Altivar HVAC ATH600

Variable Speed Drives for Asynchronous and Synchronous Motors

BACnet MS/TP Embedded - BACnet IP VW3A3726 Manual

JPS89285.01
04/2026

www.se.com

Legal Information

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

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

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

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

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

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

Table of Contents

Safety Information

Important Information

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please Note

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

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

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 Ex 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 ATH630 and ATH650 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 ATH600 drives: ATH630 and ATH650.

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

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:

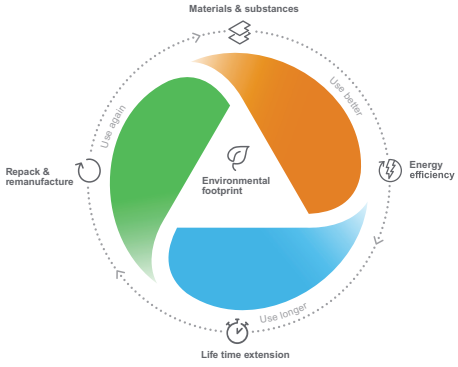
- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity 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 repairability 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:

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

Title of Documentation	Reference number	
Catalog: Altivar HVAC ATH600 variable speed drives	DIA2ED2260301EN (English)	DIA2ED2260301FR (French)
ATH600 Getting Started	NAT16141 (English) NAT16142 (French) NAT16143 (German) NAT16144 (Spanish)	NAT16149 (Italian) NAT16151 (Chinese) NAT27844 (Portuguese) NAT27843 (Turkish)
ATH600 Getting Started Annex (SCCR)	NAT16152 (English)	
ATH630, ATH650 Installation Manual	NAT19018 (English) NAT19019 (French) NAT19021 (German) NAT19022 (Spanish)	NAT19020 (Italian) NAT19024 (Chinese) NAT19026 (Portuguese) NAT19025 (Turkish)
ATH600 Programming Manual	NAT19027 (English) NAT19028 (French) NAT19031 (German) NAT19032 (Spanish)	NAT19029 (Italian) NAT19033 (Chinese) NAT19036 (Portuguese) NAT19035 (Turkish)
ATH600 Enclosed Handling Instruction Sheet	JPS53591 (English + French)	
ATH600 Enclosed Instruction Bulletin	JPS53593 (English)	JPT22730 (French)
ATH600 ATEX/IECEx Manual	JPS89265 (English)	
ATH600 Embedded Safety Function Manual	JPS89266 (English)	
ATV212 to ATH600 & ATH200 Substitution Manual	JPS89284 (English)	
ATH600 BACnet Manual	JPS89285 (English)	
ATH600 Modbus Manual	JPS89286 (English)	
ATH600 communication addresses	JPS89292 (English)	
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)	
ATH600: DTM	ATH600_DTM_Library_EN (English - to be installed first) ATH600_DTM_Lang_FR (French) ATH600_DTM_Lang_DE (German)	ATH600_DTM_Lang_SP (Spanish) ATH600_DTM_Lang_IT (Italian) ATH600_DTM_Lang_CN (Chinese)
ATH600 Application Note – Air handling units	JPS89313 (English)	
ATH600 Application Note – Fire modes	JPS89316 (English)	
ATH600 latest Firmware	ATH600-Firmware	

EcoStruxure Automation Device Maintenance	EcoStruxure Automation Device Maintenance (English)	
EcoStruxure Automation Device Maintenance - Altivar User Manual	JYT50472 (English)	JYT50485 (Portuguese)
	JYT50482 (German)	JYT50484 (Turkish)
	JYT50474 (French)	JYT50483 (Chinese)
	JYT50476 (Spanish)	
	JYT50478 (Italian)	

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/UL 60204-1: Safety of machinery - Electrical equipment of machines – Part 1: General requirements.
- IEC/UL 61010: Safety requirements for electrical equipment for measurement, control, and laboratory use.
- IEC 61158 series: Industrial communication networks - Fieldbus specifications
- IEC/UL 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/UL 61800 series: Adjustable speed electrical power drive systems.
- IEC 61918: Industrial communication networks - Installation of communication networks in industrial premises.
- IEC 62443 /UL 2900: 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.

Also see the Glossary at the end of this manual.

Contact us

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

Schneider Electric

1884 Boulevard de la Défense

92000 Nanterre

France

Hardware Setup

What's in This Part

BACnet MSTP Network Configurations

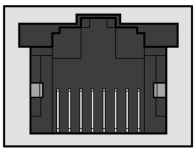
Modbus/ BACnet MSTP Port usage

To use the port with the BACnet MSTP configuration, use the parameter **[Embedded Protocol]** COM (**[Communication]** COM– ➡ **[Comm parameters]** CMP– ➡ **[Emb Serial Line]** SPC–) and select **[Bacnet MS/TP]** EBM, 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 (Modbus signals)
5	D0 (Modbus signals)
6	Reserved
7	VP, 12 Vdc **NOTE:** Supply for RS232 / RS485 converter or a remote terminal.
8	Common (Modbus signals)

Open Style Modbus/BACnet MSTP Connection

NOTE: The two physical connectors, Modbus VP12S and Open Style, correspond to a single logical port. **Internally they are connected to the same RS-485 interface**.

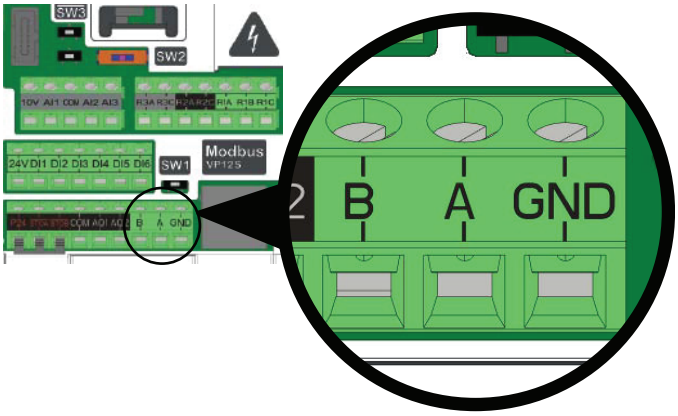
Only one port should be used at the same time to communicate with an external device. But a display terminal and a communication with an external device can be connected at the same time (one on each port).

⚠WARNING

LOSS OF CONTROL

- Never use the two available communication ports at the same time when they are connected to different PLC, otherwise any communication interruption cannot be detected.

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

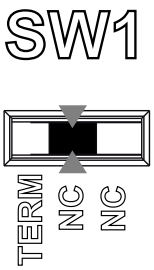


Pin	Signal
B	BACnet MS/TP RS-485 differential data line (+)
A	BACnet MS/TP RS-485 differential data line (-)
GND	Common reference reserved for BACnet MS/TP application. **NOTE:** GND is not the same as protective earth ground and should not be tied to earth ground except at one point in the network.

Modbus adaptor cable — LV434211

Use the cable Modbus adaptor cable LV434211.

Information on the use of switch SW1



- TERM = 120Ω termination enabled
- NC = No termination

NOTE: In BACnet MS/TP configuration, it is necessary to place the switch SW1 to the left, at TERM position.

NOTE: It is recommended to use a tool to change the switch position.

RS485 Bus Schematic

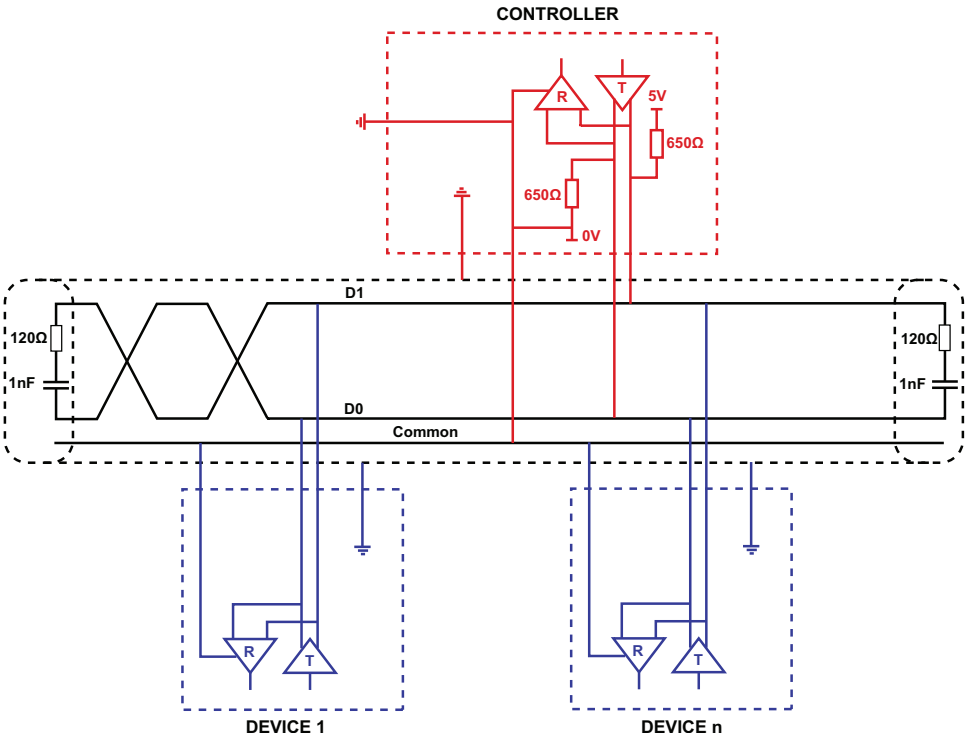
The RS485 standard allows variants of different characteristics:

- 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	• 20 m for 1 tape link • 40 m divided by the number of tape links on a multiple junction box
Bus polarization	• 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) This polarization is recommended for the controller.
Velocity of propagation	78%
Capacitance	< 41.0105 pF/m (12.5 pF/ft) between conductors
	< 72.1784 pF/m (22 pF/ft) between the conductor connected to ground and the next conductor
Line termination	Two polarization of the pair are available with a R or RC circuit as line termination: • R circuit: One 150Ω resistor. • RC circuit: One 120Ω 0.25W resistor in series with 1nF 10V capacitor. **NOTE:** An analysis is to be carried out to determine which solution is best suited for the network topology.
Common polarity	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.

BACnet IP Network Configurations

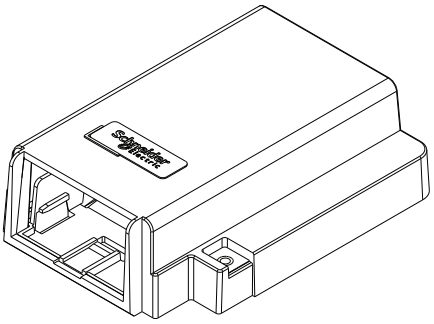
BACnet Fieldbus Module

The following figure shows the VW3A3726 BACnet module:

NOTE: the sticker with "*PW XXXXX*" is not applicable for ATH600 products.

VW3A36001 – Module adapter

For frame size 0 to 2B, to use VW3A3726 BACnet module, install the VW3A36001 module adapter first.



Firmware version

The VW3A3726 BACnet IP module is compatible with, at least, V1.1IE02 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

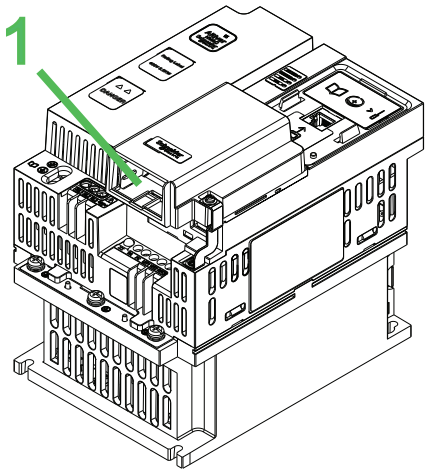
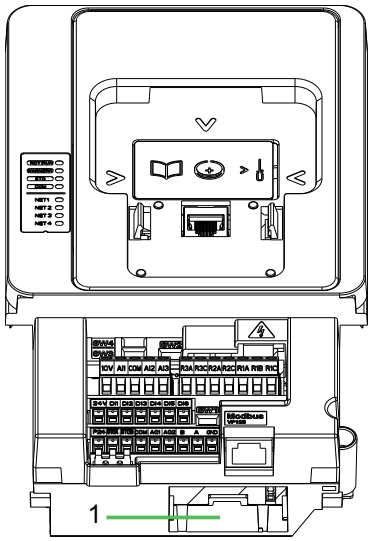
Check that the module catalog number marked on the label is the same as that on the delivery note corresponding to the purchase order.

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.
3	Insert the module.
4	Check that the module is correctly inserted and locked mechanically in the drive.

Control Unit Port (LHP)	Control Unit Port (HHP)
	

Legend:

1 VW3A36001 – Module adapter or 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.

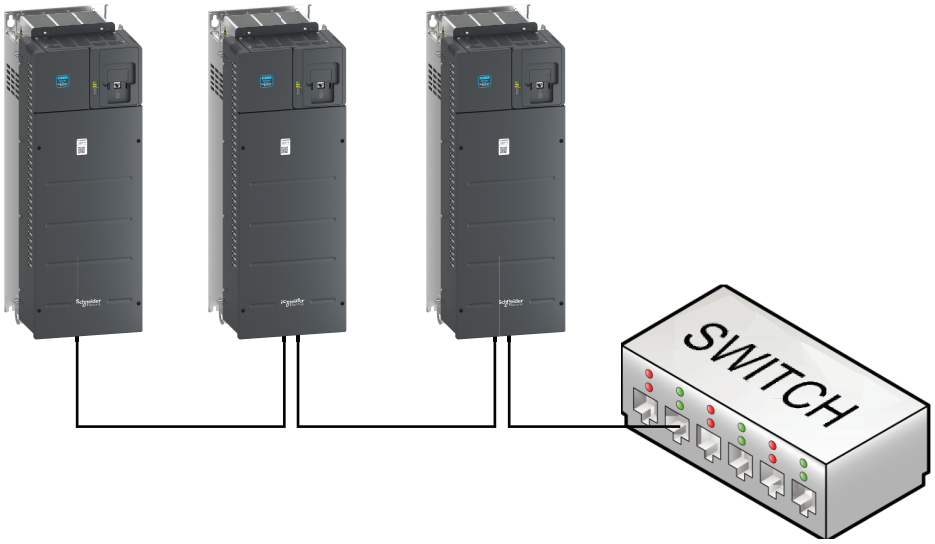
Installation Topology

Daisy chain topology is the recommended topology to use on BACnet IP networks.

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.

NOTE:

- Star networks can be supported.
- Ring networks are not supported.



Cybersecurity Generalities

What's in This Part

Overview

Title of documentation	Catalog number
Recommended Cybersecurity Best Practices	7EN52-0390 (English)

NOTE: In case of using an option module, please refer to the corresponding fieldbus manual in Related Documents, page 12 for additional information.

The objective of Cybersecurity 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 Cybersecurity 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.

Network administrators, system integrators and personnel that commission, maintain or dispose of a device should:

- Apply and maintain the device's security capabilities.
- Review assumptions about protected environments.
- Address potential risks and mitigation strategies.
- Follow recommendations to optimize cybersecurity.
- See the programming manual for details about:
  - Address potential risks and mitigation strategies (Product Defense-in-depth).
  - Login
  - Logout
  - Account Management
  - Password
  - PIN code
  - Admin Credentials Recovery
  - Save and Restore a Security Policy
  - Security Functionality Verification
  - Clear Device / Secure Decommissioning

For detailed information on the system defense-in-depth approach, refer to the TVDA: How Can I Reduce Vulnerability to Cyber Attacks (STN V3.0) on se.com.

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

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default password to help prevent unauthorized access to device settings and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least rights, separation of duties) to help prevent unauthorized exposure, loss or modification of data and logs, interruption of services, or unintended operation.

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

Protected Environment Assumptions

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.

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 authorized 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

- 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 devices 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

⚠WARNING

ACCESSIBILITY LOSS

- Setup a security policy to your device and backup the device image with security administrator user account.
- Define and regularly review the password policy.
- Periodic change of the passwords, Schneider Electric recommends a modification of the password each 90 days.

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

Cybersecurity helps to provide:

- Confidentiality (to help prevent unauthorized access)
- Integrity (to help prevent unauthorized modification)
- Availability/authentication (preventing the denial of service and assuring authorized access)
- Non-repudiation (preventing the denial of an action that took place)
- Traceability/detection (logging and monitoring)

Norm IEC 62443 is the worldwide standard for security of industrial control system (ICS) networks.

The Altivar HVAC ATH600 holds certification for IEC 62443-4-1 for Secure Development Lifecycle and IEC 62443-4-2 Security Level 1 (SL1) for Security features provided. The certification applies to products with a firmware version V1.1 IE03 or later. The firmware can be updated, please refer to .

Altivar HVAC ATH600 security features prevent the unauthorized disclosure of information via eavesdropping or casual exposure.

All the security rules implemented in the ATH600 are in complement of the points mentioned above.

The device does not have the capability to transmit data encrypted using the following protocols: Modbus slave/BACnet MS/TP over serial. 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 or DTM should have an updated anti-virus, anti-malware, anti-ransomware application activated during the use.

The ATH600 has the capability to export its settings and files manually or automatically. It is recommended to archive any settings and files (device backup images, device configuration, device security policies) in a secure area.

Product Defense-in-Depth

ATH600 offers the following security features:

Threats	Desired security property on Embedded Device	ATH600 security features
Information disclosure	Confidentiality	Password encrypted in a non-reversible way
		User access control
Tampering	Device integrity	Cryptographic signature of firmware package
		Secure root of trust
Denial of Service	Availability	Device backup/restore
		Security export/import
Spoofing/Elevation of privilege	User Authentication / Authorization	Strong password and user account policy
		Access control local display terminal
		Access control commissioning tools Modbus Serial
		Access control commissioning through option board
Elevation of privilege	Authorization	Port hardening
		User roles & rights
Repudiation	Non-repudiability	Secure event logging

Confidentiality

Information confidentiality capacity prevents unauthorized access to the device and information disclosure.

- The user access control helps on managing users that are authorized to access the device. Protect user credential at usage.
- The user’s passwords are encrypted in non-reversible way at rest

Device Integrity Protection

The device integrity protection prevents unauthorized modification of the device with tampered or spoofed information.

This security capability helps protect the authenticity and integrity of the firmware running on the ATH600 and facilitates protected file transfer: digitally signed firmware is used to help protect the authenticity of the firmware running on the and only allows firmware generated and signed by Schneider Electric.

- Cryptographic signature of the firmware package executed at the firmware update
- Secure root of trust ensures integrity and authenticity of the device firmware at each power-up

Availability

The control system backup is essential for recovery from a control system failure and/or misconfiguration and participate on preventing denial of service. It also helps ensure global availability of the device by reducing operator overhead on security application/deployment.

These security capabilities help manage control system backup with the device:

- Independent security policy import/export for local secure backup and security policy sharing with other devices.
- Complete device backup/restore available on local HMI, DTM.

Authentication and Authorization

The user authentication helps prevent the repudiation issue by managing user identification and prevents information disclosure and device integrity issues by unauthorized users.

These security capabilities help enforce authorizations assigned to users, segregation of duties and least rights:

- User authentication is used to identify and authenticate software processes and devices managing accounts
- Device Password policy and password strength configurable using SoMove and DTM
- Authorization managed according to channels
- User account lockouts configurable with number of unsuccessful login attempts

In line with user authentication and authorization, the device has access control cryptographic features to check user credential before access is granted to the system.

In the ATH600, the control of accessibility to the settings, parameters, configuration, and logging database is done with a user authentication after "Log in", with a name and password.

The ATH600 controls the access through :

- SoMove DTM (Serial and through Option Board connection)

Port Hardening

The communication ports of the ATH600 can be disabled. Logical ports can be enabled/disabled. Port hardening configuration can be set from SoMove DTM with the ADMIN or SecAdmin right.

Security Event Logging

The security event logging prevents the repudiation issues by ensuring traceability and detection of any service executed and affecting the security policy of the device.

These security capabilities support the analysis of security events, help protect the device from unauthorized alteration and records configuration changes and user account events:

- Human-readable reports for device security settings
- Audit event logs to identify:
  - The ATH600 security configuration modification
  - The device users' activity (e.g. login, logout)
  - The device firmware updates
  - Audit storage capacity of 500 security event logs
  - Timestamps, including date and time, match ATH600 clock

ATH600 Security Policy

To facilitate cybersecurity first configurations, the ATH600 offers 2 security policies with preset ATH600 security features. This operation applies default values adapted to the security level targeted by the system of which the device is part.

Selection of these 2 security policies can be done upon first power up of the device, both with the display terminal (Refer to for more information) and Commissioning tool (DTM).

Security Policy “Minimum”

This policy offers a minimum of cybersecurity features. User access control (login & password check at connection) is disabled across various software tools and platforms used for system configuration. These connections remain unsecured and open to potential elevation of privilege. This policy is intended for installations where authentication and authorization constraints are managed by external access control mitigation. When the Minimum policy is selected, each user accessing the device is considered to have ADMIN role and privileges.

Security Policy “Advanced”

This policy presets the device security by enabling security features. The user access control is enabled across various software tools and platforms used for system configuration. When activating the "Advanced" security policy, the user is identified as ADMIN and is requested to create a password unique to the device. During the initial setup, the user is invited to define a new password even if a default password is proposed .
If initial setup is done on DTM, there is no use of default password

Refer to the following cybersecurity features summary per security policy:

ATH600 security feature	Open for configuration (activation or settings)	Preset security policy	
		Minimum	Advanced
Password encrypted in a non-reversible way	-	-	✓
User access control	-	-	✓
Cryptographic signature of firmware package	-	✓	✓
Secure root of trust	-	✓	✓
Device backup	ADMIN or SecAdmin only	✓	✓
Device restore	ADMIN or SecAdmin only	✓	✓
Security Save	ADMIN or SecAdmin only	-	✓
Security Restore	ADMIN or SecAdmin only	✓	✓
User management	ADMIN or SecAdmin only	-	✓
Strong password/pin code policy	ADMIN or SecAdmin only	-	✓
Brute force and session timeout	ADMIN or SecAdmin only	-	✓
System use notification	ADMIN or SecAdmin only	-	✓
Access control: • Display terminal • Commissioning tools (Modbus Serial and Option Module)	For all users	✓	✓
Secure events recorded	ADMIN or SecAdmin only	✓	✓
Port hardening	ADMIN or SecAdmin only	-	✓

Import / Export Security Policy

The device security settings can be exported from a device to be archived and/or applied in the same or another device. Exporting a security policy generates a corresponding security policy file, which uses the .secp file extension.

The following table describes the security settings included in the security policy export:

Security settings	Included in import / export operation
User access control settings	✓
Password & Pin code policy, including session lock and user account lockout configuration	✓
User database, including username, password, pin codes and roles	✓
Password history	✓
Ports and Service management, Brute force mitigation and session timeout, system use notification	✓
Device default password	For security reasons, the default password is unique to each device and cannot be exported.
Security events	The security events base is private property of a device and cannot be applied to another device.

NOTE: When a security configuration file is loaded, please restart the device to apply it.

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.	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: • Modbus Serial • BACNet MS/TP • BACNet IP • Modbus TCP	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 (Option module), encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution. See **Protected Environment Assumptions**, page 26.
Security banners	The local display terminal cannot display the security banner.	The users connecting to the ATH600 will not be able to be warned about potential security notifications.	If such security notification shall be shared with users, then a local message shall be added close to the ATH600. Example: A sticker on the electrical cabinet or the electrical room can inform user about specific security considerations

Data Flow Restriction

A firewall device is required to secure the access to the device and limit the data flow.

For detailed information, refer to the TVDA: How Can I Reduce Vulnerability to Cyber Attacks (STN V3.0).

Device Recovery and Reconstitution

Control system backup – available and up-to-date backups for recovery from a control system failure.
Available and up-to-date firmware package for recovery from a system disaster.
The customer stores the current used firmware version package or the latest up-to-date firmware package available on **se.com**.

Both Control System backup and firmware package, shall be considered as assets with dedicated risk analysis according to your local Cybersecurity policy. Make sure the access and use of these files are protected by appropriate security controls to ensure the trust, availability and effectiveness of the device's disaster recovery plan.

NOTE:

- Complete device recovery can be performed by applying the firmware update package and the device backup image previously stored by the customer.
- In case of a firmware recovery on the product is not possible, please contact your local Schneider Electric representative.

Upgrades Management

When the Altivar HVAC ATH600 firmware and option fieldbuses are upgraded, security configuration remains the same until changed, including usernames and passwords. Refer to the programming manual for more information.

It is recommended that security configuration is reviewed after an upgrade to analyze rights for new or changed device features and revoke or apply them according to your company’s policies and standards.

Port Hardening

It is possible to disable a communication port or a specific protocol from ATH600 DTM Admin tab on SoMove with the ADMIN or SecADMIN rights.

The table below gives an overview of the physical ports that can be disabled :

Interface / Port	Settings	Default
Modbus Serial Ports		
RJ45/HMI	ON / OFF(1)	ON
RJ45/Network	ON / OFF(1)	ON
BACNet MS/TP Port		
RJ45/Network	ON / OFF	ON
Communication Option Modules		
BACNet IP	ON / OFF	ON

(1) Either RJ45/HMI port or RJ45/Network port is always available to keep local access for Graphic Display Terminal, commissioning access or ports and service configuration.

NOTE: A change in configuration of the ports above is considered after a power cycle.

NOTE: RJ45/Network port is the same physical port for both Modbus Serial and BACnet MS/TP

BACnet IP Services

BACnet IP Services	Settings
Modbus TCP	ON / OFF

Security Functionality Verification

When the cybersecurity policy and functionalities have been configured, it is strongly recommended to verify that the following functions are working as intended.

NOTE: If VW3A3726 is used, the tests must be done through the option fieldbus.

Human User Access Control

The user access control can be individually tested on each interface of the ATH600. Please reproduce the following steps for each individual ATH600 interface:

Interface	Step	Action	✓
• Commissioning tools connected on the Modbus Serial interface • Commissioning tools connected on the option module.	1	Try to connect to the selected interface	
	2	Confirm the security banner is displayed prior authentication is requested	
		Confirm security banner message is in conformity with the message to be displayed for your organization.	
	3	Try to log in to ATH600 with no password or wrong password. **Result:** access denied.	
	4	Try to login with more than the MaxLoginAttempts (Default value : 5) with wrong password **Result:** The account is locked during Lock Duration (Default value 240s)	
		Confirm the account is locked as well on other interfaces (SoMove (DTM))	
	5	During this Lock Duration, connect another account with the right password. **Result:** access granted.	
Display Terminal access control (if enabled)	1	Try to log in to the Display Terminal with no PIN code or a wrong PIN code **Result:** access denied.	
	2	Try to log in with more than the MaxLoginAttempts (Defalut value : 5) with wrong PIN code **Result:** The account is locked during Lock Duration (Default value : 240s)	
	3	During this Lock Duration, connect another account with the right password. **Result:** access granted.	

Confirm that access control is in conformity with the access control configuration requested for your installation.

Password & PIN code Policy

Step	Action	✓
1	Connect to SoMove with your own account	
2	Try to modify your own password	
	Confirm that the password policy displayed is in conformity with the password policy expected for your installation.	
	Change your password, confirm that the selected password is accepted only if it's compliant with the password policy.	
3	Try to modify your own PIN code.	
	Confirm that the PIN code policy displayed is in conformity with the PIN code policy expected for your installation.	
	Change your PIN code, confirm that the selected PIN code is accepted only if compliant with the PIN code policy.	

Timeout Session

Step	Action	✓
1	Connect to DTM or the Display Terminal with right credentials	
2	Do nothing during the time defined in timeout tab for the specific channel. **Result:** The session is automatically disconnected	

Audit

Step	Action	✓
1	After some or all the preceding tests, access the logging page of SoMove (ADMIN or SecADMIN account is requested)	
2	Download the log file	
3	Check that the user activity is correctly monitored in the system log files	

Firmware Update

Step	Action	✓
1	Connect to SoMove	
2	Verify the version of each individual firmware version of the ATH600 and option module.	
3	Confirm that the versions are as expected	
4	Try to perform a firmware update	
5	Select a random file	

Disabling Communication Ports

Step	Action	✓
1	For each individual port disabled by configuration	
2	Confirm the ports are no longer usable	
	No data flow detected as output and no data accepted as input	
3	For each individual port disabled by configuration, confirm the protocol refuses communication according to the column verification of chapter Port Hardening, page 39	

Software Setup

What's in This Part

Software Overview

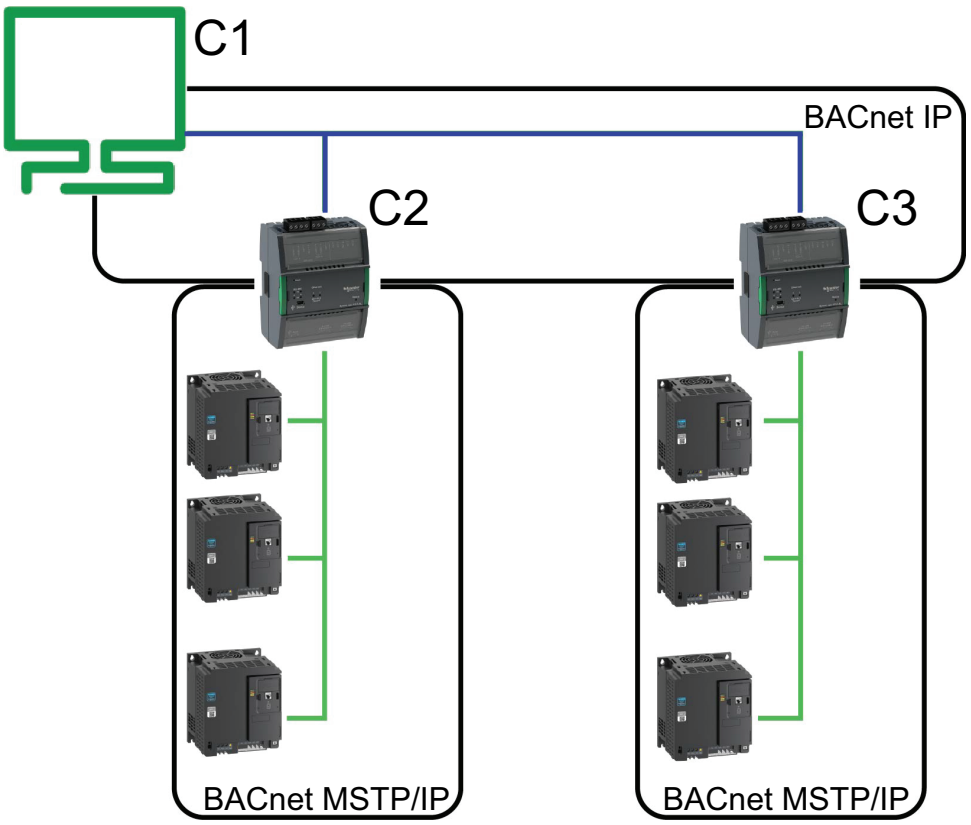
About BACnet

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.

BACnet Network example



C1: EBO (Manager)

C2: Subordinate

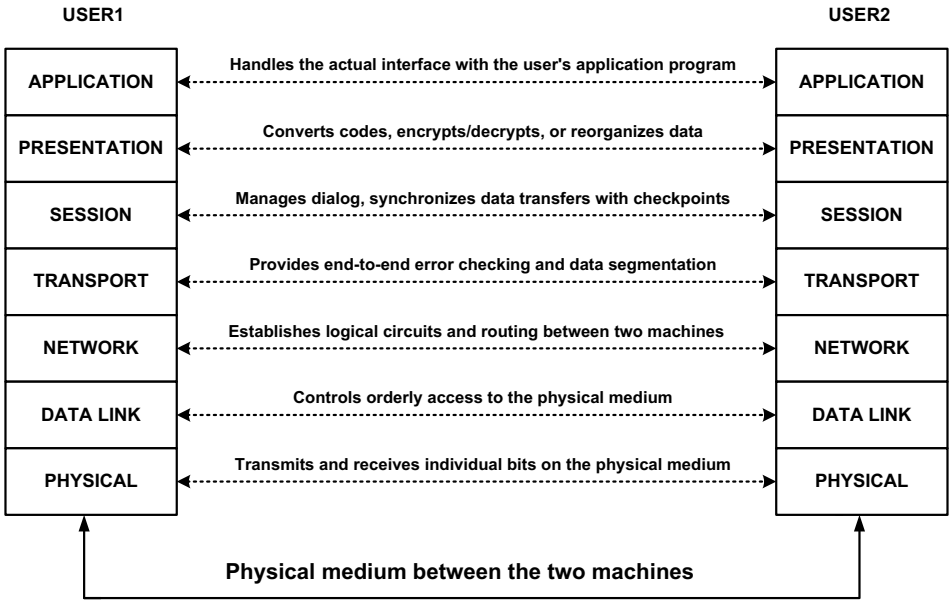
C3: Subordinate

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

<table>
<tr><th colspan="9">BACnet Layers</th><th>Equivalent OSI Layers</th></tr>
<tr><td colspan="9">BACnet Application Layer</td><td>Application</td></tr>
<tr><td colspan="9">BACnet Network Layer</td><td>Network</td></tr>
<tr><td colspan="2">ISO 8802-2 (IEEE 802.3)</td><td>MS/TP</td><td>PTP</td><td>LonTalk</td><td colspan="2">BACnet Virtual Link Layer</td><td>BACnet Data Link Layer</td><td>Secure Connect

BACnet Virtual Link Layer</td><td>Data Link</td></tr>
<tr><td>ISO 8802-3

(IEEE 802.3)</td><td>ARCNET</td><td>EIA-485</td><td>EIA-232</td><td></td><td>IPv4</td><td>IPv6</td><td>Zigbee</td><td>Web-Socket</td><td>Physical</td></tr>
<tr><td colspan="2">VW3A3726</td><td colspan="7">MSTP Embedded</td><td></td></tr>
</table>

BACnet MS/TP parameters

Access

The parameters are accessible in the **[Communication]** COM– → **[Comm parameters]** CMP → **[Bacnet MS/TP]** EBM- menu.

- When BACnet MS/TP is enabled through the VP12S port, the display terminal is unavailable and SoMove cannot connect.

Switch mode between Modbus and BACnet MS/TP for the Modbus VP12S port

The parameters are accessible in the **[Communication]** COM– → **[Emb Serial Line]** SPC- .

The parameter **[Embedded Protocol]** COM defines the Serial fieldbus switch mode.

The list presents the parameter settings:

- **[Bacnet MS/TP]** EBM
- **[Modbus]** MDB

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

[MS/TP Address] BADR

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... 127	0	R/W	16#7210 = 29200

[MS/TP Baudrate] BBDR

This parameter defines the BACnet MS/TP baud rate.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[Automatic]	Auto	19200	R/W	16#7211 = 29201
[9600 bsp]	9600			
[19200 bps]	19200			
[38.4 Kbps]	38400			
[76.8 Kbps]	76800			

[MS/TP Frame Format] BFOR

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]	8n1	[8-N-1]	R	16#7212 = 29202

[MS/TP Timeout] BTLP

This parameter defines the BACnet MS/TP fieldbus timeout.

NOTE: A **[MS/TP Com Interrupt]** BELF 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]** BTLP parameter.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1.0...6000.0 s]	1...60000	4.0 s	R/W	16#7213 = 29203

[MS/TP Device Inst Nb] BDIN

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

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...4194303]	0...4194303	1	R/W	16#721D = 29213

[MS/TP Max Master Nb] BMMN

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]	1...127	1	R/W	16#7217 = 29207

[MS/TP Max info frame] BMIF

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]	1...100	10	R/W	16#7218 = 29208

[MS/TP Rx frame count] BTFR

This parameter displays the total number of received frames.

The table presents the parameter settings:

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

[MS/TP Tx frame count] BTFS

This parameter displays the total number of transmitted frames.

The table presents the parameter settings:

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

[MS/TP Error Frames] BEFC

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]	0...65535	–	R	16#721B = 29211

[MS/TP APDU Retries] APDR

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]	1...10	3	R	16#7228 = 29224

[MS/TP APDU Timeout] APDT

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]	1...100	6 s	R	16#7229 = 29225

BACnet IP parameters

Access

The parameters are accessible in the **[Communication]** COM– → **[Comm parameters]** CMP → **[BACnet IP Config]** BAIP– menu.

[Device Name] PANM

This parameter is used to set the device name.

[MAC @] MAC

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

[IP mode] IPM

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

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
• **[Fixed]** : Manually set the IP address. • **[DHCP]** : Automatically gets the IP address from the DHCP server using the device name.	• MANU • DHCP	**[DHCP]**	R/W	16#FBC2 = 64250

[IP address] IPC1, IPC2, IPC3, IPC4

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]** IPM is set to **[Fixed]** MAnu.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R/W	IPC1: 16#FAD4 = 64212 IPC2: 16#FAD5 = 64213 IPC3: 16#FAD6 = 64214 IPC4: 16#FAD7 = 64215

[Mask] IPM1, IPM2, IPM3, IPM4

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]** IPM is set to **[Fixed]** MAnu.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R/W	IPM1: 16#FAD8 = 64216 IPM2: 16#FAD9 = 64217 IPM3: 16#FADA = 64218 IPM4: 16#FADB = 64219

[Gateway] IPG1, IPG2, IPG3, IPG4

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]** IPM is set to **[Fixed]** MAnu.

The table presents the parameter settings:

Factory settings	Access	Logic address
-	R/W	IPG1: 16#FADC = 64220 IPG2: 16#FADD = 64221 IPG3: 16#FADE = 64222 IPG4: 16#FADF = 64223

[Bacnet IP Mode] BAIM

This parameter defines the BACnet IP manager mode.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[Bacnet Normal] **[Bacnet Foreign]**	NORM FORE	**[Bacnet Normal]**	R/W	16#FB23 = 64291

[Bacnet IP UDP port] BAIU

This parameter defines the BACnet IP UDP port.

The table presents the parameter settings:

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

[Bacnet IP Time-Out] BATT

This parameter defines the BACnet IP fieldbus timeout.

NOTE: A **[Fdbus Com Interrupt]** CNF 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]** BATT parameter.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[1.0...6000.0 s]	1...60000	30.0 s	R/W	16#FB26 = 64294

[B IP Timeout Mode] BATM

This parameter defines the BACnet IP fieldbus timeout mode.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[BACnet Ctrl Traffic]: Write request on main drive parameters to control the motor.	MMC	**[BACnet All Traffic]** MBT	R/W	16#FB2B = 64299
[BACnet All Traffic]: Presence of BACnet IP network traffic.	MBT			

[BACnet IP Inst Nb] BAXP

This parameter defines the BACnet IP device instance number.

The table presents the parameter settings:

Settings	Code	Factory settings	Access	Logic address
[0...4194303]	0...4194303	1	R/W	16#FB28 = 64296

[IP APDU Retries] APRI

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]	1...10	3	R/W	16#FB27 = 64295

[IP APDU Timeout] APTI

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]	1... 100	6 s	R/W	16#FB2A = 64298

[APDU Seg Timeout] APSI

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]	1... 100	5 s	R/W	16#FB2A = 64298

Most Common parameters

For more information about the Communication Parameter Addresses, please refer to the ATH600 Communication Parameter Addresses.

NOTE: Cannot write cyclically configuration parameters (as the device can remain in **[Freewheel]** NST) tagged by R/WS.

Base Monitoring

Code	Settings	
[Motor Current] LCR	Logic address: 0C84 hex = 3204	Type: UINT (Unsigned16) Read/write: R
Motor current RMS Motor current. Average of the three line currents based on the measurement of the fundamental of the motor line currents.		
[Motor Therm State] THR	Logic address: 259E hex = 9630	Type: UINT (Unsigned16) Read/write: R Unit: 1 %
Motor thermal state This parameter monitors the motor thermal state. 100% corresponds to the nominal thermal state at the nominal motor current set to **[Motor Nom Current]**.		
[Motor Run Time] RTH via communication	Logic address: 0CAC hex = 3244	Type: UINT (Unsigned32) Read/write: R Unit: 1 s
Motor run time This parameter monitors how long the motor has been energized.		
[Motor Run Time] RTHH via Display Terminal	Logic address: 0CCA hex = 3274	Type: UINT (Unsigned32) Read/write: R/WS Unit: 1 s
Motor run time This parameter monitors how long the motor has been energized.		

Digital I/O

Code	Settings	
[Logic Inputs States] IL1R	Logic address: 1452 hex = 5202	Type: WORD (BitString16) Read/write: R Unit: -

Logic inputs states
This parameter is used to monitor the real value of the **[Logic Inputs States]**.

- Bit0 : "DI1" Digital inputs real image
- Bit1 : "DI2" Digital inputs real image
- Bit2 : "DI3" Digital inputs real image
- Bit3 : "DI4" Digital inputs real image
- Bit4 : "DI5" Digital inputs real image
- Bit5 : "DI6" Digital inputs real image
- Bit10: "DI11" Digital inputs real image (with VW3A3203)
- Bit11: "DI12" Digital inputs real image (with VW3A3203)
- Bit12 : "DI13" Digital inputs real image (with VW3A3203)
- Bit13 : "DI14" Digital inputs real image (with VW3A3203)
- Bit14 : "DI15" Digital inputs real image (with VW3A3203)
- Bit15 : "DI16" Digital inputs real image (with VW3A3203)

NOTE: The status of inputs can be read via **[Logic Inputs States]** IL1R to which a position or level sensor has been wired.

[Logic Outputs States] OL1R	Logic address: 145C hex = 5212	Type: WORD (BitString16) Read/write: R/W Unit: -

Logic outputs states
This parameter is used to write output value or monitor the value depending on if a function is assigned to the corresponding output:

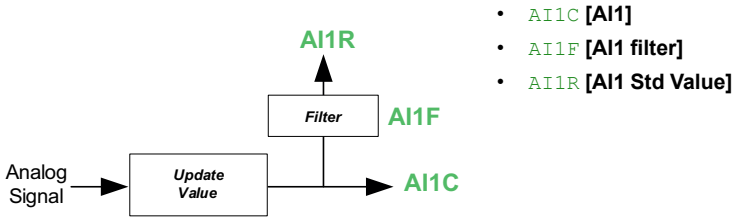
- Bit0 : "R1" relay real image
- Bit1 : "R2" relay real image
- Bit2 : "R3" relay real image
- Bit3 : "R4" relay real image (with VW3A3204)
- Bit4 : "R5" relay real image (with VW3A3204)
- Bit5 : "R6" relay real image (with VW3A3204)
- Bit12 : "DQ11" Digital outputs real image (with VW3A3203)
- Bit13 : "DQ12" Digital outputs real image (with VW3A3203)

NOTE: To write an output through communication, no function should be assigned to the corresponding output. Otherwise, writing on the bit linked to the corresponding output has no impact. If an error is triggered, outputs written through communication returns to 0.

NOTE: It is only possible to write the output through the active command channel. Consequently, forced outputs can not be disabled on local channel (such as display terminal).

Analog input

The following diagram explains how the analog input works:



- AI1C **[AI1]**
- AI1F **[AI1 filter]**
- AI1R **[AI1 Std Value]**

Code	Settings	
[AI1] AI1C	Logic address: 147A hex = 5242	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI1 This parameter is used to monitor the real value of the **[AI1]**. • (AI1T == "0A"): 0.001 mA • (AI1T == "10U") : 0.001 V • (AI1T == "LEVEL") : 0.01 kOhm • else : 0.001 V		
[AI1 filter] AI1F	**Setting range:** 0...10 s **Factory setting:** 0 s Logic address: 1164 hex= 4452	Type: UINT (Signed16) Read/write: R/W Unit: seconds
AI1 filter This parameter sets the cutoff time of the low filter for PTC1/AI1. The low pass filter aims to suppress electrical noise and avoid interference issue in the input signal.		
[AI1 Std Value] AI1R	Logic address: 1470 hex= 5232	Type: INT (Signed16) Read/write: R Unit: -
Analog input 1 standardized value Real image of AI1 consumed by functions.		
[AI2] AI2C	Logic address: 147B hex = 5243	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI2 AI2 customer image (1mV, 0.001mA) • (AI2T == "0A") : 0.001 mA • (AI2T == "10U") : 0.001 V • (AI2T == "PTC") : 0.01 kOhm • (AI2T == "KTY") : 1 Ohm • (AI2T == "1PT3") : 1 Ohm • (AI2T == "1PT2") : 0.1 Ohm • (AI2T == "LEVEL") : 0.01 kOhm • else : 0.001 V		

Code	Settings	
[AI2 Std Value] AI2R	Logic address: 1471 hex = 5233	Type: INT (Signed16) Read/write: R Unit: -
Analog input 2 standardized value AI2 real application image		
[AI3] AI3C	Logic address: 147C hex = 5244	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI3 AI3 customer image (1mV, 0.001mA) • (AI3T == "0A") : 0.001 mA • (AI3T == "10U") : 0.001 V • (AI3T == "PTC") : 0.01 kOhm • (AI3T == "KTY") : 1 Ohm • (AI3T == "1PT3") : 1 Ohm • (AI3T == "1PT2") : 0.1 Ohm • (AI3T == "LEVEL") : 0.01 kOhm • else : 0.001 V		
[AI3 Std Value] AI3R	Logic address: 1472 hex = 5234	Type: INT (Signed16) Read/write: R Unit: -
Analog input 3 standardized value AI3 real application image		
[AI4] AI4C	Logic address: 147D hex = 5245	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI4 AI4 customer image (1mV, 0.001mA) • (AI3T == "0A") : 0.001 mA • (AI3T == "10U") : 0.001 V • (AI3T == "PTC") : 0.01 kOhm • (AI3T == "KTY") : 1 Ohm • (AI3T == "1PT3") : 1 Ohm • (AI3T == "1PT2") : 0.1 Ohm • (AI3T == "LEVEL") : 0.01 kOhm • else : 0.001 V		
[AI4 Std Value] AI4R	Logic address: 1473 hex = 5235	Type: INT (Signed16) Read/write: R Unit: -
Analog input 4 standardized value AI4 real application image		

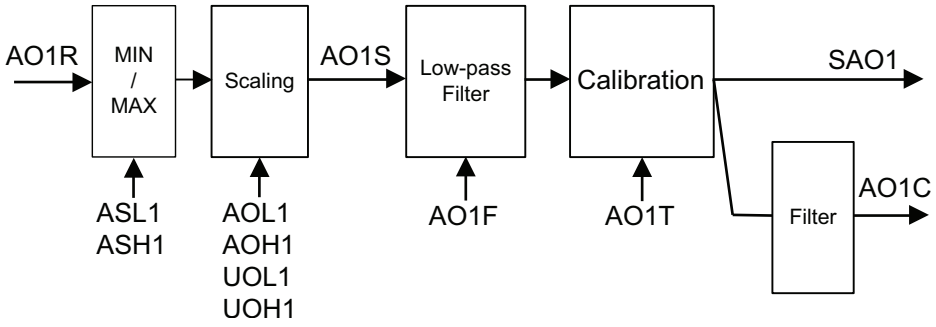
Analog outputs

The analog outputs can be controlled via the network. Simply write these parameters. The outputs to be controlled must not be assigned to a function, otherwise the write operation has no effect.

NOTE: To write an output through communication, no function should be assigned to the corresponding output. Otherwise, writing on the register linked to the corresponding output has no impact. If an error is triggered, outputs written through communication returns to 0.

NOTE: It is only possible to write the output through the active command channel. Consequently, forced outputs can not be disabled on local channel (such as display terminal).

The following diagram explains how the analog output works:



- AO1R **[AO1 Std Value]**
- ASL1 **[Scaling AQ1 Min]**
- ASH1 **[Scaling AQ1 Max]**
- AOL1 **[AQ1 min output]**
- AOH1 **[AQ1 max output]**
- UOL1 **[AQ1 min Output]**
- UOH1 **[AQ1 max Output]**
- AO1S **[AQ1 Scaling]**
- AO1F **[AQ1 Filter]**
- AO1T **[AQ1 Type]** : is too select between mA and V.
- SAO1 **[AO1 Phy Val w/o Filter]**
- AO1C **[AQ1]**

Code	Settings	
[AO1 Std Value] AO1R	Logic address: 148D hex = 5261	Type: INT (Signed16) Read/write: R/W Unit: -
Analog output 1 standardized value This parameter is used to read and write a value on AO1. Real image of AO1 consumed by functions.		
[AQ1] AO1C	Logic address: 1497 hex = 5271	Type: INT (Signed16) Read/write: R/W Unit: -
AQ1 physical value This parameter is used to read and write a value, readable on display terminal.		
[AO1 Phy Val w/o Filter] SAO1	Logic address: 14AF hex = 5295	Type: INT (Signed16) Read/write: R Unit: -
AO1 physical value without filter This parameter is used to read a value on **[AQ1]** without filter for communication devices.		

Code	Settings	
[AQ2] AO2C	Logic address: 1498 hex = 5272	Type: INT (Signed16) Read/write: R/W Unit: -
AQ2 physical value AQ2 customer image (1mV, 0.001mA)		
[AO2 Std Value] AO2R	Logic address: 148E hex = 5262	Type: INT (Signed16) Read/write: R/W Unit: -
Analog output 2 standardized value AQ2 real application image		

Communication Scanner

Local Configuration of the Communication Scanner

The communication scanner is useful when used in combination by the BACnet controller device with the function `Read/Write Multiple registers`: 23 (17 hex), which provides in a single telegram a read multiple registers and a write multiple registers. The detail of the function 23 is described in the supported BACnet functions.

The communication scanner **[Com. scanner input]** and **[Com. scanner output]** are accessible via the following menus: **[Communication]** `COM`– → **[Comm parameters]** `CMP` → **[Bacnet MS/TP]** `EBM`- and **[BACnet IP Config]** `BAIP`-.

An NCAx or NMAx parameter with a value of zero is not linked to a parameter in the drive.

The following table displays the list of Communication Scanners configuration parameters:

Sub Menu	Parameter description	Default assignment	Modbus address xxxxx (dec.) xxxx hex
[Com. scanner input] `ICS`	**[Scan. IN1 address]** `NMA1` Source address of the 1st input word	Status (ETA)	12701 319D hex
	[Scan. IN2 address] `NMA2` Source address of the 2nd input word	Output speed (RFRD)	12702 319E hex
	[Scan. IN3 address] `NMA3` Source address of the 3rd input word	0	12703 319F hex
	[Scan. IN4 address] `NMA4` Source address of the 4th input word	0	12704 31A0 hex
	[Scan. IN5 address] `NMA5` Source address of the 5th input word	0	12705 31A1 hex
	[Scan. IN6 address] `NMA6` Source address of the 6th input word	0	12706 31A2 hex
	[Scan. IN7 address] `NMA7` Source address of the 7th input word	0	12707 31A3 hex
	[Scan. IN8 address] `NMA8` Source address of the 8th input word	0	12708 31A4 hex

Sub Menu	Parameter description	Default assignment	Modbus address xxxxx (dec.) xxxx hex
[Com. scanner output] OCS	**[Scan.Out1 address]** NCA1 Destination address of the 1st output word	Command (CMD)	12721 31B1 hex
	[Scan.Out2 address] NCA2 Destination address of the 2nd output word	Speed target (LFRD)	12722 31B2 hex
	[Scan.Out3 address] NCA3 Destination address of the 3rd output word	0	12723 31B3 hex
	[Scan.Out4 address] NCA4 Destination address of the 4th output word	0	12724 31B4 hex
	[Scan.Out5 address] NCA5 Destination address of the 5th output word	0	12725 31B5 hex
	[Scan.Out6 address] NCA6 Destination address of the 6th output word	0	12726 31B6 hex
	[Scan.Out7 address] NCA7 Destination address of the 7th output word	0	12727 31B7 hex
	[Scan.Out8 address] NCA8 Destination address of the 8th output word	0	12728 31B8 hex

Fast Task of the Communication Scanner

Only the following parameters are available for the fast tasks:

Fast read	Parameters
nMA1...nMA4	ETA, RFR, FRH, LCR, OTR, ETI, ULN, UOP, THD, OPR, THR1, THR2, THR3, IL1I, IL1R, OL1R, AI1C, AI2C, AI3C, AO1R, AO1C, RFRD, FRHD, LRS1, LRS2, LRS3, LRS4, LRS5, LRS6, LRS7, LRS8, M001, M002, M003, M004, M005, M006, M007, M008

Fast write	Parameters
nCA1...nCA4	OLR1, AO1R, AO1C, CMD, LFR, PISP, LFRD, M001, M002, M003, M004, M005, M006, M007, M008

Monitoring the Communication Scanner

It is also possible to monitor the value of the parameters which has been configured in the communication scanner. This monitored values (**[Com. scan input map]** and **[Com scan output map]**) are accessible via the following menus: **[Communication]** ➡ **[Communication map]** ➡ **[BACnet MS/TP diag]** BND.

The 8 output variable values and the 8 input variable values are located into parameters **[Com Scan Out1 val.]** nC01 to **[Com Scan Out8 val.]** nC08 and **[Com Scan In1 val.]** nM01 to **[Com Scan In8 val.]** nM08.

The following table displays the list of Communication Scanner monitoring parameters:

Sub Menu	Parameter description	Default assignment	Modbus address xxxxx (dec.) xxxx hex
[Com. scan input map] ISA	**[Com Scan In1 val.]** NM1 Source value of the 1st input word	ETA value	12741 31C5 hex
	[Com Scan In2 val.] NM2 Source value of the 2nd input word	RFRD value	12742 31C6 hex
	[Com Scan In3 val.] NM3 Source value of the 3rd input word	0	12743 31C7 hex
	[Com Scan In4 val.] NM4 Source value of the 4th input word	0	12744 31C8 hex
	[Com Scan In5 val.] NM5 Source value of the 5th input word	0	12745 31C9 hex
	[Com Scan In6 val.] NM6 Source value of the 6th input word	0	12746 31CA hex
	[Com Scan In7 val.] NM7 Source value of the 7th input word	0	12747 31CB hex
	[Com Scan In8 val.] NM8 Source value of the 8th input word	0	12748 31CC hex
[Com scan output map] OSA	**[Com Scan Out1 val.]** NC1 Destination address of the 1st output word	CMD value	12761 31D9 hex
	[Com Scan Out2 val.] NC2 Destination address of the 2nd output word	LFRD value	12762 31DA hex
	[Com Scan Out3 val.] NC3 Destination address of the 3rd output word	0	12763 31DB hex
	[Com Scan Out4 val.] NC4 Destination address of the 4th output word	0	12764 31DC hex
	[Com Scan Out5 val.] NC5 Destination address of the 5th output word	0	12765 31DD hex
	[Com Scan Out6 val.] NC6 Destination address of the 6th output word	0	12766 31DE hex
	[Com Scan Out7 val.] NC7 Destination address of the 7th output word	0	12767 31DF hex
	[Com Scan Out8 val.] NC8 Destination address of the 8th output word	0	12768 31E0 hex

Monitoring of Communication Channel

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

- 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 control word (**[Cmd Register]** CMD) from the active command channel
- The control word containing the command switch (bit configured on **[Command Switching]** CCS)
- 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, **[MS/TP Com Interrupt]** `BELF` 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	Modbus Serial	Fieldbus Module	BACnet MSTP
Control word	CMD	CMD1	CMD3	CMD9
Extended control word	CMI	CMI1	CMI3	CMI9
Reference speed (rpm)	LFRD	LFRD1	LFRD3	LFRD9
Reference frequency (0.1 Hz)	LFR	LFR1	LFR3	LFR9
Reference value supplied by PI controller	PISP	PISP1	PISP3	PISP9
Reference value supplied by analog multiplier function	MFR	MFR1	MFR3	MFR9
(1): If available				

Software Setup with SpaceLogic™ AS-P Automation Server

What's in This Part

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 and refer to the following video to configure the SpaceLogic Automation server:

How to Configure SpaceLogic Ready-Server using Configuration Wizard

Command and communication configuration

Switch mode between Modbus and BACnet MS/TP for the Modbus VP12S port

The parameters are accessible in the **[Communication]** COM– → **[Emb Serial Line]** SPC- .

The parameter **[Embedded Protocol]** COM defines the Serial fieldbus switch mode.

The list presents the parameter settings:

- **[Bacnet MS/TP]** EBM
- **[Modbus]** MDB

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

Command Configuration

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

[Complete settings] CST → **[Cmd and Reference]** CRP

Then configure **[Ref Freq 1 Config]** FR1 parameter to:

- **[MS/TP Ref Freq]** EBM for BACnet MSTP
- **[Ref. Freq-Com. Module]** NET for BACnet IP.

Communication Configuration with BACnet MSTP Example

Select the BACnet MS/TP address in the menu:

[Communication] COM– → **[Comm parameters]** CMP → **[Bacnet MS/TP]** EBM

Then configure:

- **[MS/TP Address]** BADR 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]** BBDR to **[19200 bps]** 19200,
- **[MS/TP Max info frame]** BMIF to 10 maximum information trames,
- **[MS/TP Max Master Nb]** BMMN to 3.

  NOTE: It is recommended to set **[MS/TP Max Master Nb]** to **[MS/TP Address]** + 1.
- **[MS/TP Timeout]** BTLP to 4 s (in our example).

  NOTE: set other parameters linked to **[Bacnet MS/TP]** EBM according to your application.

Communication Configuration with BACnet IP Example

Select the BACnet IP address in the menu:

[Communication] COM– → **[Comm parameters]** CMP → **[BACnet IP Config]** BAIP

Then configure **[IP address]** and **[Mask]**.

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

- **[BACnet IP Inst Nb]** BAXP to 1,
- **[IP mode]** IPM to **[DHCP]** dHCP,
- **[Bacnet IP Time-Out]** BATT to 4 s.

  NOTE: set other parameters linked to **[BACnet IP Config]** BAIP according to your application.

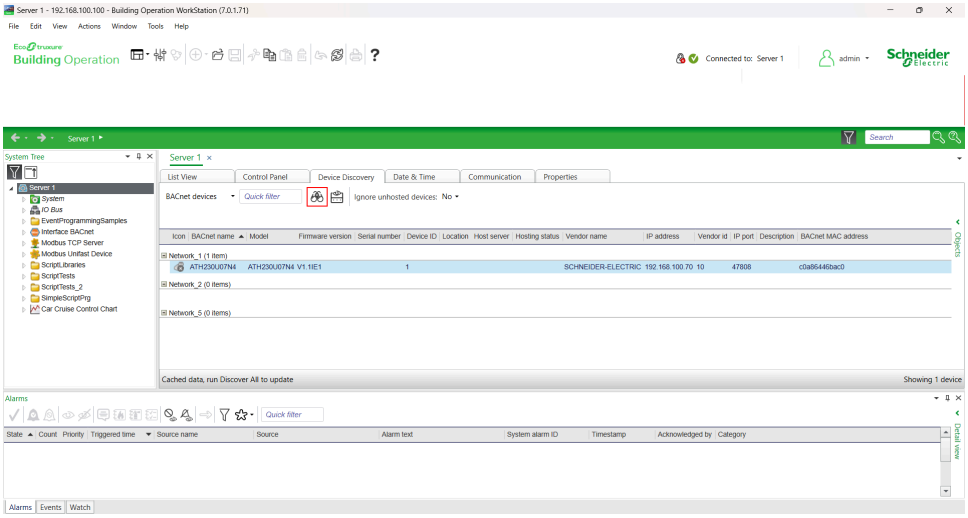
Connect the drive and the controller with EcoStruxure™ Building Operation

Example for ATH200

The following example refers to ATH200 drives, but also applies to ATH600 drives.

Discover and add the drive in a network

Click on  .

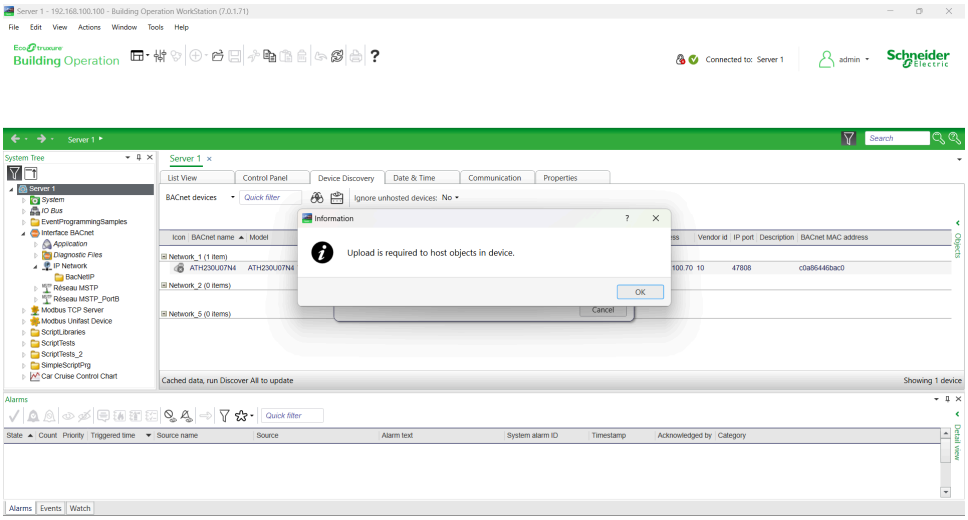


Click on the drive and drop it into the:

- BACnet MSTP network

OR

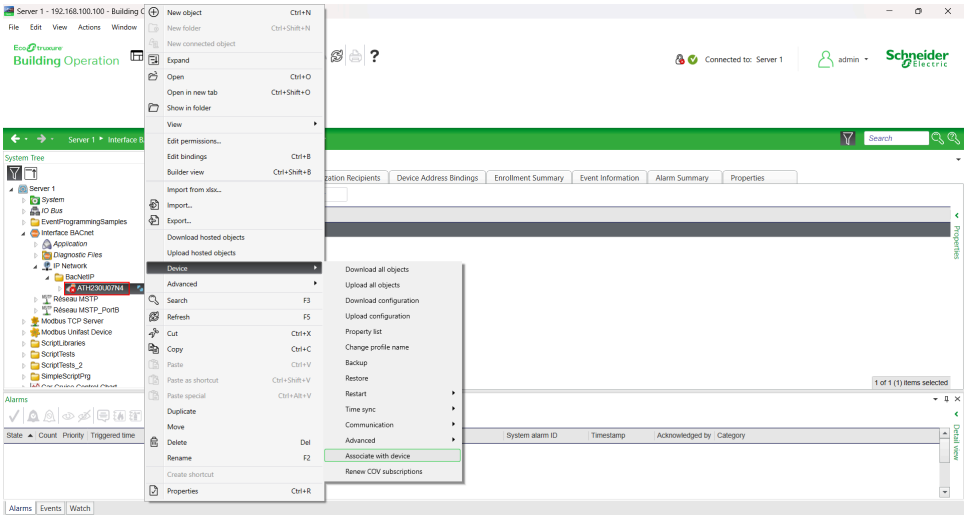
- BACnet IP network (if using the VW3A3726 module)



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

Associate with device

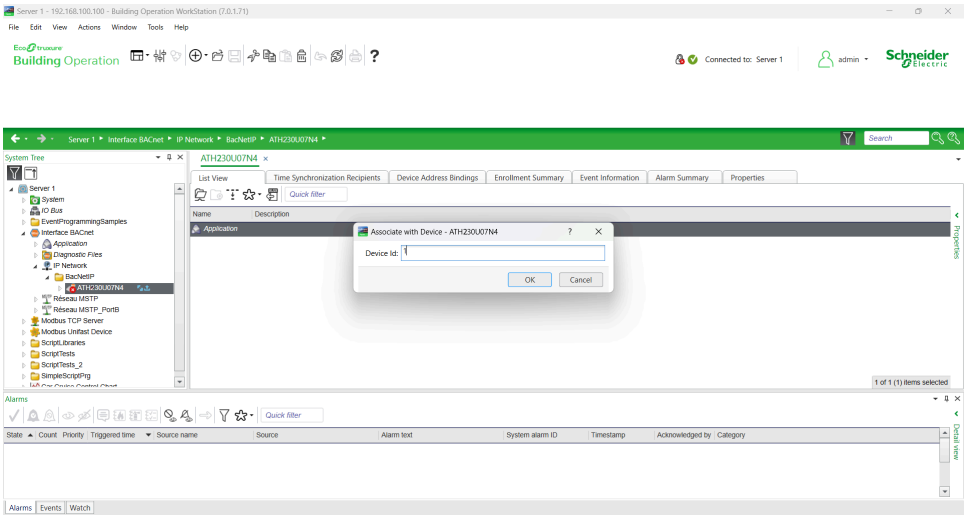
Right-Click on the drive → **Device** → **Associate with device**



Select the number of the device ID linked to the :

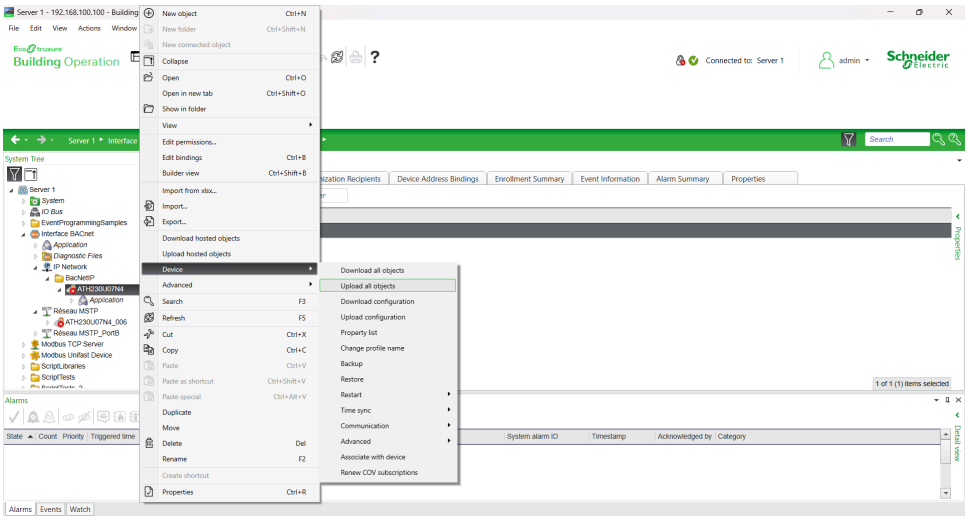
- **[MS/TP Inst Nb High]** bInH for the BACnet MSTP Network
- **[Bacnet Instance High]** bAoH for the BACnet IP network.

  NOTE: For ATH600 drives, this step can be ignored. The Device ID is already displayed.

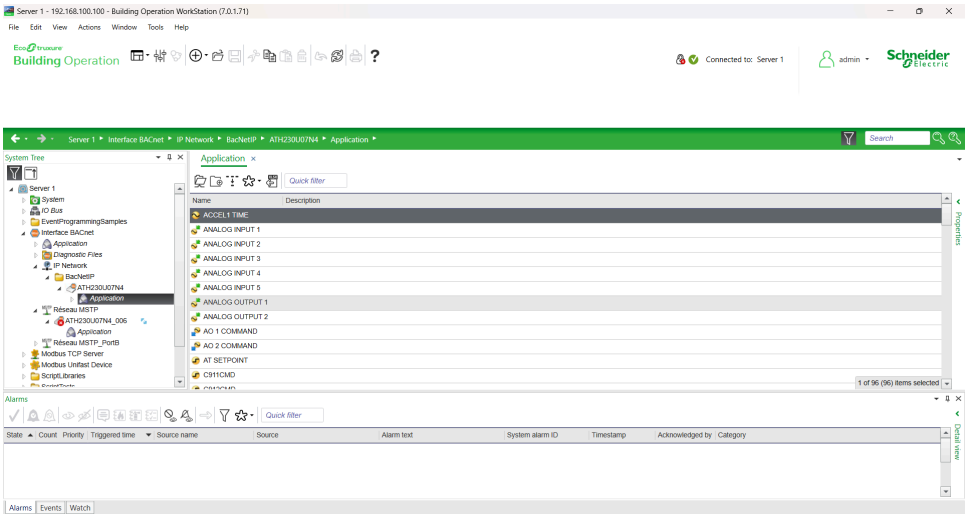


Upload of the BACnet Objects

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



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



Diagnostics and Troubleshooting

What's in This Part

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]** BTLP or **[Bacnet IP Time-Out]** BATT parameter

For BACnet IP, the parameter **[B IP Timeout Mode]** BATM defines the BACnet IP fieldbus timeout mode.

The values of the **[BACnet MSTP Err Resp]** BSLL (*logical address: 29215*) parameter for BACnet MS/TP and **[Fdbus Interrupt Resp]** CLL (*logical address: 7015*) parameter for BACnet IP, which :

Value	Meaning
triggers a drive detected error ([MS/TP Com Interrupt] BELF for BACnet MS/TP and [Fdbus Com Interrupt] CNF for BACnet IP) are:	
[Freewheel Stop] YES	Motor triggers in error and is stopped in freewheel. **Factory setting**
[Ramp stop] RMP	Motor is stopped in ramp and triggers in error at the end of stop.
[Fast stop] FST	Motor is stopped in fast stop and triggers in error at the end of stop.
[DC injection] DCI	Motor is stopped with DC injection and triggers in error at the end of stop.
does not trigger an error are:	
[Ignore] NO	Detected error ignored (in this case, the warning **[MS/TP Com Warn]** BLLA for BACnet MSTP or **[Fieldbus Com Warn]** CLLA for BACnet IP is activated).
[Configured Stop] STT	Motor is stopped according to **[Type of stop]** STT parameter.
[Fallback Speed] LFF	Reference frequency modified to fallback speed, maintained as long as the detected error persists and the run command has not been removed.
[Speed maintain] RLS	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 **[MS/TP Com Interrupt]** `BELF` 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 **[Fdbus Interrupt Resp]** `CLL` for BACnet IP and **[BACnet MSTP Err Resp]** `BSLL` for BACnet MSTP).

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 fieldbusses 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

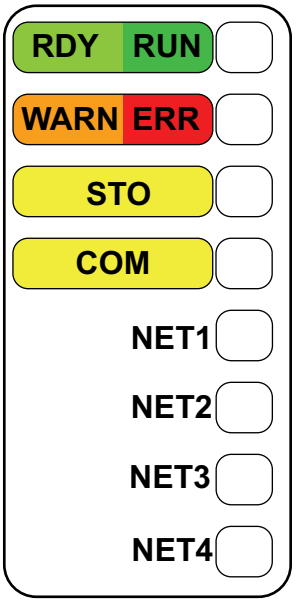
The **[Ref Freq Channel]** RFCC parameter indicates the active channel for reference frequency.

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.

Fieldbus Status LEDs

LED Description — BACnet MSTP



Following table describe the LED **COM** behavior during transmitted and received frames:

Color & Status	Description
OFF	No link
Green flickering	Frames are being transmitted or received

LED Description — BACnet IP

Item	LED	Description
1	BF	Module status
2	SF	Network status
3	LNK1	Port A activity
4	LNK2	Port B activity

Module Status

Color & status	Description
OFF	The device is powered off
Red ON	The device has detected an ILF error
Green ON	The device is ready and operational
Red flickering	The device has detected a communication interruption.
Green/Red flickering	Power up testing
Red single flash	No connection to the BACNET manager

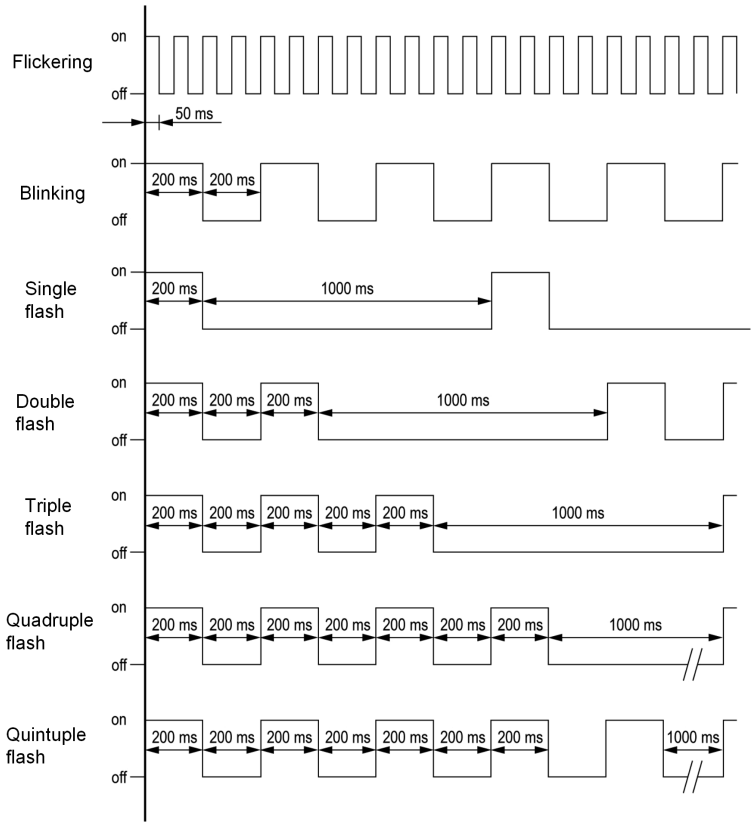
Network error status

Color & status	Description
OFF	The device does not have an IP address or is powered off
Red ON	Error detected on the module
Green ON	At least a port is connected and has a valid IP address.
Red flickering	The device has detected a communication interruption.
Green/Red flickering	Power up testing
Green flashing 3 times	All ports are unplugged, but the module has an IP address
Green flashing 4 times	Error detected: duplicate IP address
Green flashing 5 times	The module is performing a DHCP sequence

Link leds port status

Color & status	Description
OFF	No link
Green ON	Link established at 100 Mbit/s
Green blinking	Network activity at 100 Mbit/s
Yellow ON	Link established at 10 Mbit/s
Yellow blinking	Network activity at 10 Mbit/s

LED Behavior



Warning Codes

List of Available Warnings Messages

Setting	Code	Description
[No Warn stored]	NOA	No warning stored
[Static Port/Serv Warn]	PSSA	***Static port/service warning***
[Modbus Com Warn]	SLLA	***Modbus comm interruption warning***
[MS/TP Com Warn]	BLLA	***BACnet MS/TP comm interruption warning***
[Fieldbus Com Warn]	CLLA	***Fieldbus comm interruption warning***

Communication error codes

What's in This Chapter

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.

[MS/TP Com Interrupt] BELF

BACnet MS/TP Communication interrupt

Probable Cause	Communication interruption on the BACnet bus.
Remedy	• 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]** BTLP meets the requirements of your application. • Verify that the **[MS/TP Max Master Nb]** is set to **[MS/TP Address]** + 1.
Clearing the Error Code	This detected error can be cleared with the **[Auto Fault Reset]** ATR or manually with the **[Fault Reset Assign]** RSF parameter after its cause has been removed. This also possible to reset with the command word 0080 hex (*Fault reset*).

[Incorrect Config] CFF

Incorrect configuration

Probable Cause	At power on, the device proceeds to a self-test and checks its configuration. If the configuration is not correct, the error **[Incorrect Config]** CFF is triggered. • Option module changed or removed.
Remedy	• Verify that all option modules are inserted correctly into the option module slot. • Verify that there is no detected error on the option module. • 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 Config] CFI

Invalid configuration

 Probable Cause	Invalid configuration. The configuration loaded in the device via the commissioning tool or fieldbus is inconsistent. • Invalid parameter value. • BACnet IP option module is plugged and **[Control Mode]** CHCF is set to **[I/O profile]** IO.
 Remedy	• Verify the loaded configuration. • Load a valid configuration.
 Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Conf Transfer Error] CFI2

Configuration transfer error

 Probable Cause	• The configuration transfer to the device was not successful or interrupted. • The configuration loaded is not compatible with the device.
 Remedy	• Verify the configuration loaded previously. • Load a compatible configuration. • Use PC software commissioning tool to transfer a compatible configuration. • Perform a factory setting.
 Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Fdbus Com Interrupt] CNF

Fieldbus communication interruption

 Probable Cause	Communication interruption on fieldbus module. This error is triggered when the communication between the fieldbus module and the manager (PLC) is interrupted.
 Remedy	• 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 timeout setting. • Check the parameters **[MS/TP APDU Retries]** APDR and **[MS/TP APDU Timeout]** APDT for BACnet MS/TP and **[IP APDU Retries]** APRI and **[IP APDU Timeout]** APTI for BACnet IP according to the application. • In case of timeout, check the parameter **[B IP Timeout Mode]** BATM by setting it to **[BACnet All Traffic]** MBT. • Replace the option module. • Verify that the value set on **[Bacnet IP Time-Out]** BATT meets the requirements of your application. • Contact your local Schneider Electric representative.
 Clearing the Error Code	This detected error can be cleared with the **[Auto Fault Reset]** ATR or manually with the **[Fault Reset Assign]** RSF parameter after its cause has been removed. This also possible to reset with the command word 0080 hex (*Fault reset*).

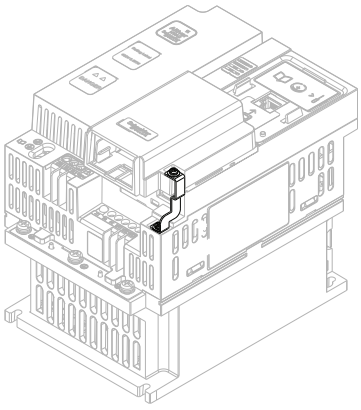
[Channel Switch Error] CSF

Channel switching detected error

Probable Cause	An invalid channel has been selected. This error may be triggered if the device has been switched to a configuration which implies an invalid channel.
Remedy	Verify the function parameters.
Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Internal Link Error] ILF

Internal communication interruption with option module

Probable Cause	Communication interruption between option module and the device.
Remedy	• Verify the environment (electromagnetic compatibility). **NOTE:** In case of unintended **[Internal Link Error]** ILF error triggering caused by EMC disturbance, when using BACnet IP VW3A3726 module and module adapter VW3A36001, replace the grounding plate used for the ground connection between the module adapter and the ground with a cable of 2.5 mm² (AWG 14) and with a cable length of 10 cm (3.94 in).  • 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	• 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 (if existing) is not recognized. • The device firmware is not compatible with the option module. • Option module corrupted due to multiple firmware updates.
Remedy	• 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.

Annex

What's in This Part

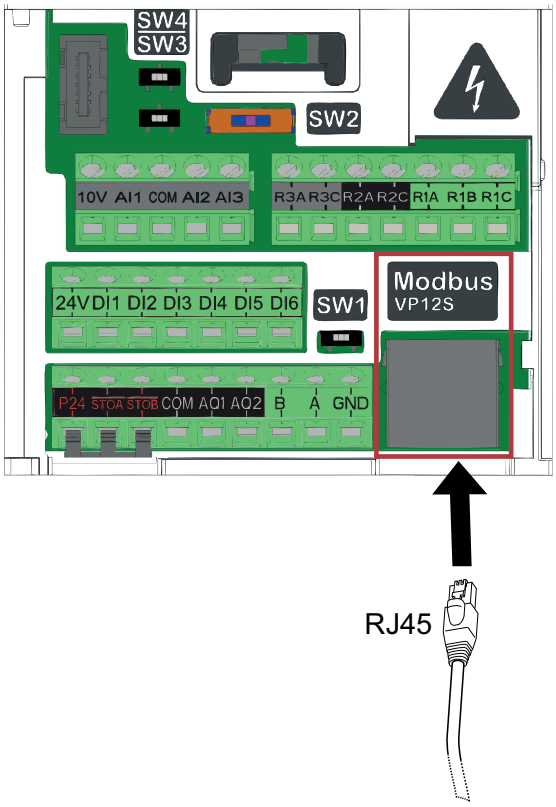
Firmware Update

BACnet MS/TP

The firmware update of BACnet MS/TP is done during the firmware update of the drive.

BACnet IP – VW3A3726

The firmware update of the VW3A3726 can be updated directly via Ecostruxure Automation Device Maintenance (EADM) or SoMove. Connect the device to the PC. Use the following serial communication cable: VW3A8127 for Modbus VP12S connection.



NOTE: If **[Embedded Protocol]** COM was previously set to **[Bacnet MS/TP]** EBM, make sure to set it to **[Modbus]** MDB, then restart the product so the change can take effect.

Download Altivar HVAC firmwares.

For additional support, contact our Customer Care Center on:

www.se.com/CCC.

Operation

What's in This Chapter

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]** SEP
- *Not separate* **[Not separ.]** SnM,

Functional Description

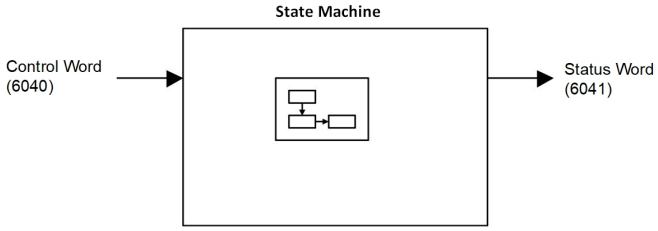
Introduction

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

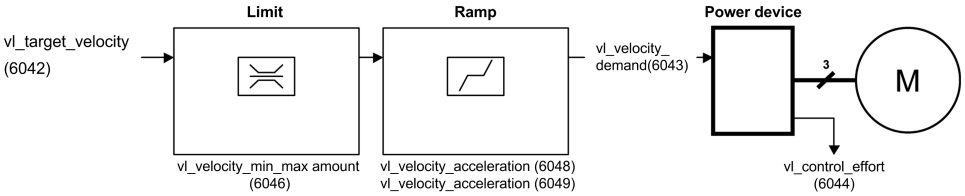
CiA402

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:



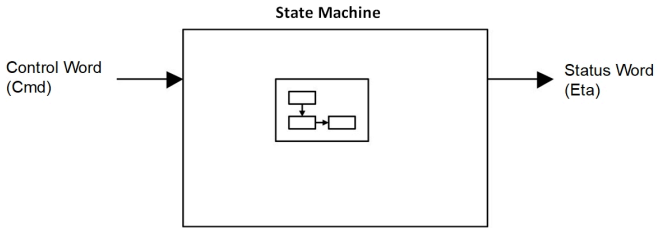
Simplified diagram for speed control in *Velocity* mode:



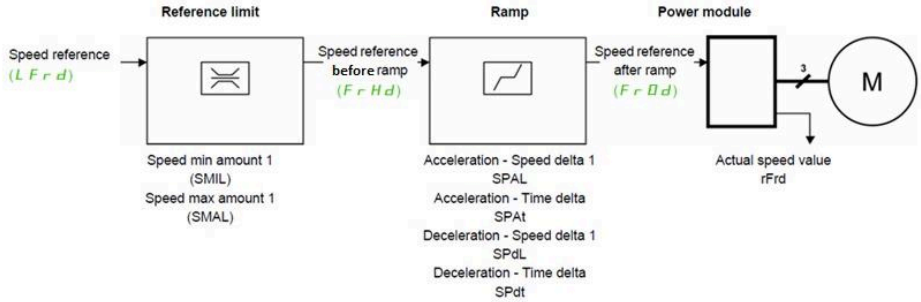
Altivar HVAC Drive

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:

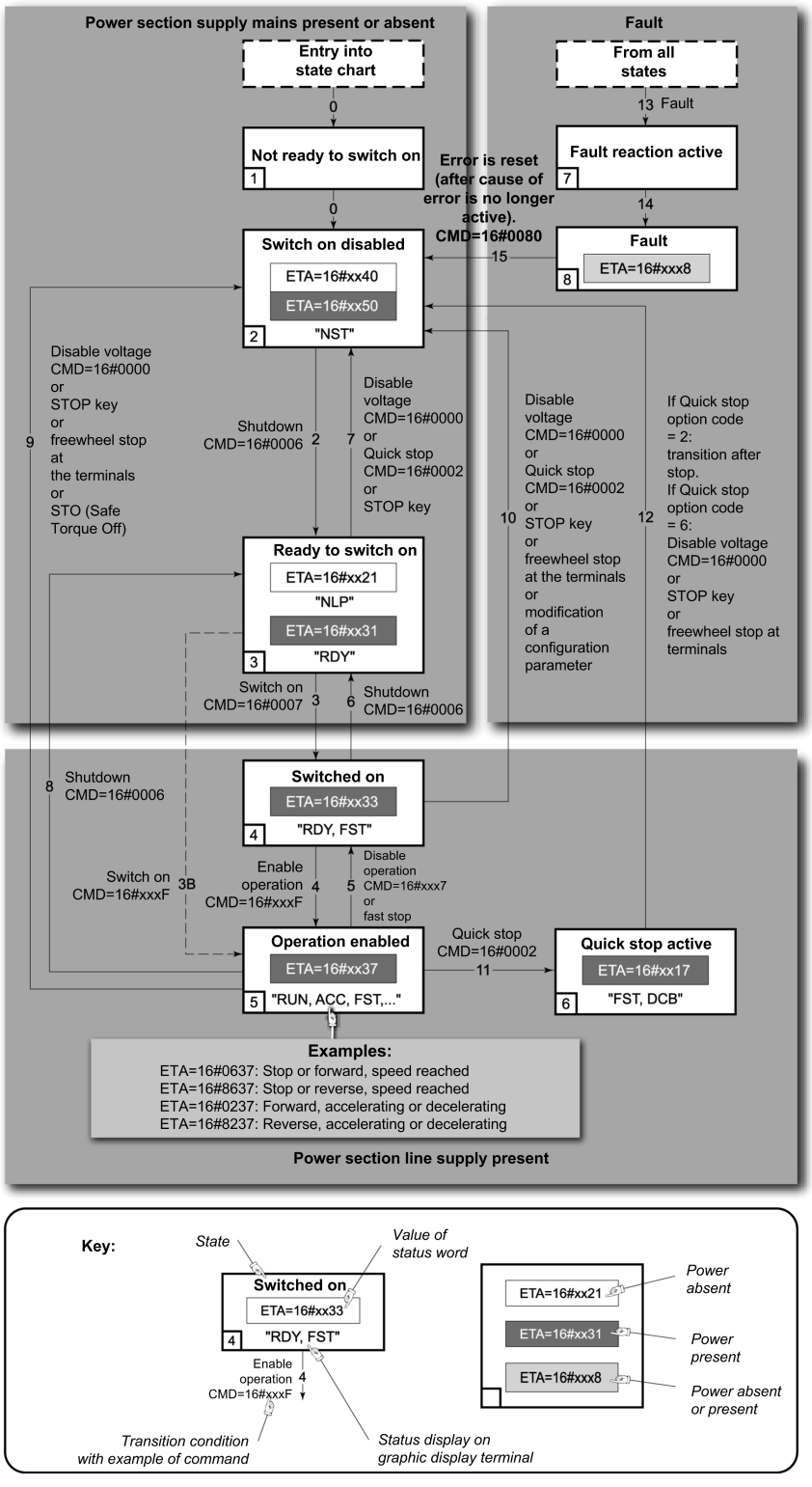


CIA402 Operating State Diagram

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	• Initialization starts. This is a transient state invisible to the communication network.
2 - Switch on disabled	• 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	• 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 - Switched on*. • 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	• 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 - Switch on disable* .
5 - Operation enabled	• 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 Halt 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 - Operation enabled*. • The adjustment parameters can be modified. • The configuration parameters cannot be modified. **NOTE:** The command *4 - Enable operation* 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. • The reaction of the drive to a Disable operation command depends on the value of the **[SwitchOnDisable Stp]** DOTD parameter: ◦ If the **[SwitchOnDisable Stp]** DOTD parameter is set to 0, the drive changes to operating state *4 - Switched on* 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 - Switched on*.

Operating State	Description
6 - Quick stop active	• 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: ◦ 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	• Transient state during which the drive performs an action corresponding to the selected error response.
8 - Fault	• 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 CMD

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	Enable voltage	Switch on
0 to 1 transition = Error is reset (after cause of error is no longer active)				1 = Run command	0 = Quick stop active	Authorization to supply AC power	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 = Forward direction asked 1= Reverse direction asked			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	
Shutdown	2, 6, 8	*3 - Ready to switch on*	X	X	1	1	0	0006 hex
Switch on	3	*4 - Switched on*	X	X	1	1	1	0007 hex
Enable operation	4	*5 - Operation enabled*	X	1	1	1	1	000F hex
Disable operation	5	*4 - Switched on*	X	0	1	1	1	0007 hex
Disable voltage	7, 9, 10, 12	*2 - Switch on disabled*	X	X	X	0	X	0000 hex
Quick stop	11	*6 - Quick stop active*	X	X	0	1	X	0002 hex
	7, 10	*2 - Switch on disabled*						
Fault reset	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 MSTP	BACnet IP
Bit 11	C911	C311
Bit 12	C912	C312
Bit 13	C913	C313
Bit 14	C914	C314
Bit 15	C915	C315

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

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

[CIA402 State Reg] ETA

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	002F hex
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.
- Verify that Bit1 and Bit4 of the parameter **EEPROM Status** EEPS (logical address **5E2 hex = 1506**) are set to 0 to confirm that the configuration storage process is completed.

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.

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

Code	Settings	
[Extended Ctrl Word] CMI	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	***Restore factory setting***	***Store current configuration***	***Restore current configuration***	***External error***	***Reserved***			
Bit at 0	Active on rising edge when motor is stopped. Once request is considered, this bit is automatically reset.	Active on rising edge. Once request is considered, this bit is automatically reset.	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								

	Bit 8	Bit 9	Bit 10	Bit 11	Bit 12	Bit 13	Bit 14	Bit 15
Function	***Reserved***	***Frequency reference (FRH, LFR, RFR ...)***	***Fast stop requested***	***DC injection requested***	***Reverse direction requested***	***Device locked in STOP***	***Reserved***	***Parameter coherence deactivated and drive locked in STOP***
Bit at 0		in 0.1Hz	Deactivate.	Deactivate.	Deactivate.	Deactivate.		Deactivate. All parameters are validated.
Bit at 1		in internal unity (32767 = TFR)	Activate.	Activate.	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	***Write parameter authorization***	***Parameter consistency checked***	***Device reset authorization***	***Reserved***
Bit at 0	Authorized	Not active.	Not active.	
Bit at 1	Not authorized	Active.	Active.	

	Bit 4	Bit 5	Bit 6	Bit 7
Function	***Run order present***	***DC injection running***	***Drive in transitional state***	***Motor thermal threshold reached***:
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	***Braking transistor activated***	***Product in acceleration***	***Product in deceleration***	***Current limitation or torque limitation is running***
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	***Fast stop in progress***	***Active mode***:		***Reverse direction applied to the ramp***
Bit at 0	Not active.	• 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.

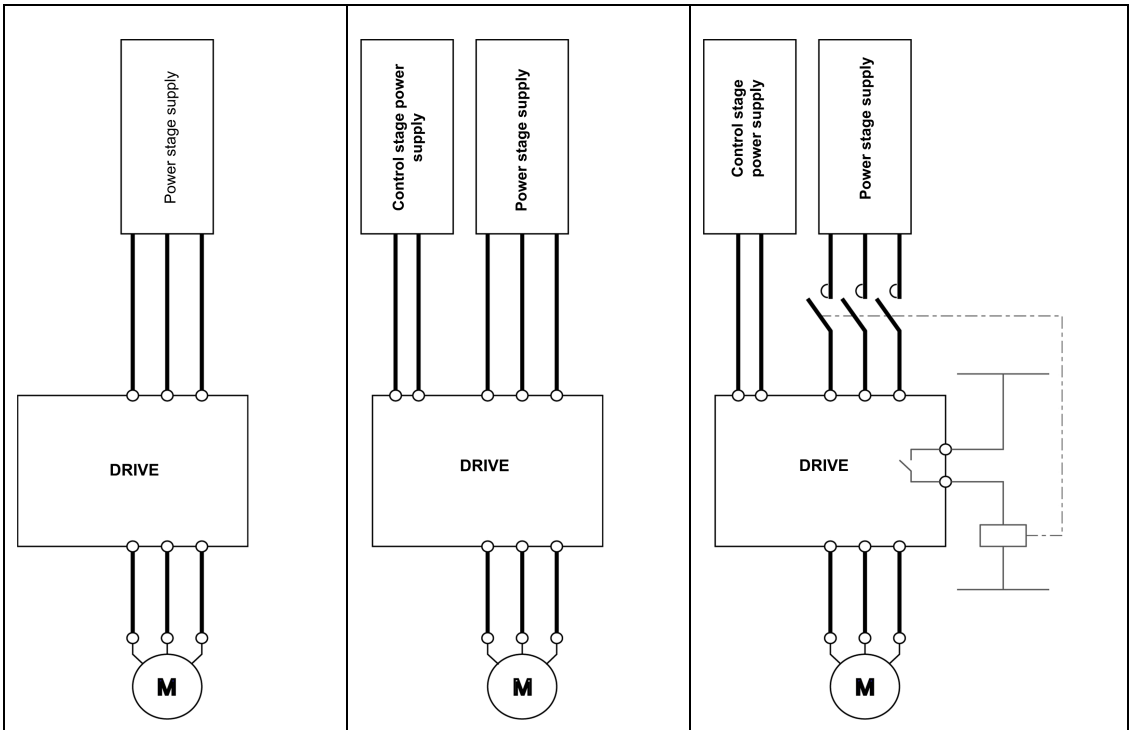
Starting Sequence

What's in This Chapter

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

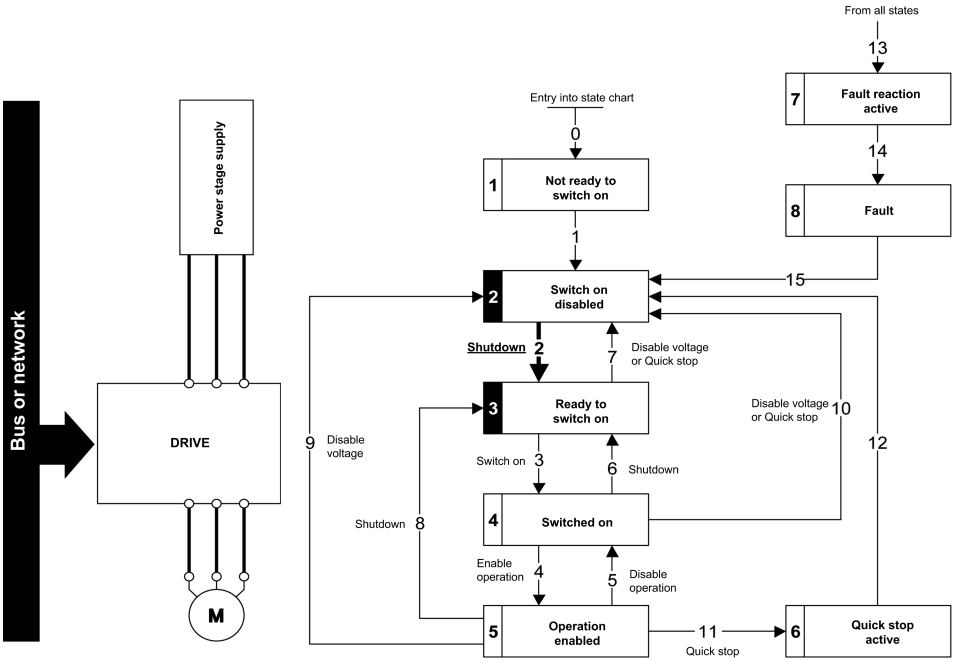
Both the power and control stages are powered by the power stage supply.

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:

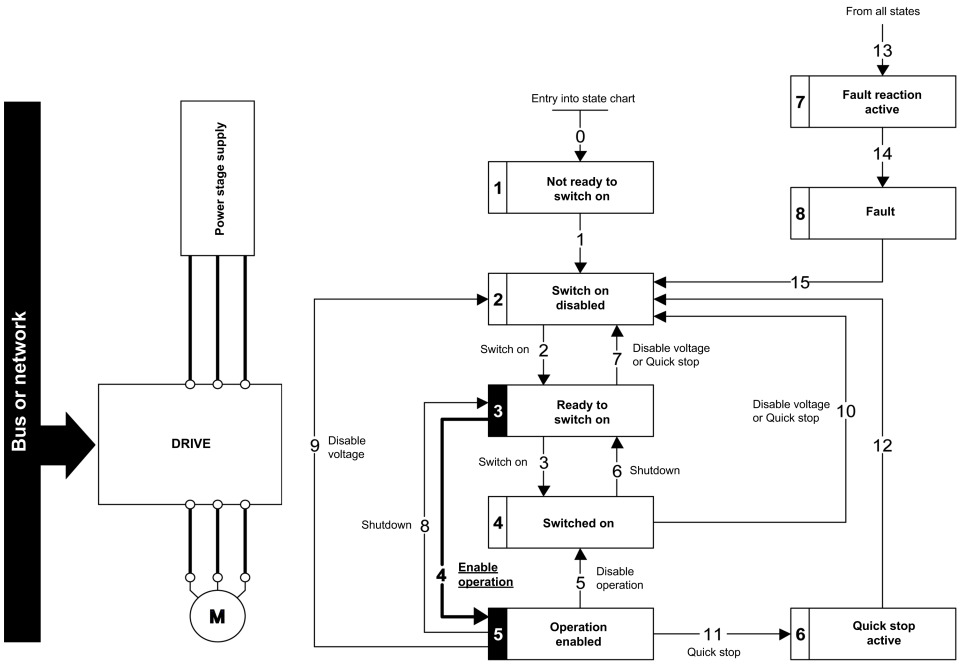
Step 1

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

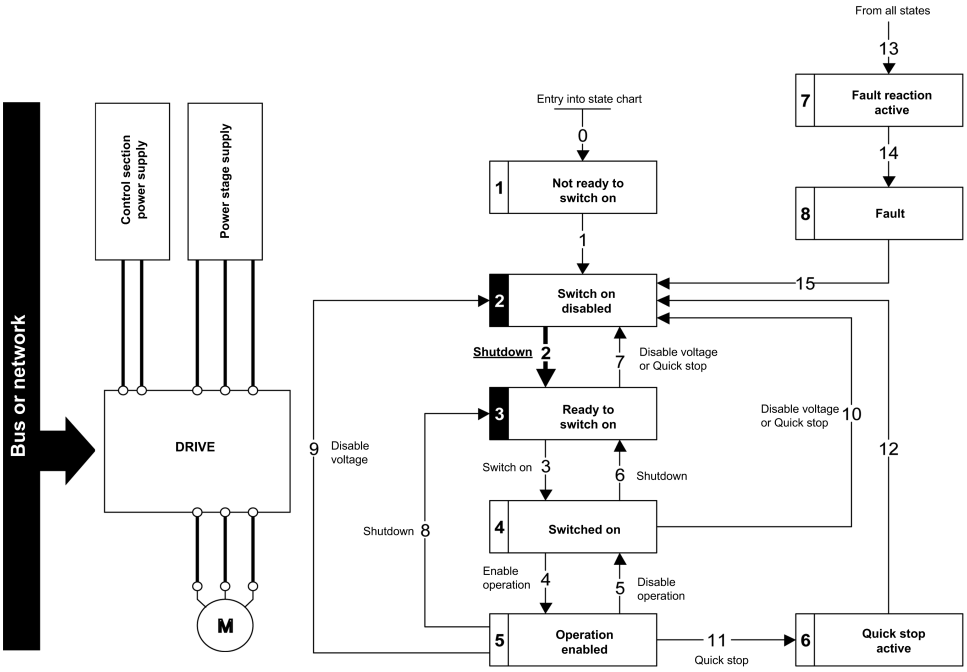
Power is supplied separately to the power and control stages.

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

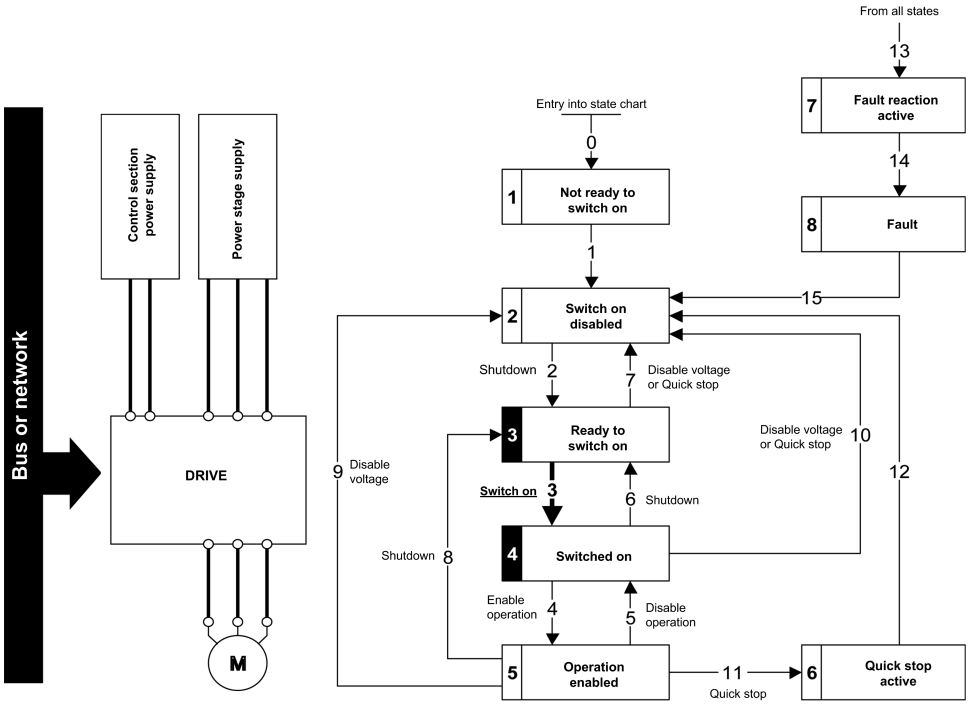


Step 2

- 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).

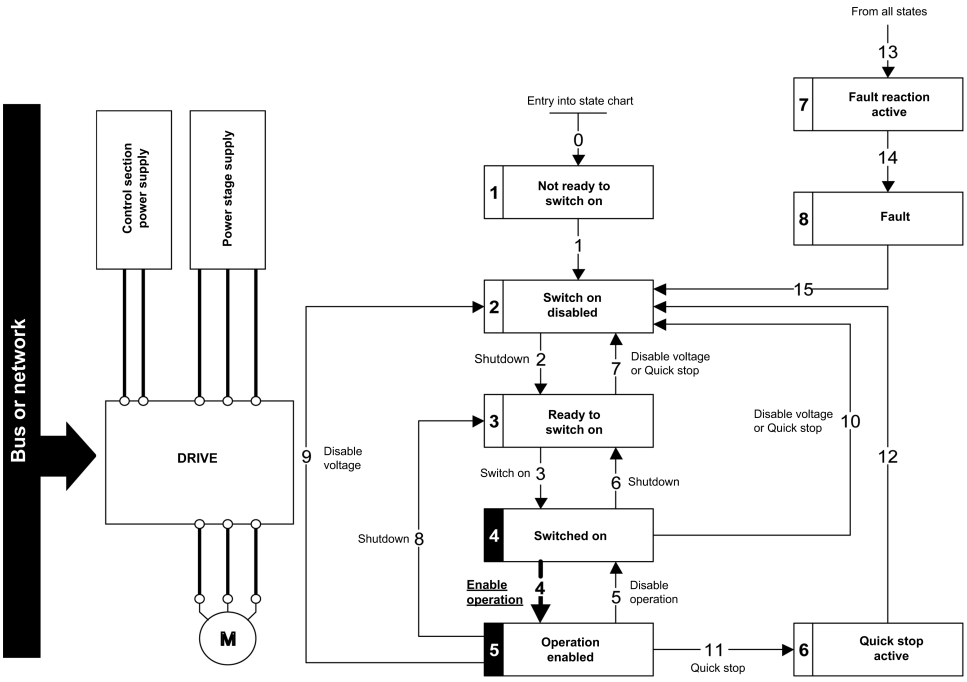
Power Stage Supply	HMI Panel	Status Word
Not present	**[No Mains Voltage]** NLP	21 hex
Present	**[Ready]** RDY	31 hex

- 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

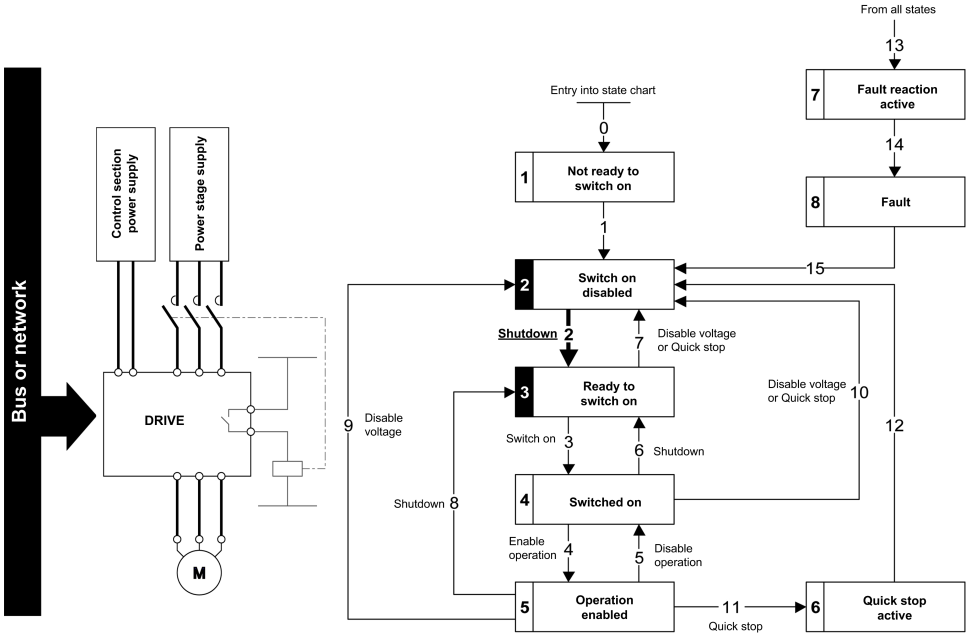
Power is supplied separately to the power and control stages.

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:

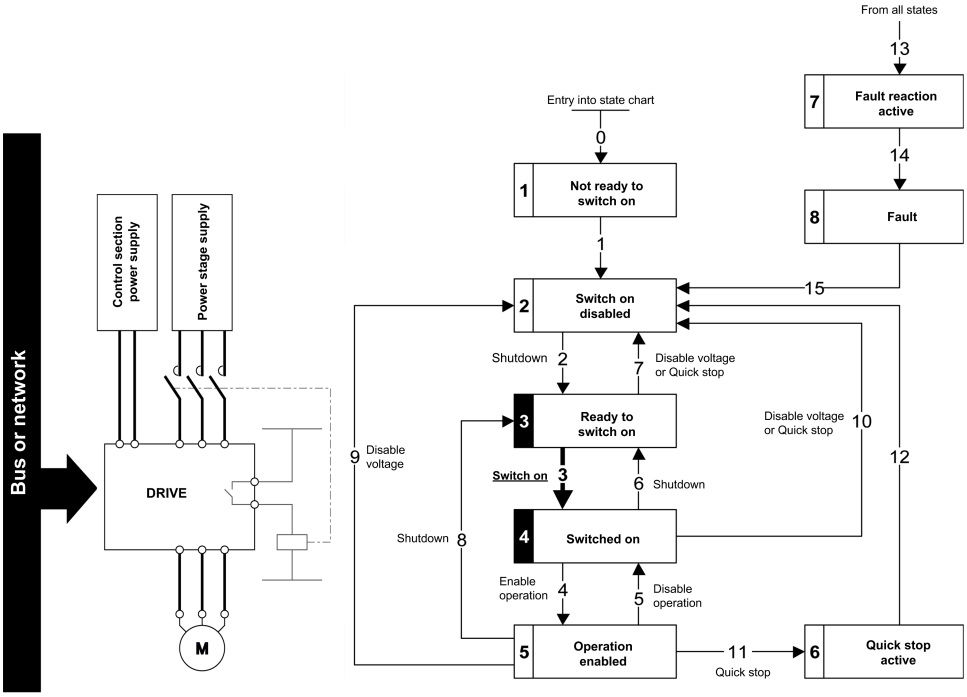
Step 1

- 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

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 **[Complete settings]** CST- menu ➡ **[Cmd and Reference]** CRP- submenu :

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

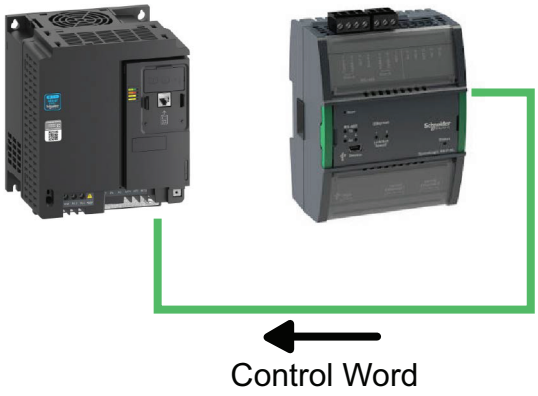
For the current example, **[Control Mode]** CHCF is adjusted to **[Not separ.]** SIM as reference and control are originated from the communication network.

Profile	Ref1 Channel setting
CiA 402 combined mode	**[Not separ.]** SIM
CiA 402 separate mode	**[Separate]** SEP

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 frequence reference value is adjusted on the display terminal. 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	**[HMI]** LCC
[Reverse Disable] RIN	Default
[Stop Key Enable] PST	Default
[Control Mode] CHCF	**[Separate]** SEP
[Command Switching] CCS	Default
[Cmd channel 1] CD1	**[BACnet MS/TP]** EBM

BACnet Basics

What's in This Chapter

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
  - CMD111CMD
  - CMD112CMD
  - CMD113CMD
  - CMD114CMD
  - CMD115CMD
- 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)
- 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 Profile

The BACnet device profile supported is:

- BACnet Application Specific Controller (B-ASC).

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
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		
0x00C00003	RO3 ACT	Indicates status of R3		
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		
0x00C0000C	DI 7 ACT	Value of LI7		
0x00C0000D	DI 8 ACT	Value of LI8		

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
0x01000002	RO 3 CMD	R3 relay out	NO	C if R3 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
0x00000011	Indicates status of AO2	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
0x00400001	AO2 COMMAND	Analog output value 2	NO	C - if AO2 value is NOR - otherwise

Binary value object

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 bit 2
0x01400001	FWD/REV ACT	Indicate the motor rotation direction	NO	NO	ETA bit 15
0x01400002	FAULT ACT	indicate if the drive error status	NO	NO	ETA bit 3
0x01400004	HAND/AUTO ACT	Indicates if the drive is locally controller or not	NO	NO	ETA bit 9
0x01400007	DRIVE READY	The VSD is ready and wait for start command	NO	NO	ETA bit 1
0x01400008	AT SETPOINT	The VSD has reached the target speed	NO	NO	ETA bit 10
0x0140000A	RUN/STOP CMD	Command a drive start	NO	NO	Internal command channel. See CiA402 • OFF = CMD bit 1&2 set • ON = CMD bit 0&1&2&3 set
0x0140000B	FWD/REV CMD	Command a motor direction change	RIN=NO	NO	CMD bit 11. See CiA402
0x0140000E	FAULT RESET	Reset error (rising edge)	NO	NO	ON = CMD 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	C911CMD (for Bacnet MS/TP) C311CMD (for Bacnet IP)	CMD word 3 bit 11	NO	NO	CMD bit 11
0x01400013	C912CMD (for Bacnet MS/TP) C312CMD (for Bacnet IP)	CMD word 3 bit 12	NO	NO	CMD bit 12
0x01400014	C913CMD (for Bacnet MS/TP) C313CMD (for Bacnet IP)	CMD word 3 bit 13	NO	NO	CMD bit 13
0x01400015	C914CMD (for Bacnet MS/TP) C314CMD (for Bacnet IP)	CMD word 3 bit 14	NO	NO	CMD bit 14
0x01400016	C915CMD (for Bacnet MS/TP) C315CMD (for Bacnet IP)	CMD word 3 bit 15	NO	NO	CMD 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
0x00800002	DC BUS VOLT	DC bus voltage	ASN.1 - 5 - V	R		10V	VBUS
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
0x00800008	KWH(r)	Energy counter (erasable)	ASN.1 - 19 - kWh	R		1kWh	Based on values given by the following parameters: IC0 to IC4
0x00800009	KWH(NR)	Energy counter (not resettable)	ASN.1 - 19 - kWh	R		1kWh	Based on values given by the following parameters: IC0 to IC4
0x0080000A	PRC PID FBCK	PID regulartor feedback	ASN.1 - 98 - %	R		3%	RPF
0x0080000B	PRC PID DEV	PID regulartor 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	ASN.1 - 95 - NULL	C	0	NA	NC1 (drive forward the

Object_ Identifier	Object_Name (default)	Description (no link with property)	Units	Present Value access	Relinquish default	COV_ Increment	TV Drive param
		==> Comm scan					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 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

Object_ Identifier	Object_Name (default)	Description (no link with property)	Units	Present Value access	Relinquish default	COV_ Increment	TV Drive param
							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
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

The following table is provided as an example:

BACnet Property	Value
Object Identifier	OBJECT_DEVICE:1
Object Name	ATH630U07N4Z_17
Object Type	8 : Object Device
System Status	0 : Operational
Vendor Name	SCHNEIDER-ELECTRIC
Vendor Identifier	10
Model Name	ATH630U07N4Z
Firmware Revision	V1.11E1
Application Software Version	V0.71E1
Protocol Version	1
Protocol Revision	22
Protocol Services Supported	000001100000111110100000000000011100000-001000000100
Protocol Object Types Supported	111111101010011110011101110001111101011-0000101000
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.

The following table is provided as an example:

BACnet Property	Value
Property List	Object[] Array
System Status	0 : Operational
Vendor Name	Schneider Electric
Vendor Identifier	10
Model Name	ATH630U07N4Z
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	000001000000101111001000001000000011000-000000
Protocol Object Types Supported	111111001000000000000000000000000000000-000000000000000000001000000
Object List	Object [] Array
Max Master	1
Max Info Frames	10
Device Address Binding	
Database Revision	0
Active Cov Subscriptions	
Object Name	ATH630U07N4Z_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	47808
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	1
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

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**.

DI: Digital Input

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
1884 Boulevard de la Défense
92000 Nanterre
France

www.se.com

JPS89285.01