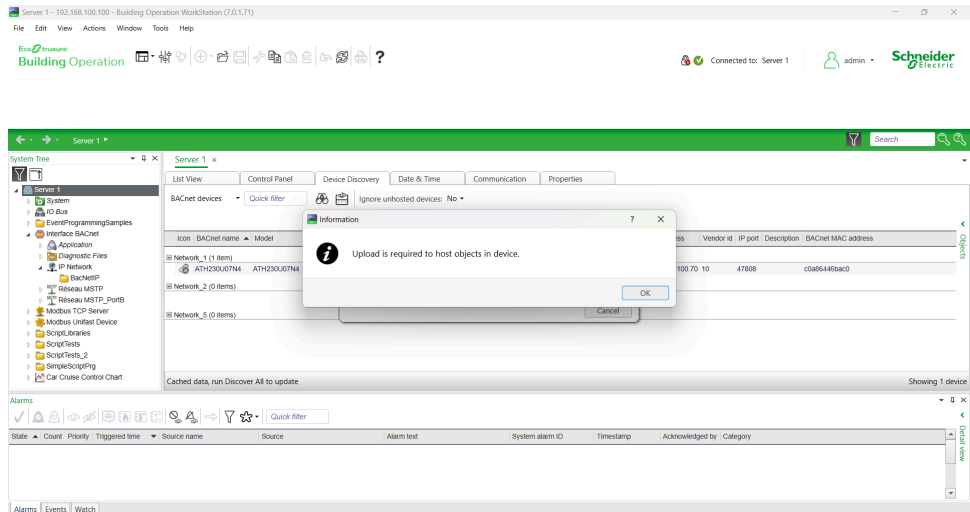


Click on the drive and drop it into the:

- BACnet MSTP network

OR

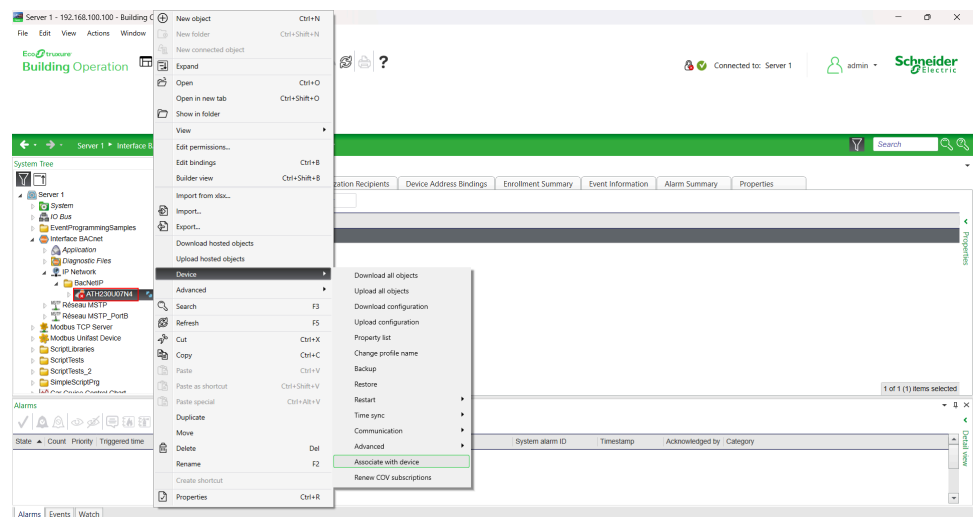
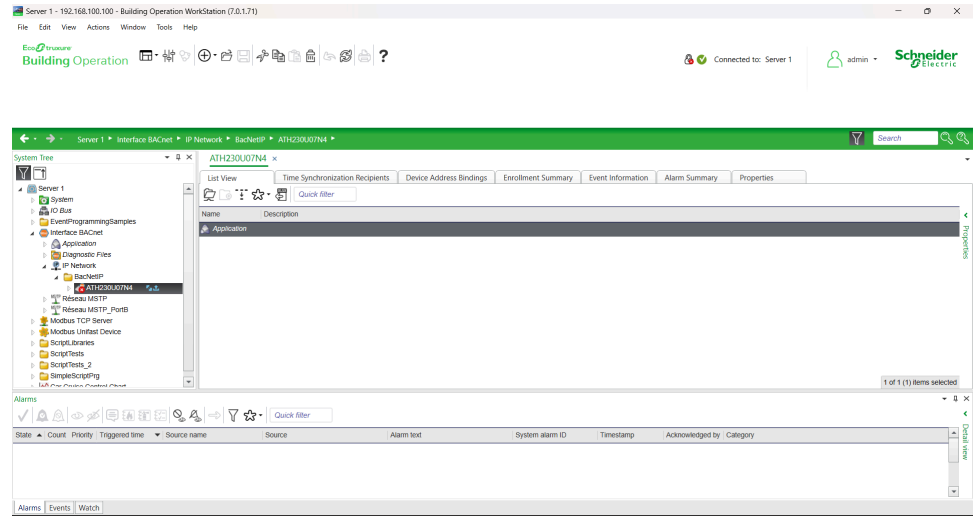
- BACnet IP network (if using the VW3A3726 module)



Click on **OK** to confirm the message.

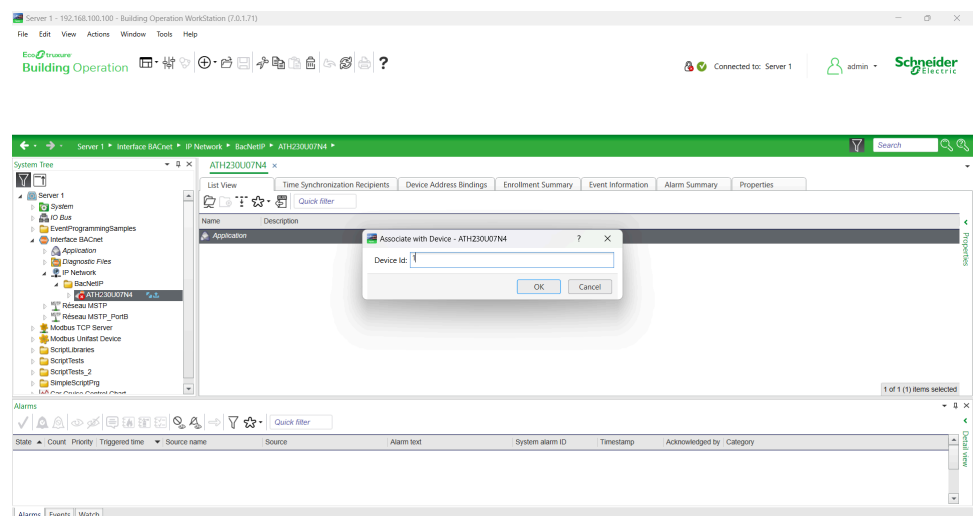
Associate with device

Right-Click on the drive → Device → Associate with device



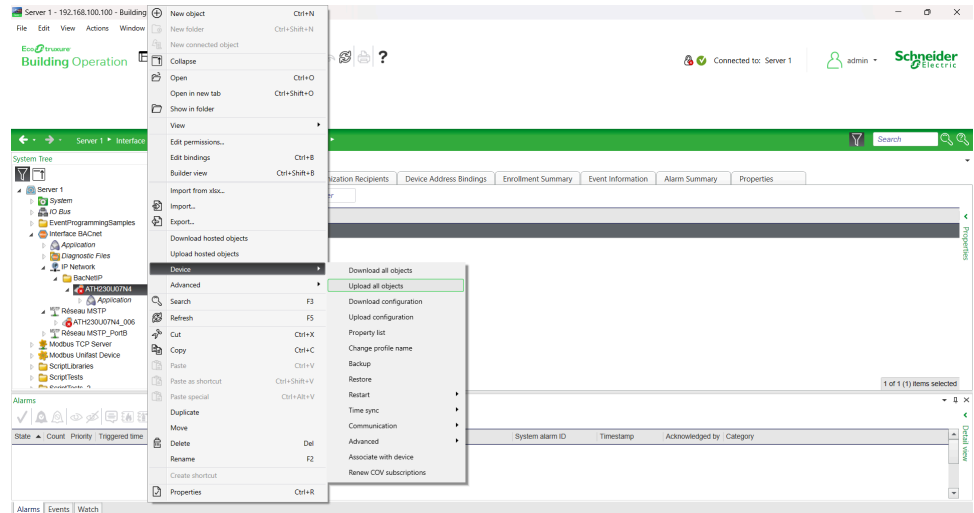
Select the number of the device ID linked to the :

- **[MS/TP Inst Nb High]** *b i n H* for the BACnet MSTP Network
- **[Bacnet Instance High]** *b a c H* for the BACnet IP network.

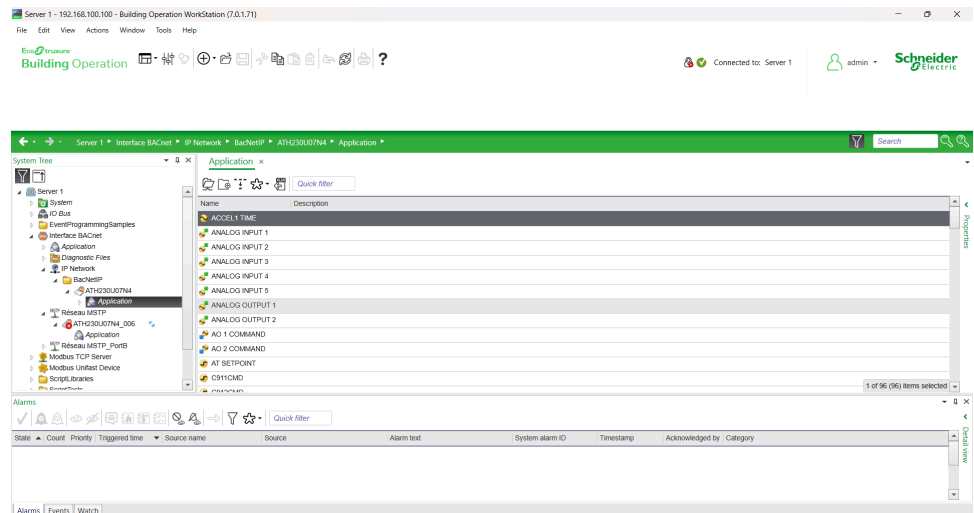


Upload of the BACnet Objects

Right-Click on the drive → Device → Upload all objects



Click on **Association** to check that all BACnet objects have been uploaded.



Diagnostics and Troubleshooting

What's in This Part

Configuring Communication Error Response	54
Communication troubleshooting	56
Control-Signal Diagnostics	57
Communication error codes	58

Configuring Communication Error Response

⚠ WARNING

LOSS OF CONTROL

Perform a comprehensive commissioning test to verify that communication monitoring properly detects communication interruptions.

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

The response of the drive in the event of a communication interruption can be configured. The timeout of Communication Error Response can be set via **[MS/TP Timeout]** *b t L P* or **[Bacnet IP Time-Out]** *b R t t* parameter

The values of the **[Modbus Error Resp]** and **[Fdbus Interrupt Resp]** parameter, which :

Value	Meaning
triggers a drive detected error ([Mdb Com Interrupt] <i>s L F 1</i> for BACnet MSTP and [Fdbus Com Interrupt] <i>C N F</i> for BACnet IP) are:	
[Freewheel Stop] <i>Y E S</i>	Motor triggers in error and is stopped in freewheel. Factory setting
[Ramp stop] <i>R M P</i>	Motor is stopped in ramp and triggers in error at the end of stop.
[Fast stop] <i>F S T</i>	Motor is stopped in fast stop and triggers in error at the end of stop.
[DC injection] <i>D C I</i>	Motor is stopped with DC injection and triggers in error at the end of stop.
does not trigger an error are:	
[Ignore] <i>N O</i>	Detected error ignored (in this case, the warning [Modbus Com Warn] <i>s L L A</i> for BACnet MSTP or [Fieldbus Com Warn] <i>C L L A</i> for BACnet IP is activated).
[Configured Stop] <i>S T T</i>	Motor is stopped according to [Type of stop] <i>S T T</i> parameter.
[Fallback Speed] <i>L F F</i>	Reference frequency modified to fallback speed, maintained as long as the detected error persists and the run command has not been removed.
[Speed maintain] <i>R L S</i>	The drive maintains the speed at the time the detected error occurred, as long as the detected error persists, and the run command has not been removed.

⚠ WARNING

LOSS OF CONTROL

If this parameter is set to **[Ignore]**, fieldbus module communication monitoring is disabled.

- Only use this setting after a thorough risk assessment in compliance with all regulations and standards that apply to the device and to the application.
- Only use this setting for tests during commissioning.
- Verify that communication monitoring has been re-enabled before completing the commissioning procedure and performing the final commissioning test.

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

▲ WARNING**LOSS OF CONTROL**

If this parameter is set to **[Fallback Speed]** LFF or **[Speed maintain]** RLS, no error is triggered in case of communication interruption.

Only use this setting after a thorough risk assessment in compliance with all regulations and standards that apply to the device and to the application.

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

Communication troubleshooting

Checking Connections

If the product cannot be addressed using the fieldbus, verify that:

- The connector is plugged in correctly.
- The drive and the PLC are supplied.
- The wires are correctly connected to the port (if possible).
- The ends of line resistors are connected on both sides of the complete network.
- The ends of line resistors have the good values.
- The wiring of the all devices on the network is consistent.

Behavior when an communication error occurs

Send a word with **[Cmd Register]** to validate the **[Cmd channel 1]** or the **[Cmd channel 2]** to activate this channel.

If a communication interruption appears:

1. After the end of the delay of timeout, the motor is stopped.
2. An error **[Mdb Com Interrupt]** *SLF1* for BACnet MSTP or **[Fdbus Com Interrupt]** *CNF* BACnet IP is triggered, and depending of **[Auto Fault Reset]**, **[R1 Assignment]** is deactivated (if set to **[Operating State Fault]** following the value set on **[Modbus Error Resp]** for BACnet MSTP or **[Fdbus Interrupt Resp]** for BACnet IP).

Control-Signal Diagnostics

Introduction

On the display terminal, the **[Display] MON-**, **[Communication map] CMM-** submenu can be used to display control-signal diagnostic information between the drive and the controller:

- Active command channel **[Command Channel] CMDC**
- Value of the control word **[Cmd Register] CMD** from the active command channel **[Command Channel] CMDC**
- Active reference frequency channel **[Ref Freq Channel] RFCC**
- Value of the reference frequency **[Pre-Ramp Ref Freq] FRH** from the active target channel **[Ref Freq Channel] RFCC**
- Value of the operating state word **[Status Register] ETA**
- Specific data for all available fieldbuses are in dedicated submenus.
- In the **[Cmd word image] CWI-** submenu: control words from all channels
- In the **[Freq. ref. word map] RWI-** submenu: reference frequency values produced by all channels

Control Word Display

The **[Command Channel] CMDC** parameter indicates the active command channel.

The **[Cmd Register] CMD** parameter indicates the hexadecimal value of the control word (CMD) used to control the drive.

- **BACnet MSTP:** The **[Cmd word image] CWI** submenu (**[Modbus Cmd] CMD1**) parameter is used to display the hexadecimal value of the control word from the fieldbus.
- **BACnet IP:** The **[Cmd word image] CWI** submenu (**[COM. Module cmd.] CMD3**) parameter is used to display the hexadecimal value of the control word from the fieldbus.

Reference Frequency Display

The **[Ref Freq Channel] RFCC** parameter indicates the active channel for reference frequency.

The **[Ref Frequency] LFR** parameter indicates the value (in 0.1 Hz units) of the reference frequency used to control the drive.

- **BACnet MSTP:** The **[Freq. ref. word map] RWI** submenu (**[Modbus Ref Freq] LFR1**) parameter is used to display the value (in 0.1 Hz units) of the reference frequency from the fieldbus.
- **BACnet IP:** The **[Freq. ref. word map] RWI** submenu (**[Com Module Ref Freq] LFR3**) parameter is used to display the value (in 0.1 Hz units) of the reference frequency from the fieldbus.

Communication error codes




What's in This Chapter

[Incorrect Config] <i>C F F</i>	58
[Invalid Configuration] <i>C F ,</i>	58
[Conf Transfer Error] <i>C F , 2</i>	59
[Fdbus Com Interrupt] <i>C n F</i>	59
[Ch Switch Error] <i>C S F</i>	59
[Internal Link Error] <i>, L F</i>	60
[Internal Error 6] <i>, n F B</i>	60
[Modb Com Interrupt] <i>S L F I</i>	60

In this chapter, a list of some of the errors that can be triggered by the communication-related drive can be found, for a full description please refer to the programming manual.




[Incorrect Config] *C F F*

Incorrect configuration error

 Probable Cause	<ul style="list-style-type: none"> Option module changed or removed. Control block replaced by a control block configured on a drive with a different rating. The current configuration is inconsistent.
 Remedy	<ul style="list-style-type: none"> Check that there are no detected module errors. In the event of the option module being changed/removed deliberately, see the remarks below. Return to factory settings or retrieve the backup configuration, if it is valid.
 Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Invalid Configuration] *C F ,*

Invalid configuration error

 Probable Cause	<p>Invalid configuration.</p> <p>The configuration loaded in the drive via the bus or communication network is inconsistent.</p>
 Remedy	<ul style="list-style-type: none"> Check the configuration loaded previously. Load a compatible configuration.
 Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Conf Transfer Error] [F 12]

Configuration transfer error

	Probable Cause	<p>Invalid configuration. The configuration loaded in the drive via the bus or communication network is inconsistent.</p>
	Remedy	<ul style="list-style-type: none"> • Check the configuration loaded previously. • Load a compatible configuration.
	Clearing the Error Code	<p>This detected error is cleared as soon as its cause has been removed.</p>

[Fdbus Com Interrupt] [n F]

Fieldbus communication interruption

	Probable Cause	<p>Communication interruption on fieldbus module. This error is triggered when the communication between the fieldbus module and the manager (PLC) is interrupted.</p>
	Remedy	<ul style="list-style-type: none"> • Verify the communication settings on the devices (Drive, PLC, switches, repeater...). • Check for duplicate communication addresses. • Verify the environment (electromagnetic compatibility). • Verify the fieldbus wiring (continuity, cable type, grounding, and shielding). • Verify the terminating resistor. • Verify the timeout setting. • Check the parameters [MS/TP APDU Retries] <i>RPdr</i> and [MS/TP APDU Timeout] <i>RPdt</i> for BACnet MS/TP and [IP APDU Retries] <i>RPri</i> and [IP APDU Timeout] <i>RPti</i> for BACnet IP according to the application. • Replace the option module. • Verify that the value set on [Bacnet IP Time-Out] <i>BAEt</i> meets the requirements of your application. • Contact your local Schneider Electric representative.
	Clearing the Error Code	<p>This detected error can be cleared with the [Auto Fault Reset] <i>ARr</i> or manually with the [Fault Reset Assign] <i>r5F</i> parameter after its cause has been removed. This also possible to reset with the command word 0080 hex (<i>Fault reset</i>).</p>




[Ch Switch Error] [5 F]

Channel switching detected error

	Probable Cause	<p>Switch to not valid channels.</p>
	Remedy	<p>Check the function parameters.</p>
	Clearing the Error Code	<p>This detected error is cleared as soon as its cause has been removed.</p>




[Internal Link Error] *ILF*

Internal communication interruption with option module

 Probable Cause	Communication interruption between option module and the device.
 Remedy	<ul style="list-style-type: none"> • Verify the environment (electromagnetic compatibility). • Verify the connections. • Replace the option module. • Contact your local Schneider Electric representative.
 Clearing the Error Code	This detected error requires a power reset of the device after its cause has been removed.




[Internal Error 6] *INF6*

Internal error 6 (Option)

 Probable Cause	<ul style="list-style-type: none"> • The option module installed in the device is not recognized. • The removable control terminal modules (if existing) are not present or not recognized. • The embedded Ethernet adapter is not recognized. • The device firmware is not compatible with the option module. • Option module corrupted due to multiple firmware updates.
 Remedy	<ul style="list-style-type: none"> • Verify the catalog number and compatibility of the option module. • Plug the removable control terminal modules after the device has been switched off. • Update the device firmware. • Contact your local Schneider Electric representative.
 Clearing the Error Code	This detected error requires a power reset of the device after its cause has been removed.

[Modb Com Interrupt] *5LF1*

Modbus communication interruption error

 Probable Cause	Communication interruption on the BACnet bus.
 Remedy	<ul style="list-style-type: none"> • Verify the communication settings on the devices (Drive, PLC, switches, repeater...). • Check for duplicate communication addresses. • Verify the environment (electromagnetic compatibility). • Verify the fieldbus wiring (continuity, cable type, grounding, and shielding). • Verify the terminating resistor. • Verify that the value set on [MS/TP Timeout] <i>bELP</i> meets the requirements of your application.
 Clearing the Error Code	This detected error can be cleared with the [Auto Fault Reset] <i>ALr</i> or manually with the [Fault Reset Assign] <i>r5F</i> parameter after its cause has been removed. This also possible to reset with the command word 0080 hex (<i>Fault reset</i>).

Annex

What's in This Part

Firmware Update	62
Operation	63
Starting Sequence.....	75
Operating Modes	83
BACnet Basics.....	86

Firmware Update

BACnet MSTP

The firmware update of BACnet MSTP is done during the firmware update of the drive .

BACnet IP – VW3A3726

The firmware update of the VW3A3726 is done by the services.

For additional support, you can contact our Customer Care Center on:

www.se.com/CCC.

Operation

What's in This Chapter

Profile.....	64
Functional Profiles Supported by the Drive	65
Functional Description	66
CIA402 Operating State Diagram	67
Description of Operating States	68
Device Status Summary	69
Command Register <i>C P d</i>	70
Stop Commands	71
Assigning Control Word Bits	71
[CIA402 State Reg] <i>E L R</i>	72
Extended Control Word.....	73
Internal State register	74

Profile

There are 3 types of profile:

- Communication profiles
- Functional profiles
- Application profiles

Communication Profile

A communication profile describes the characteristics of a bus or network:

- Cables
- Connectors
- Electrical characteristics
- Access protocol
- Addressing system
- Periodic exchange service
- Messaging service
- ...

A communication profile is unique to a type of fieldbus (such as Modbus, and so on) and is used by different types of devices.

Functional Profile

A functional profile describes the behavior of a type of device:

- Functions
- Parameters (such as name, format, unit, type, and so on.)
- Periodic I/O variables
- State chart
- ...

A functional profile is common to all members of a device family (such as variable speed drives, encoders, I/O modules, displays, and so on).

They can feature common or similar parts. The standardized (IEC 61800-7) functional profiles of variable speed drives are:

- CiA402

Application Profile

Application profile defines the services to be provided by the devices on a machine.

Interchangeability

The aim of communication and functional profiles is to achieve interchangeability of the devices connected via the fieldbus.

Functional Profiles Supported by the Drive

CiA402 Profile

The drive only starts up following a command sequence.

The control word is standardized.

5 bits of the control word (bits 11...15) can be assigned to a function.

The CiA402 profile is supported by the drive itself and therefore by all the communication ports.

The drive supports the *velocity* mode of CiA402 profile.

In the CiA402 profile, there are two modes that are specific to the drive and characterize commands and references value management:

- *Separate* [**Separate**] $S E P$
- *Not separate* [**Not separ.**] $S , P ,$

Functional Description

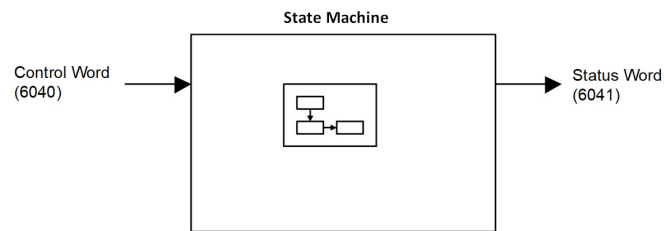
Introduction

Drive operation involves two main functions, which are illustrated in the diagrams below.

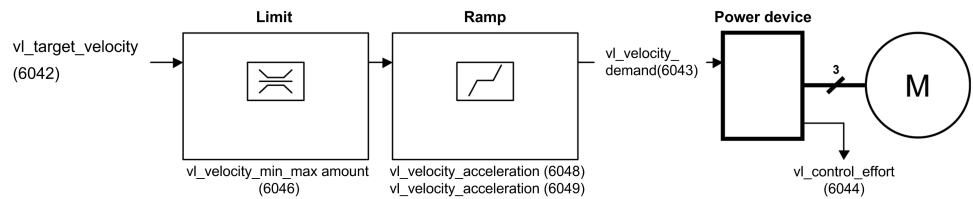
CiA402

The main parameters are shown with their CiA402 name and their CiA402/Drivecom index (the values in brackets are the CANopen addresses of the parameter).

The following figure shows the control diagram for drive operation:



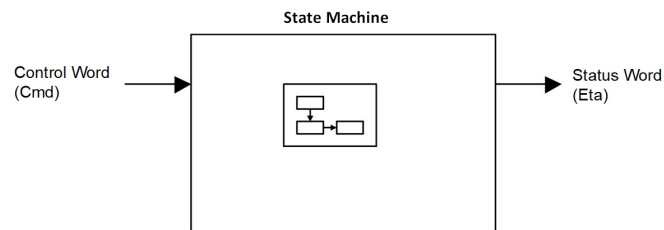
Simplified diagram for speed control in *Velocity* mode:



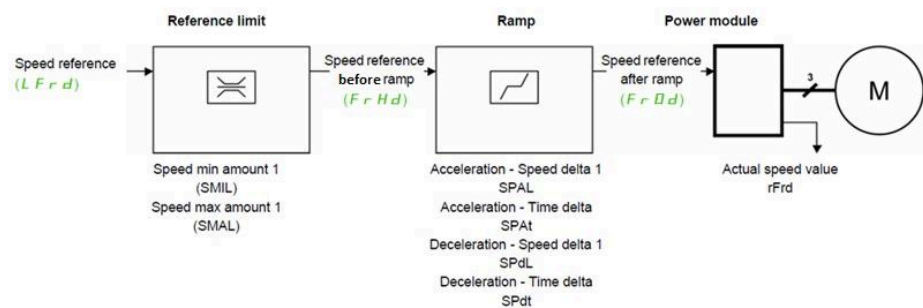
Altivar HVAC Drive

These diagrams translate as follows for the Altivar HVAC drive.

The following figure shows the control diagram for drive operation:



Simplified diagram for speed control in *Velocity* mode:

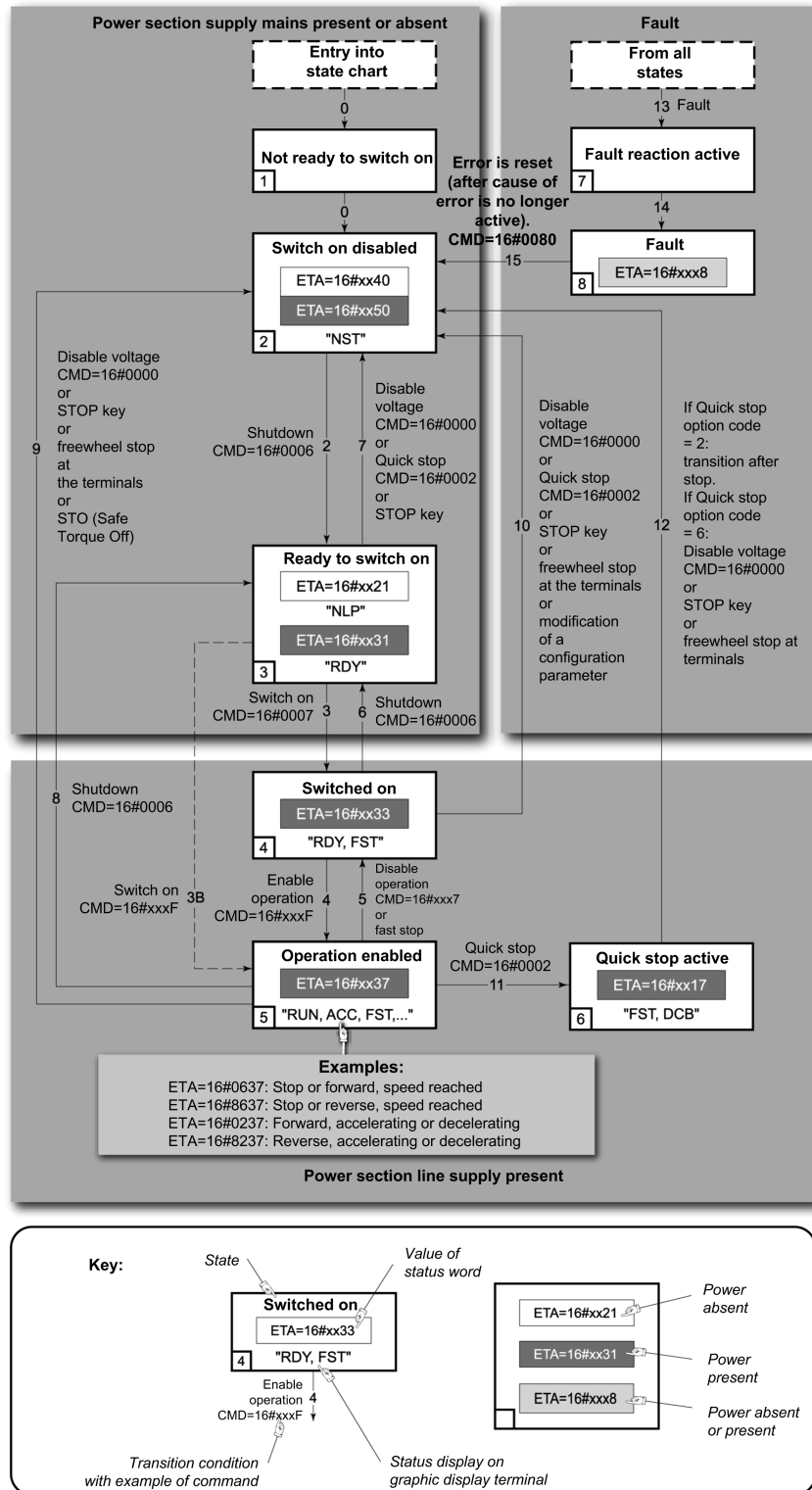


CIA402 Operating State Diagram

After switching on and when an operating mode is started, the product goes through a number of operating states.

The state diagram (state machine) shows the relationships between the operating states and the state transitions. The operating states are internally monitored and influenced by monitoring functions.

The following figure shows the CIA402 state diagram:



Description of Operating States

Each state represents an internal reaction by the drive.

The operating state of the drive changes depending on whether the control word is sent to **[Cmd Register] CMD** or an event occurs (an error detection, for example).

The drive operating state can be identified by the value of the status word **[Status Register] ETA**. For more information, refer to the **[Status Register] ETA** chapter.

Operating State	Description
1 - Not ready to switch on	<ul style="list-style-type: none"> Initialization starts. This is a transient state invisible to the communication network.
2 - Switch on disabled	<ul style="list-style-type: none"> The power stage is not ready to switch on. The drive is locked, no power is supplied to the motor. For a separate control stage, it is not necessary to supply the power. For a separate control stage with mains contactor, the contactor is not closed. The configuration and adjustment parameters can be modified.
3 - Ready to switch on	<ul style="list-style-type: none"> The power stage is ready to switch on and awaiting power stage supply mains. For a separate control stage, it is not necessary to supply the power stage, but the system expects it in order to change to state 4 - <i>Switched on</i>. For a separate control stage with mains contactor, the contactor is not closed. The drive is locked, no power is supplied to the motor. The configuration and adjustment parameters can be modified.
4 - Switched on	<ul style="list-style-type: none"> Power stage is switched on. For a separate control stage, the power stage must be supplied. For a separate control stage with mains contactor, the contactor is closed. The drive is locked, no power is supplied to the motor. The power stage of the drive is ready to operate, but voltage has not yet been applied to the output. The adjustment parameters can be modified. If a configuration parameter is modified, the drive returns to the state 2 - <i>Switch on disable</i>.
5 - Operation enabled	<ul style="list-style-type: none"> Power stage is enabled. The drive is in running state. For a separate control stage, the power stage must be supplied. For a separate control stage with mains contactor, the contactor is closed. The drive is unlocked, power is supplied to the motor. The drive functions are activated and voltage is applied to the motor terminals. If the reference value is zero or the <code>HALT</code> command is applied, no power is supplied to the motor and no torque is applied. To perform [Autotuning] TUN, the drive must be in state 5 - <i>Operation enabled</i>. The adjustment parameters can be modified. The configuration parameters cannot be modified. <p>NOTE: The command <i>4 - Enable operation</i> must be taken into consideration only if the channel is valid. In particular, if the channel is involved in the command and the reference value, transition 4 is possible only after the reference value has been received once.</p> <ul style="list-style-type: none"> The reaction of the drive to a <code>Disable operation</code> command depends on the value of the [SwitchOnDisable Stp] DOTD parameter: <ul style="list-style-type: none"> If the [SwitchOnDisable Stp] DOTD parameter is set to 0, the drive changes to operating state 4 - <i>Switched on</i> and stops in freewheel stop. If the [SwitchOnDisable Stp] DOTD parameter is set to 1, the drive stops on ramp and then changes to operating state 4 - <i>Switched on</i>.

Operating State	Description
6 - Quick stop active	<ul style="list-style-type: none"> The drive performs a fast stop and remains locked in the operating state 6-Quick stop active. Before restarting the motor, it is required to go to the operating state 2-switch on disabled. During fast stop, the drive is unlocked and power is supplied to the motor. The configuration parameters cannot be modified. The condition for transition 12 to state 2 - Switch on disabled depends on the value of the parameter [Quick Stop Mode] QSTD: If the Quick stop mode parameter has the value [Fast stop then stay in quick stop state] FST2, the drive stops according to the fast stop ramp and then changes to state 2 - Switch on disabled . If the Quick stop mode parameter has the value [Fast stop then disable voltage] FST6, the drive stops according to the fast stop ramp and then remains in state 6 - Quick stop active until: <ul style="list-style-type: none"> A Disable voltage command is received. OR the STOP key is pressed. OR a freewheel stop command via the digital input of the terminal.
7 - Fault reaction active	<ul style="list-style-type: none"> Transient state during which the drive performs an action corresponding to the selected error response.
8 - Fault	<ul style="list-style-type: none"> Error response terminated. Power stage is disabled. The drive is locked, no power is supplied to the motor.

Device Status Summary

Operating State	Power Stage Supply for Separate Control Stage	Power Supplied to Motor	Modification of Configuration Parameters
1 - Not ready to switch on	Not required	No	Yes
2 - Switch on disabled	Not required	No	Yes
3 - Ready to switch on	Not required	No	Yes
4 - Switched on	Required	No	Yes, return to 2 - Switch on disabled operating state
5 - Operation enabled	Required	Yes	No
6 - Quick stop active	Required	Yes, during fast stop	No
7 - Fault reaction active	Depends on error response configuration	Depends on error response configuration	-
8 - Fault	Not required	No	Yes

NOTE:

- Configuration parameters are described in communication parameter file as R/WS access type parameters.
- An adjustment parameter can be accessed in all operating state of the drive.

Command Register [Π]

Bit Mapping of the Control Word

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Error reset	Reserved (=0)	Reserved (=0)	Reserved (=0)	Enable operation	Quick stop	Switch on disabled	Switch on
0 to 1 transition = Error is reset (after cause of error is no longer active)				1 = Run command	0 = Quick stop active	0 = Authorization to supply AC power	1 = Mains contactor control

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Manufacturer specific assignable	Manufacturer specific assignable	Manufacturer specific assignable	Manufacturer specific assignable	Manufacturer specific assignable	Reserved (=0)	Reserved (=0)	Halt
							0 = RUN asked 1 = STOP asked

Command	State Transition	Final Operating State	Bit 7	Bit 3	Bit 2	Bit 1	Bit 0	Example Value
			Fault Reset	Enable Operation	Quick Stop	Enable Voltage	Switch On	
<i>Shutdown</i>	2, 6, 8	3 - Ready to switch on	X	X	1	1	0	0006 hex
<i>Switch on</i>	3	4 - Switched on	X	X	1	1	1	0007 hex
<i>Enable operation</i>	4	5 - Operation enabled	X	1	1	1	1	000F hex
<i>Disable operation</i>	5	4 - Switched on	X	0	1	1	1	0007 hex
<i>Disable voltage</i>	7, 9, 10, 12	2 - Switch on disabled	X	X	X	0	X	0000 hex
<i>Quick stop</i>	11	6 - Quick stop active	X	X	0	1	X	0002 hex
	7, 10	2 - Switch on disabled						
<i>Fault reset</i>	15	2 - Switch on disabled	0 → 1	X	X	X	X	0080 hex

X: Value is of no significance for this command.

0→1: Command on rising edge.

Stop Commands

Halt Command

The `Halt` command enables movement to be interrupted without having to leave the 5 - *Operation enabled* state. The `Halt` is performed in accordance with the **[Type of stop]** `STT` parameter.

If the `Halt` command is active, no power is supplied to the motor and no torque is applied.

Regardless of the assignment of the **[Type of stop]** `STT` parameter **[On Ramp]** `RMP`, **[Freewheel Stop]** `NST`, the drive remains in the 5 - *Operation enabled* state.

Fast Stop Command

A `Fast Stop` command at the terminals or using a bit of the control word assigned to `Fast Stop` causes a change to the operating state 4 - *Switched on*

Freewheel Command

A `Freewheel Stop` command using a digital input of the terminal or a bit of the control word assigned to `Freewheel Stop` causes a change to operating state 2 - *Switch on disabled*.

Assigning Control Word Bits

Function Codes

In the CiA402 profile, fixed assignment of a function input is possible using the following codes:

Bit	Embedded	BACnet IP
Bit 11	C111	C311
Bit 12	C112	C312
Bit 13	C113	C313
Bit 14	C114	C314
Bit 15	C115	C315

For example, to assign the DC injection braking to bit13 of BACnet IP, simply configure the **[DC injection]** `DCI` parameter with the **[C313]** `∃ I ∃` value.

Bit 11 is assigned by default to the operating direction command **[Reverse Assign]** `RRS`.

[CIA402 State Reg] E L R**Bit Mapping of the Status Word**

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Warning	Switch on disabled	Quick stop	Voltage enabled	Fault	Operation enabled	Switched on	Ready to switch on
A warning is active	Power stage supply disabled	0 = Quick stop is active	Power stage supply present	Error detected	Running	Ready	1 = Awaiting power Stage supply

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Manufacturer-specific Direction of rotation	Manufacturer-specific Stop via STOP key	Reserved (=0)	Reserved (=0)	Internal limit active	Target reached	Remote	Reserved (=0)
				Reference value outside limits	Reference value reached	Command or reference value via fieldbus	

Operating State	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	ETA Masked by 006F H ⁽¹⁾
	Switch On Disabled	Quick Stop	Voltage Enabled	Fault	Operation Enabled	Switched On	Ready to Switch On	
1 -Not ready to switch on	0	X	X	0	0	0	0	-
2 -Switch on disabled	1	X	X	0	0	0	0	0040 hex
3 -Ready to switch on	0	1	X	0	0	0	1	0021 hex
4 -Switched on	0	1	1	0	0	1	1	0023 hex
5 -Operation enabled	0	1	1	0	1	1	1	0027 hex
6 -Quick stop active	0	0	1	0	1	1	1	0007 hex
7 -Fault reaction active	0	X	X	1	1	1	1	-
8 -Fault	0	X	X	1	0	0	0	0008 hex ⁽²⁾ ... 0028 hex

⁽¹⁾ This mask can be used by the PLC program to test the diagram state.

⁽²⁾ Detected error following operating state 6 - Quick stop active.

X: In this state, the value of the bit can be 0 or 1.

Extended Control Word

When a configuration parameter is modified by fieldbus, it is not stored automatically in the EEPROM. The value will be lost after a power cycle if the request to store the new configuration has not been done.

⚠ WARNING

LOSS OF PARAMETER CONFIGURATION AFTER A POWER CYCLE

Bit 1 of **[Extended Ctrl Word]** *CMI* must be written at 1 each time the configuration is modified by fieldbus.

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

NOTE: Do not write **[Extended Ctrl Word]** BITs cyclically (especially BIT 1), as this may damage the EEPROM.

NOTE: Monitor the parameter **EEPROM Status** *EEPS* (logical address 5E2 hex = 1506) to check that the configuration storage is completed (bit at 0).

[Extended Ctrl Word] is used to control the product defined as followed:

Code	Settings	
[Extended Ctrl Word] <i>CMI</i>	Logic address: 2138 hex = 8504	Type: WORD (BitString16) Read/write: R/W Unit: -
Extended control word		

	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Function	Factory setting asked	Memorize current configuration in EEPROM	Read current configuration in EEPROM	External error	Reserved			
Bit at 0	Active on rising edge when motor is powered off.	Active on rising edge.	Active on rising edge when motor is powered off. Once request is considered, this bit is automatically reset.	Active on rising edge.				
Bit at 1	Once request is considered, this bit is automatically reset.	Once request is considered, this bit is automatically reset.						

	Bit 8	Bit 9	Bit 10	Bit 11	Bit 12	Bit 13	Bit 14	Bit 15
Function	Reserved	Frequency reference (FRH, LFR, RFR ...)	Reserved			Drive locked in STOP	Serial link error inhibition	Parameter coherence deactivated and drive locked in STOP
Bit at 0		in 0.1Hz				Deactivate.	Deactivate.	Deactivate. All parameters are validated.
Bit at 1		in internal unity (32767 = TFR)				Activate.	Activate.	Activate. No check of parameter consistency and device is locked when stopped.

Internal State register

	Bit 0	Bit 1	Bit 2	Bit 3
Function	<i>EEPROM access running</i>	<i>Parameter consistency checked</i>	<i>No more error present and drive in error state</i>	<i>Reserved</i>
Bit at 0	Access to the non-volatile memory stopped.	Not active.	The device: <ul style="list-style-type: none"> • is not in operating state "Error" • is in operating state "Error" and the error is active. 	
Bit at 1	Access to the non-volatile memory in progress.	Active.	The device is in operating state "Error" and the error is no longer active (not reset).	

	Bit 4	Bit 5	Bit 6	Bit 7
Function	<i>Run order present</i>	<i>DC injection running</i>	<i>Drive in transitional state</i>	<i>Motor thermal threshold reached:</i>
Bit at 0	Not active.	Not active.	Transient state.	Threshold for the active motor not reached.
Bit at 1	Active.	Active.	Steady state.	Threshold for the active motor reached.

	Bit 8	Bit 9	Bit 10	Bit 11
Function	<i>Braking transistor activated</i>	<i>Product in acceleration</i>	<i>Product in deceleration</i>	<i>Current limitation or torque limitation is running</i>
Bit at 0	Not active.	Not active.	Not active.	Not active.
Bit at 1	Active.	Active.	Active.	Active.

	Bit 12	Bit 13	Bit 14	Bit 15
Function	<i>Fast stop in progress</i>	<i>Active mode:</i>		<i>Reverse direction applied to the ramp</i>
Bit at 0	Not active.	<ul style="list-style-type: none"> • Bit 13 = 0 + Bit 14 = 0: Device controlled by terminal • Bit 13 = 1 + Bit 14 = 0: Device controlled by the display terminal • Bit 13 = 0 + Bit 14 = 1: Device controlled by Embedded Modbus • Bit 13 = 1 + Bit 14 = 1: Device controlled by fieldbus card 		Forward operation applied before the ramp.
Bit at 1	Active.			Reverse operation applied before the ramp.

Starting Sequence

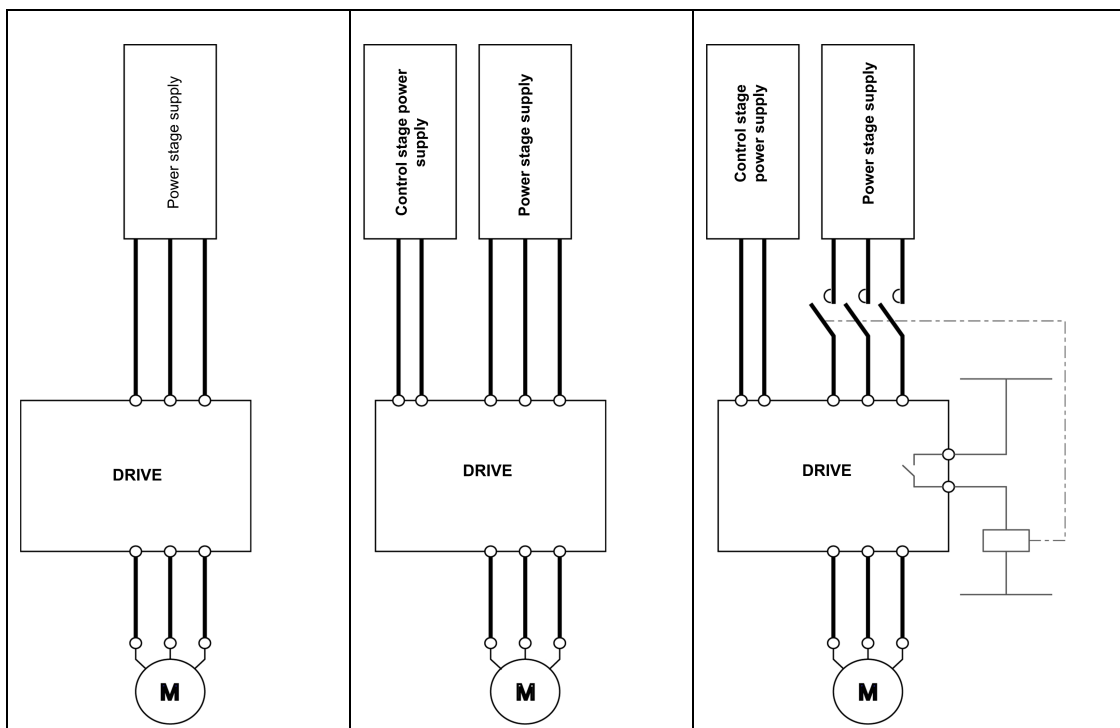
What's in This Chapter

Starting Sequence for a Drive Powered by the Power Stage Supply 76
 Starting Sequence for a Drive with Separate Control Stage 78
 Starting Sequence for a Drive with Mains Contactor Control 81

Description

The command sequence in the state diagram depends on how power is being supplied to the drive.

There are 3 possible scenarios:



Power stage supply	Direct	Direct	Mains contactor controlled by the drive
Control stage supply	Not separate ⁽¹⁾	Separate	Separate
⁽¹⁾ The power stage supplies the control stage.			

Starting Sequence for a Drive Powered by the Power Stage Supply

Description

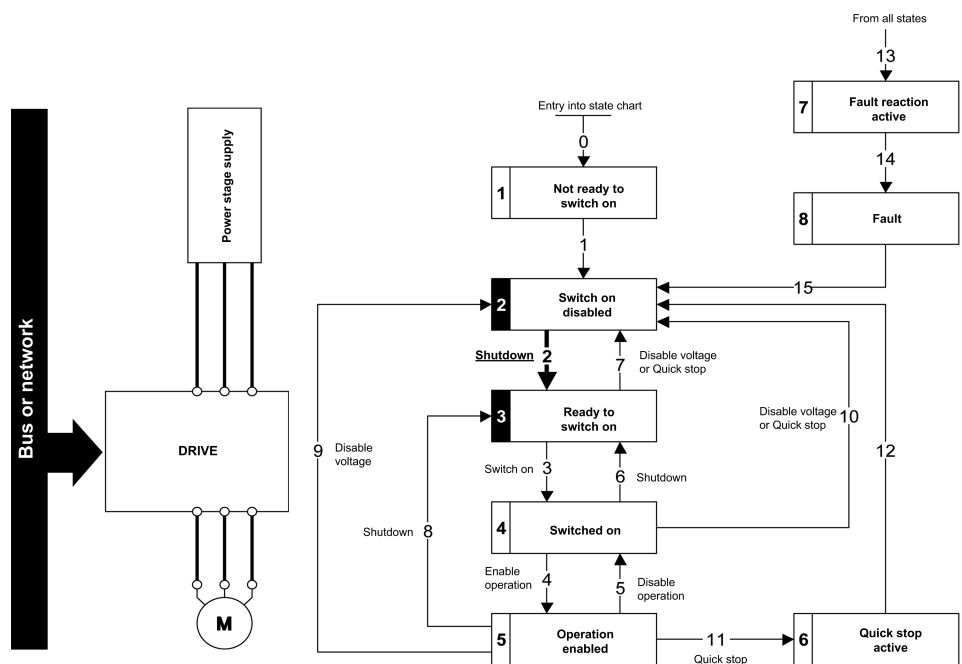
Both the power and control stages are powered by the power stage supply.

If power is supplied to the control stage, it has to be supplied to the power stage as well.

The following sequence must be applied:

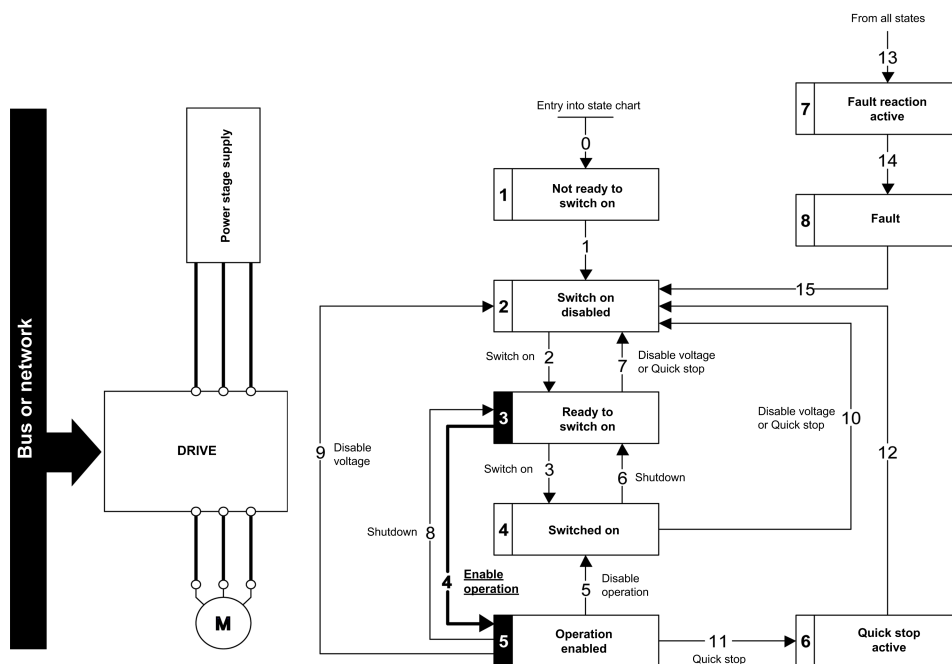
Step 1

Apply the 2 - *Shut down* command



Step 2

- Check that the drive is in the operating state 3 - *Ready to switch on*.
- Then apply the 4 - *Enable operation* command.
- The motor can be controlled (send a reference value not equal to zero).



NOTE: It is possible, but not necessary to apply the 3 - *Switch on* command followed by the 4 - *Enable Operation* command to switch successively into the operating states 3 - *Ready to Switch on*, 4 - *Switched on* and then 5 - *Operation Enabled*. The 4 - *Enable operation* command is sufficient.

Starting Sequence for a Drive with Separate Control Stage

Description

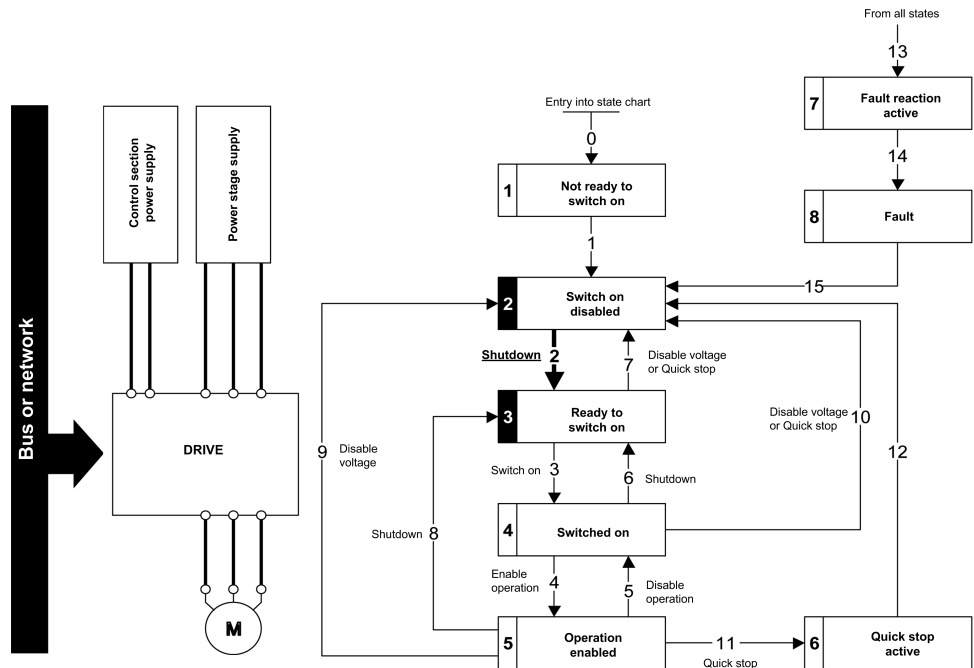
Power is supplied separately to the power and control stages.

If power is supplied to the control stage, it does not have to be supplied to the power stage as well.

The following sequence must be applied:

Step 1

- The power stage supply is not necessarily present.
- Apply the 2 - *Shut down* command

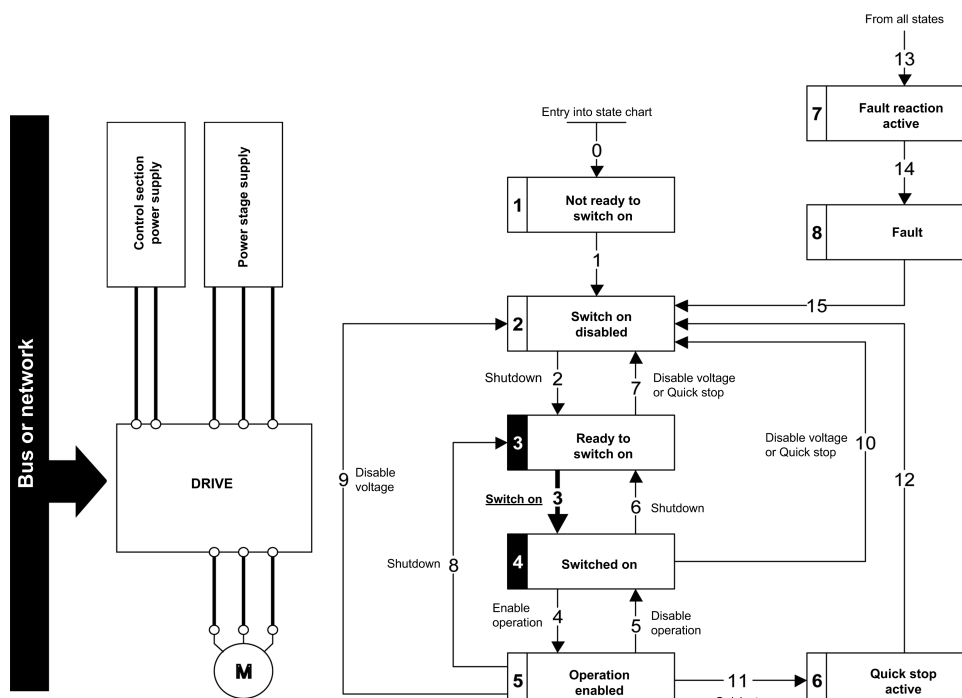


Step 2

- Check that the drive is in the operating state 3 - *Ready to switch on*.
- Check that the power stage supply is present (*Voltage enabled* of the status word).

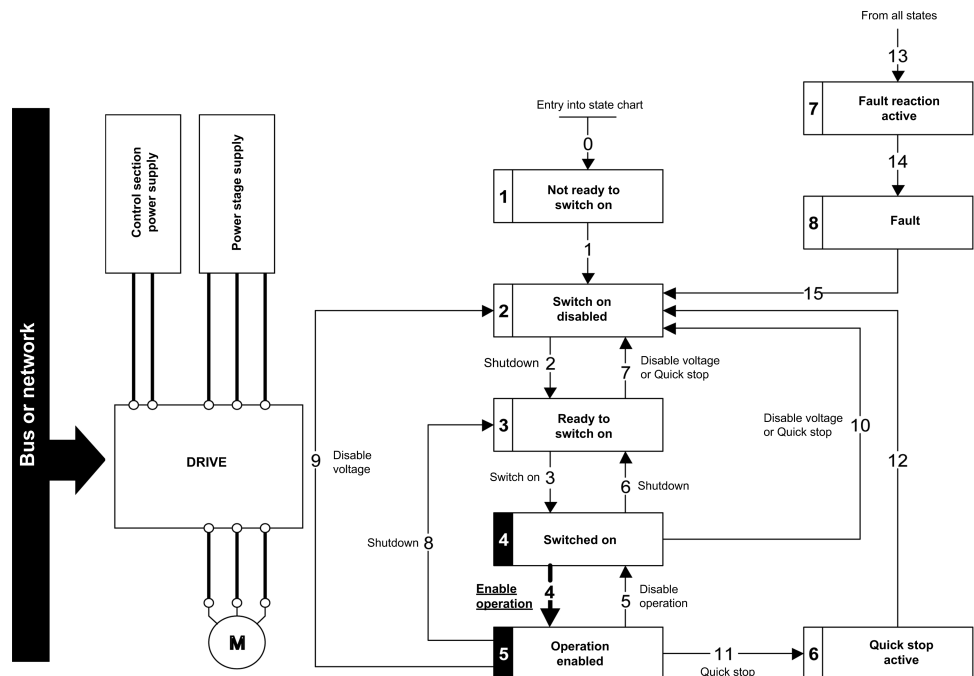
Power Stage Supply	HMI Panel	Status Word
Not present	[No Mains Voltage] NLP	21 hex
Present	[Ready] RDY	31 hex

- Apply the 3 - *Switch on* command



Step 3

- Check that the drive is in the operating state 4 - *Switched on*.
- Then apply the 4 - *Enable operation* command.
- The motor can be controlled (send a reference value not equal to zero).
- If the power stage supply is still not present in the operating state 4 - *Switched on* after a time delay [**Mains V. time out**] *LCT*, the drive triggers an error [**Input Contactor**] *LCF*.



Starting Sequence for a Drive with Mains Contactor Control

Description

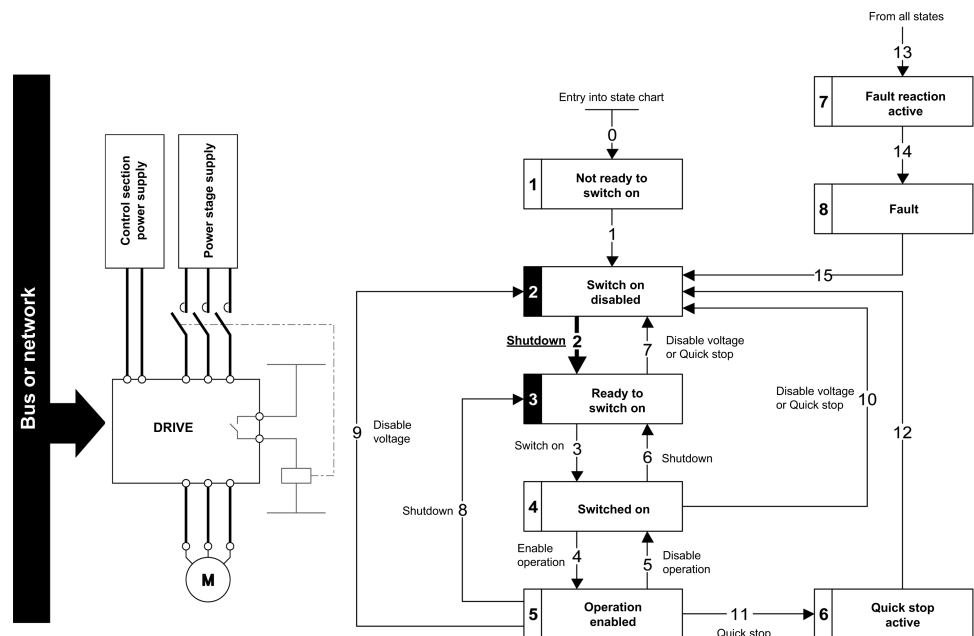
Power is supplied separately to the power and control stages.

If power is supplied to the control stage, it does not have to be supplied to the power stage as well. The drive controls the mains contactor.

The following sequence must be applied:

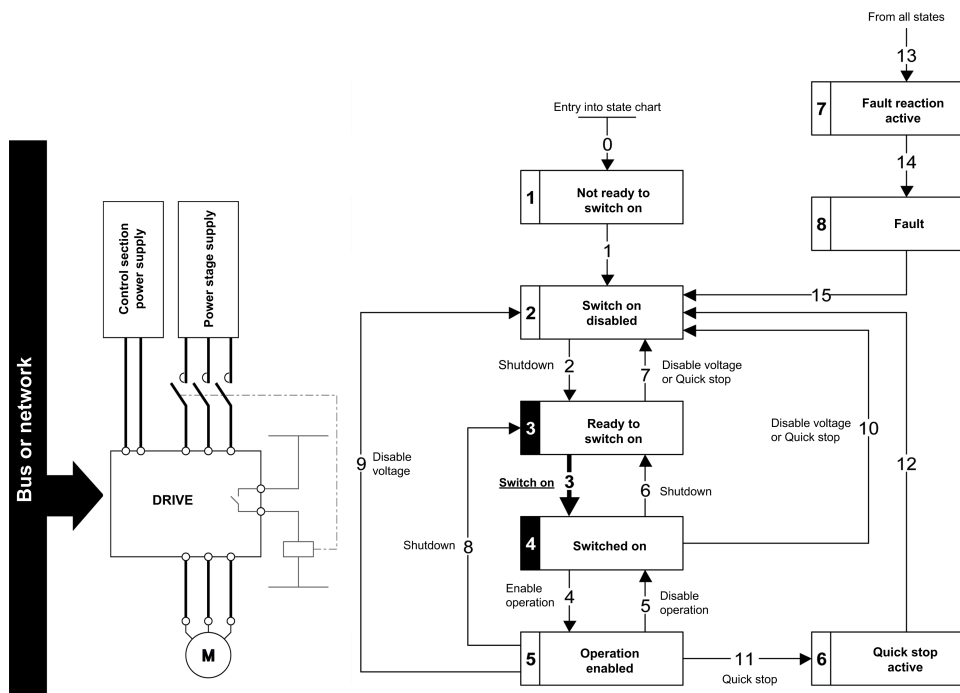
Step 1

- The power stage supply is not present as the mains contactor is not being controlled.
- Apply the 2 - *Shutdown* command.



Step 2

- Check that the drive is in the operating state 3 - *Ready to switch on*.
- Apply the 3 - *Switch on* command, which closes the mains contactor and switch on the power stage supply.



Operating Modes

What's in This Chapter

Configuring the Control Channel.....	84
Configuration of the Drive for Operation with CiA 402 Profile in Combined Mode.....	84
Configuration of the Drive for Operation with CiA 402 Profile in Separate Mode.....	85

Configuring the Control Channel

This chapter explains how to configure the drive for operation from the communication network through three following examples.

- Combined mode (with native profile CiA 402) - Both reference value and command word come from the communication network.
- Separate (with native profile CiA 402) - reference value and command word come from separate sources: for example, the command word (in CiA 402) comes from the communication network and the reference value from the HMI.

Configuration of the Drive for Operation with CiA 402 Profile in Combined Mode

This section describes how to configure the settings of the drive if it is controlled in CiA 402 mode. The example focuses on the not separate mode. Additional modes are detailed in the drive programming manual.

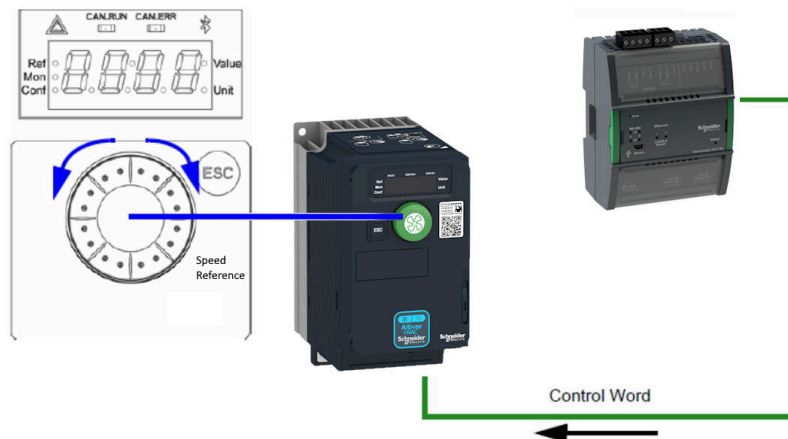
In the **[Command]** \llcorner \llcorner \llcorner - menu:

- Check if **[Ref Freq 1 Config]** FR1 is set on according to the communication source ().
- **[Control Mode]** CHCF : defines if the drive operates in combined mode (reference and command from the same channel).

Configuration of the Drive for Operation with CiA 402 Profile in Separate Mode

Alternate combinations are possible, see the drive programming manual for the list of possible settings.

For example:



The drive is controlled from the communication but the frequency reference value is adjusted on the local HMI. The control word comes from the controller and is written according to CiA 402 profile.

The settings are as shown in the table:

[Ref Freq 1 Config] FR1	[AI virtual 1] R u l
[Reverse Disable] RIN	Default
[Stop Key Enable] PST	Default
[Control Mode] CHCF	[Separate] SEP
[Command Switching] CCS	Default
[Cmd channel 1] CD1	[Modbus] M b d

BACnet Basics

What's in This Chapter

BACnet Devices	87
Monitoring of communication channel / Bacnet timeout	88
BACnet Device Profiles and BIBBs	89
BACnet Object	91
Additional Functions	100

BACnet Devices

About BACnet Devices

A BACnet device conforms to the BACnet standard. The device can perform following services:

- Building controller
- Field controller
- Router
- Gateway
- End device (for example, a sensor or actuator)

Devices in a building are networked as peer-to-peer devices, subordinate devices, or manager/subordinate devices.

Device Identifiers

The following table gives the structure of BACnet device identification characteristics for MS/TP networks:

Identifier	Description	Valid Numeric Values
Device identifier	This instance number is unique to the device across many different networks that comprise a BACnet system.	1...4194303
Network number	This number is unique to the network to which the device belongs.	1...65535
MAC address	This address is unique only within its own network.	1...254

NOTE: A MAC address is typically read from DIP switches or from non-volatile memory. Some devices auto-assign MAC addresses when devices are placed on the network.

BACnet devices can have input/output functionality or no input/output functionality.

Monitoring of communication channel / Bacnet timeout

BACnet protocol is not providing any timeout mechanism.

The drive system is managing a specific timeout mechanism based on write access on sensitive drive parameters or some specific BACnet objects involved on the motor control. Meaning that if none of those data/parameters listed hereafter is accessed within timeout time, the timeout error will be raised by the drive.

Refresh of BACnet timeout shall involve the following access:

- Binary value object – Write on :
 - RUN/STOP CMD
 - FWD/REV CMD
 - FAULT RESET
 - CMD311CMD
 - CMD312CMD
 - CMD313CMD
 - CMD314CMD
 - CMD315CMD
- Scan objects in Analog value – Write on :
 - INPUT REF1
 - COM SCAN OUT 1 (if CMD or RFR address are defined in those parameters)
 - COM SCAN OUT 2 (if CMD or RFR address are defined in those parameters)
- Specific to **BACnet IP** implementation, following list of parameters over MBOX access refresh the timeout when a write access is performed:
 - AO1R, // Address 5261
 - PISP, // Address 8503
 - IL1R, // Address 5202
 - RPI, // Address 11920
 - NC1, // Address 12761
 - NC2, // Address 12762
 - NC3, // Address 12763
 - NC4, // Address 12764
 - NC5, // Address 12765
 - NC6, // Address 12766
 - NC7, // Address 12767
 - NC8 // Address 12768

NOTE: Parameters CMD / CMDD / RFR / RFRD are refused in write over MBOX.

BACnet Device Profiles and BIBBs

About BACnet Device Profiles

The BACnet standard identifies 6 device types, also known as device profiles:

- BACnet Operator Workstation (B-OWS)
- BACnet Building Controller (B-BC)
- BACnet Advanced Application Controller (B-AAC)
- BACnet Application Specific Controller (B-ASC)
- BACnet Smart Actuator (B-SA)
- BACnet Smart Sensor (B-SS)

BACnet Interoperability Building Blocks (BIBBs)

BACnet Interoperability Building Blocks (BIBBs) are collections of BACnet services.

Here is a list of BACnet Interoperability Building Blocks abbreviations used:

- DS: Data Sharing
- B: Server Role
- RP: Read Property
- WP: Write Property
- RPM: Read Multiple Property
- WPM: Write Multiple Property
- COV: Change of Value

The Change of Value service allows a client to subscribe to an object.

The device will send a notification according to the following conditions.

- For binary values objects, the notification is sent when the Present Value property changes.
- For analog values objects, the notification is sent when the Present Value property changes to a value greater than the COV increment configured.
- DDB: Dynamic Device Binding
- DOB: Dynamic Object Binding
- DCC: Device Communication Control
- RD: Reinitialize Device

Bacnet Services

The following table shows the services supported by the fieldbus module:

BACnet Service	BIBB	Family	Description
ReadProperty	DS-RP-B	Data Sharing	Provide the current value of one object property
WriteProperty	DS-WP-B	Data Sharing	Modify the current value of one object property
ReadMultipleProperty	DS-RPM-B	Data Sharing	Read several properties of several objects
WriteMultipleProperty	DS-WPM-B	Data Sharing	Write several properties of several objects

BACnet Service	BIBB	Family	Description
SubscribeCOV	DS-COV-B	Data Sharing	The drive accepts subscription and sends COV notification to the remote device.
ConfirmedCOVNotification			
UnconfirmedCOVNotification			
Who-Is	DM-DDB-B	Device and Network management	The device provides information about its attributes and answers to request to identify itself.
Who-Has	DM-DOB-B	Device and Network management	The device provides address information about its objects upon request.
I-Have	DM-DOB-B	Device and Network management	
DeviceCommunicationControl	DM-DCC-B	Device and Network management	The device responds to communication control exercised by the external device.
ReinitializeDevice	DM-RD-B	Device and Network management	The device performs reinitialization requests when requested.

Bacnet reset service

The `ReinitializeDevice` BACnet service can be used to reinitialize the communication link for both Bacnet IP and Bacnet MSTP.

Reinitialised state of Device	Effect on the Drive
COLDSTART	Acts as a power-on, it can be used to restart the communication
WARMSTART	
ACTIVATE_CHANGES	

BACnet Object

About BACnet Objects

BACnet objects are the logical representation of system data. Objects represent data that originate in physical inputs, physical outputs, or software processes (for example, single physical points or logical groupings / collections of points) that perform a specific function.

Binary input object

Object_Identifier	Object_Name (default)	Description	Object Access restriction	Property access restriction
0x00C00001	RO1 ACT	Indicates status of R1	NO	NO
0x00C00002	RO2 ACT	Indicates status of R2		
0x00C00006	DI 1 ACT	Value of LI1		
0x00C00007	DI 2 ACT	Value of LI2		
0x00C00008	DI 3 ACT	Value of LI3		
0x00C00009	DI 4 ACT	Value of LI4		
0x00C0000A	DI 5 ACT	Value of LI5		
0x00C0000B	DI 6 ACT	Value of LI6		

Binary output object

Object_Identifier	Object_Name (default)	Description	Object Access restriction	Property access restriction
0x01000000	RO 1 CMD	R1 relay out	NO	C if R1 value is NOR otherwise
0x01000001	RO 2 CMD	R2 relay out	NO	C if R2 value is NOR otherwise

Analog input object

Object_Identifier	Description	Object Access restriction	Property access restriction
0x00000000	Analog input value 1	NO	NO
0x00000001	Analog input value 2	NO	NO
0x00000002	Analog input value 3	NO	NO
0x00000010	Indicates status of AO1	NO	NO

Analog output object

Object_Identifier	Object_Name (default)	Description	Object Access restriction	Property access restriction
0x00400000	AO1 COMMAND	Analog output value 1	NO	C - if AO1 value is NOR - otherwise

Binary value object

About Status Word ETA	About Control Word CMD
<ul style="list-style-type: none"> ETA_1 for Bacnet MSTP ETA_3 for Bacnet IP 	<ul style="list-style-type: none"> CMD_1 for Bacnet MSTP CMD_3 for Bacnet IP

Object_Identifier	Object_Name (default)	Description	Object Access restriction	Property access restriction	Internal registers link
0x01400000	RUN/STOP ACT	Indicates the drive status	NO	NO	ETA_x bit 2
0x01400001	FWD/REV ACT	Indicate the motor rotation direction	NO	NO	ETA_x bit 15
0x01400002	FAULT ACT	indicate if the drive error status	NO	NO	ETA_x bit 3
0x01400004	HAND/AUTO ACT	Indicates if the drive is locally controller or not	NO	NO	ETA_x bit 9
0x01400007	DRIVE READY	The VSD is ready and wait for start command	NO	NO	ETA_x bit 1
0x01400008	AT SETPOINT	The VSD has reached the target speed	NO	NO	ETA_x bit 10
0x0140000A	RUN/STOP CMD	Command a drive start	NO	NO	Internal command channel. See CiA402 <ul style="list-style-type: none"> OFF = CMD_x bit 1&2 ON = CMD bit 0&3
0x0140000B	FWD/REV CMD	Command a motor direction change	NO	NO	CMD_x bit 11. See CiA402
0x0140000E	FAULT RESET	Reset error (rising edge)	NO	NO	ON = CMD_x bit 7. See CiA402
0x0140000F	MBOX READ	Command to read a parameter	NO	NO	NO
0x01400010	MBOX WRITE	Command to write a parameter	NO	NO	NO
0x01400012	C111CMD C311CMD (for Bacnet IP)	CMD word 3 bit 11	NO	NO	CMDx bit 11
0x01400013	C112CMD C312CMD (for Bacnet IP)	CMD word 3 bit 12	NO	NO	CMDx bit 12
0x01400014	C113CMD C313CMD (for Bacnet IP)	CMD word 3 bit 13	NO	NO	CMDx bit 13
0x01400015	C114CMD C314CMD (for Bacnet IP)	CMD word 3 bit 14	NO	NO	CMDx bit 14
0x01400016	C115CMD C315CMD (for Bacnet IP)	CMD word 3 bit 15	NO	NO	CMDx bit 15
0x01400017	STORE_CONFIG	CMI=2	NO	NO	CMI=2

Analog value object

Object Identifier	Object Name (default)	Description (no link with property)	Units	Present Value access	Relinquish default	COV_Increment	TV Drive param
0x00800000	OUTPUT SPEED	Outpt speed	ASN.1 - 104 - rpm	R		10rpm	SPD
0x00800001	OUTPUT FREQ	Output frequency	ASN.1 - 27 - Hz	R		3Hz	RFRD
0x00800003	OUTPUT VOLT	Motor voltage	ASN.1 - 5 - V	R		10V	UOP
0x00800004	CURRENT	Motor current	ASN.1 - 3 - A	R		0,1A	LCR
0x00800005	TORQUE	Motor torque	ASN.1 - 98 - %	R		3%	OTR
0x00800006	POWER	Motor power	ASN.1 - 98 - %	R		3%	OPR
0x00800007	DRIVE TEMP	Drive thermal state	ASN.1 - 98 - %	R		3%	THD
0x0080000A	PRC PID FBCK	PID regularor feedback	ASN.1 - 98 - %	R		3%	RPF
0x0080000B	PRC PID DEV	PID regularor feedback	ASN.1 - 98 - %	R		3%	RPE
0x0080000E	RUN TIME	Operating time	ASN.1 - 71 - H	R		0,1h	RTH
0x0080000F	MOTOR TEMP	Motor temperature	ASN.1 - 98 - %	R		5%	THR
0x00800010	INPUT REF 1	Velocity/ frequency setpoint from BacNet	ASN.1 - 98 - %	C	0	NA	LFR
0x00800012	LAST FAULT	Current error n	ASN.1 - 95 - NULL	R		NA	DP0
0x00800013	PREV FLT 1	Previous error n-1	ASN.1 - 95 - NULL	R		NA	DP1
0x00800014	PREV FLT 2	Previous error n-2	ASN.1 - 95 - NULL	R		NA	DP2
0x00800017	ACCEL1 TIME	Acceleration time	ASN.1 - 73 - s	W		NA	ACC
0x00800018	DECEL1 TIME	Deceleration time	ASN.1 - 73 - s	W		NA	DEC
0x00800019	MBOX PARAM	Parameter number	ASN.1 - 95 - NULL	W		NA	
0x0080001A	MBOX DATA	Parameter value	ASN.1 - 95 - NULL	W		NA	
0x0080001B	EXT PID STPT	PID regulator setpoint from Bacnet	ASN.1 - 98 - %	C	0	3%	PISP
0x0080001C	COM SCAN OUT1	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC1 (drive forward the value to register pointed by NCA1)
0x0080001D	COM SCAN OUT2	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC2 (drive forward the value to register pointed by NCA2)
0x0080001E	COM SCAN OUT3	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC3 (drive forward the value to register

Object_Identifier	Object_Name (default)	Description (no link with property)	Units	Present Value access	Relinquish default	COV_Increment	TV Drive param
							pointed by NCA3)
0x0080001F	COM SCAN OUT4	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC4 (drive forward the value to register pointed by NCA4)
0x00800020	COM SCAN OUT5	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC5 (drive forward the value to register pointed by NCA5)
0x00800021	COM SCAN OUT6	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC6 (drive forward the value to register pointed by NCA6)
0x00800022	COM SCAN OUT7	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC7 (drive forward the value to register pointed by NCA7)
0x00800023	COM SCAN OUT8	General purpose AV ==> Comm scan	ASN.1 - 95 - NULL	C	0	NA	NC8 (drive forward the value to register pointed by NCA8)
0x00800024	COM SCAN IN1	General purpose AV <== Comm scan	ASN.1 - 95 - NULL	R		NA	NM1 drive forward to register pointed by NMA1
0x00800025	COM SCAN IN2	General purpose AV <== Comm scan	ASN.1 - 95 - NULL	R		NA	NM2 drive forward to register pointed by NMA2
0x00800026	COM SCAN IN3	General purpose AV <== Comm scan	ASN.1 - 95 - NULL	R		NA	NM3 drive forward to register pointed by NMA3
0x00800027	COM SCAN IN4	General purpose AV <== Comm scan	ASN.1 - 95 - NULL	R		NA	NM4 drive forward to register pointed by NMA4
0x00800028	COM SCAN IN5	General purpose AV <== Comm scan	ASN.1 - 95 - NULL	R		NA	NM5 drive forward to register pointed by NMA5
0x00800029	COM SCAN IN6	General purpose AV <== Comm scan	ASN.1 - 95 - NULL	R		NA	NM6 drive forward to register pointed by NMA6

Object_Identifier	Object_Name (default)	Description (no link with property)	Units	Present Value access	Relinquish default	COV_Increment	TV Drive param
0x0080002A	COM SCAN IN7	General purpose AV <= Comm scan	ASN.1 - 95 - NULL	R		NA	NM7 drive forward to register pointed by NMA7
0x0080002B	COM SCAN IN8	General purpose AV <= Comm scan	ASN.1 - 95 - NULL	R		NA	NM8 (drive forward the value to register pointed by NMA8)

Device object

Bacnet IP

BACnet Property	Value
Object Identifier	OBJECT_DEVICE:1
Object Name	ATH230U06M2_17
Object Type	8 : Object Device
System Status	0 : Operational
Vendor Name	SCHNEIDER-ELECTRIC
Vendor Identifier	10
Model Name	ATH230U06M2
Firmware Revision	V1.11E1
Application Software Version	V0.71E1
Protocol Version	1
Protocol Revision	22
Protocol Services Supported	00000110000011111010000000000001110000-001000000100
Protocol Object Types Supported	1111111010100111100111011100011111010111-0000101000
Object List	Object[] Array
Max Apdu Length Accepted	1476
Segmentation Supported	0 : Both
Max Segments Accepted	22
Apdu Segment Timeout	5000
Apdu Timeout	6000
Number Of Apdu Retries	3
Device Address Binding	—
Database Revision	1
Active Cov Subscriptions	—

Bacnet MSTP

This content of this object is write protected. Max managers and Max info frames can be set using the network port object.

BACnet Property	Value
Property List	Object[] Array
System Status	0 : Operational
Vendor Name	Schneider Electric
Vendor Identifier	10
Model Name	ATH230U06M2
Firmware Revision	V1.11E1
Application Software Version	V1.11E1
Description	
Location	
Protocol Version	1
Protocol Revision	19
Max Apdu Length Accepted	480
Segmentation Supported	3 : None
Apdu Timeout	3000
Number Of Apdu Retries	10
Protocol Services Supported	00000100000010111100100000100000011000-000000
Protocol Object Types Supported	11111100100000000000000000000000000000-000000000000000000001000000
Object List	Object [] Array
Max MAster	10
Max Info Frames	10
Device Address Binding	
Database Revision	0
Active Cov Subscriptions	
Object Name	ATH230U06M2_001
Object Type	8: Object Device
Object Identifier	OBJECT_DEVICE: 1

Port object

BACnet IP

This is a standardized object.

IP Address parameters are linked to the parameters that can be set either using the local HMI or the DTM.

BACnet Property	Value
Object Identifier	OBJECT_NETWORK_PORT:0
Object Name	Internal port
Object Type	56 : Object Network Port
Status Flags	0000
Reliability	0 : No error detected
Out Of Service	False
Network Type	5 : Ipv4
Protocol Level	2 : Bacnet Application
Network Number	0
Network Number Quality	0 : Unknown
Changes Pending	False
Command	0: Idle
Mac Address	Byte[] Array
Apdu Length	1476
Link Speed	0
Bacnet Ip Mode	0: Normal
Ip Address	Byte[] Array
Bacnet Ip Udp Port	47809
Ip Subnet Mask	Byte[] Array
Ip Default Gateway	Byte[] Array
Ip Dns Server	Object[] Array
Ip Dhcp Enable	False
Fd Bbmd Address	ip_address 0.0.0.0 Port :47808
Fd Subscription Lifetime	0
Property List	Object[] Array

BACnet MSTP

When a parameter is changes, the bit changes pending is set to True.

To store values it's required to either reset the drive using BACnet reset or write the value using binary value property STORE CONFIG.

Values will be fully considered after a power cycle.

Property	Value
Object Identifier	OBJECT_NETWORK_PORT:1
Object Name	Network Port
Object Type	56 : Object Network Port
Status Flags	0000
Reliability	0 : No error detected
Out Of Service	False
Network Type	2 : Mstp
Protocol Level	2 : Bacnet Application
Network Number	0
Network Number Quality	0 : Unknown
Changes Pending	False
Mac Address	Byte[] Array
Apdu Length	480
Number Of Apdu Retries	10
Apdu Timeout	3000
Link Speed	19200
Link Speeds	Object[] Array
Link Speed Auto-negotiate	False
Max Master	10
Max Info Frames	10

Additional Functions

Full Parameter Access

By the use of indirect access, it is possible to read or write any of the internal parameters of the drive. Except:

- CMD
- CMDD
- LFR
- LFRD
- CMD3
- CMD1

This functionality is done by the following 4 objects:

MBOX DATA, MBOX PARAM, MBOX READ, MBOX WRITE.

NOTE: MBOX READ and MBOX WRITE automatically return back to inactive once command is sent. Always return 0 when read action is performed.

Reading a Parameter

1. Write the logical address of the parameter to the Present Value property of the MBOX PARAM object.
2. Set Present Value property of the MBOX READ to read.
3. The current value of the parameter can be read in the Present Value property of MBOX DATA object.

Writing a Parameter

1. Write the logical address of the parameter to the Present Value property of the MBOX PARAM object.
2. Write the new value in the Present Value property of the MBOX DATA object.
3. Set the Present Value property of MBOX WRITE to write.

NOTE: The modified parameters are not saved in EEPROM. If the values written have to be saved, it is needed to specify it by writing CMI bit 1 to 1. This command is only active if the drive is stopped.

Glossary

A

Abbreviations:

Req. = Required

Opt. = Optional

AC:

Alternating Current

Adjustment parameter: A parameter always accessible as **[Access Level]**.

ASN.1:

Abstract Syntax Notation One is a standard and notation for representation of units.

For BACnet, refer to BACnetEngineeringUnits ASN.1.

C

Configuration Parameter: A parameter affected by the operating states of the machine as **[Motor Nom Current]**.

Controller:

A **controller** is a device that is actively polling for data from one or multiple devices.

Similar to a **Master**, a **Client** or a **Scanner**.

D

DC:

Direct Current

dec.:

Decimal

Device:

A **device** is the passive device, waiting for the **controller** to poll for data to actually send it.

Similar to a **Slave**, an **Adapter** or a **Server**.

E

Error :

Discrepancy between a detected (computed, measured, or signaled) value or condition and the specified or theoretically correct value or condition.

F

Factory setting:

Machine status in factory settings when the product was shipped.

Fault Reset:

A function used to restore the drive to an operational state after a detected error is cleared by removing the cause of the error so that the error is no longer active.

Fault:

Fault is an operating state. If the monitoring functions detect an error, a transition to this operating state is triggered, depending on the error class. A "Fault reset" is required to exit this operating state after the cause of the detected error has been removed.

H

hex:

Hexadecimal

L

LSB:

Least Significant Byte

M

MEI:

Modbus Encapsulated Interface

P

PELV:

Protective Extra Low Voltage, low voltage with isolation. For more information: IEC 60364-4-41.

PLC:

Programmable logic controller.

Power stage:

The power stage controls the motor. The power stage generates current for controlling the motor.

S

SF: Switch Frequency

U

Unit Load:

According to the TIA-485A, a single Unit Load is equivalent to a 12 kΩ Impedance attached to the + and - data lines (connected to ground or supply).

V

VSD:

Variable Speed Drive

W

Warning:

If the term is used outside the context of safety instructions, a warning alerts to a potential error that was detected by a monitoring function. A warning does not cause a transition of the operating state.

Z

Zone of operation:

This term is used in conjunction with the description of specific hazards, and is defined as it is for a **hazard zone** or **danger zone** in the EC Machinery Directive (2006/42/EC) and in ISO 12100-1.

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.

© 2025 Schneider Electric. All rights reserved.

JPS43216.01