Altivar HVAC ATH200

Variable Speed Drives for Synchronous and Asynchronous Motors

Modbus Serial Link Manual

JPS43217.01
02/2026

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 ATEX zone. Prior to using the product, you must perform a risk assessment in view of the planned application. Based on the results, the appropriate safety measures must be implemented. Since the product is used as a component in an entire system, you must ensure the safety of persons by means of the design of this entire system (for example, machine design). Any use other than the use explicitly permitted is prohibited and can result in hazards.

About the document

Document Scope

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

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

Validity Note

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

This documentation is valid for the Altivar HVAC ATH200 drives.

Product Related Information

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

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

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

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

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

⚠⚠DANGER

ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION

Do not use damaged products or accessories.

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

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

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

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

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

⚠WARNING

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

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

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

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

⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

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

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

⚠WARNING

LOSS OF CONTROL

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

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

(1) For USA: Additional information, refer to NEMA ICS 1.1 (latest edition), Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control and to NEMA ICS 7.1 (latest edition), Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems.

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

⚠WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

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

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

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

⚠WARNING

LOSS OF CONTROL

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

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

General Cybersecurity Information

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

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

Schneider Electric provides additional information and assistance:

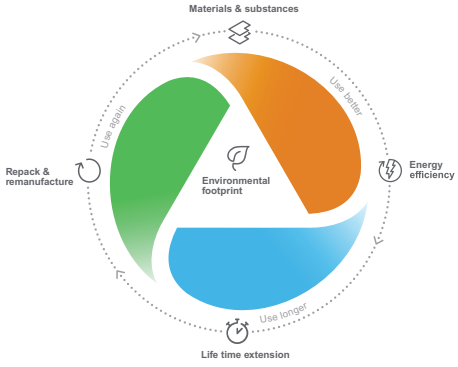
- Subscribe to the Schneider Electric security newsletter.
- Visit the Cybersecurity Support Portal web page to:
  - Find Security Notifications.
  - Report vulnerabilities and incidents.
- Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:
  - Access the cybersecurity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

Environmental Data

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

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

Five data categories across the product lifecycle



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

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

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

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

Information on Non-Inclusive or Insensitive Terminology

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

Terminology used in this document

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

Among others, these standards include:

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

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

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

Contact us

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

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

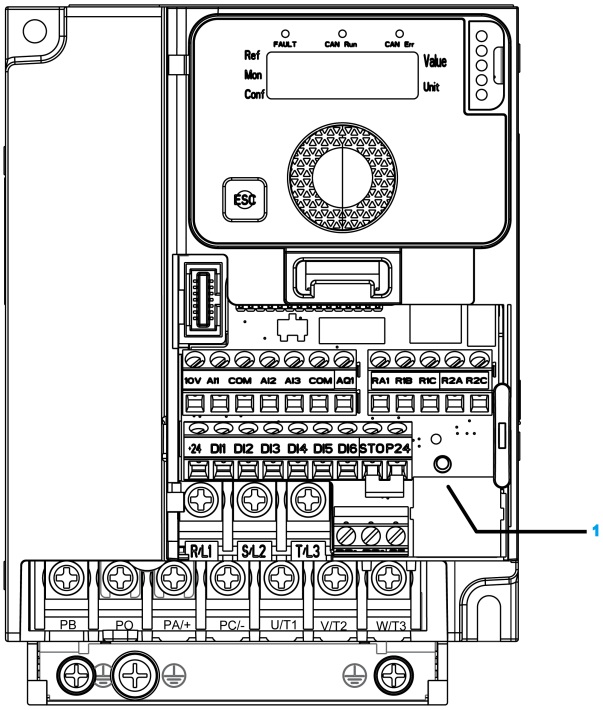
Hardware Setup

What’s in This Part

Hardware Presentation

Modbus Serial Communication Port

The following figure shows the terminal view of the ATH230 drive:



1 Modbus serial communication port

Firmware Version

Compatibility

There is no specific firmware for Modbus serial communication. The drive firmware embeds the Modbus serial.

Electrical Data

Immunity Against Interference

- Use the Schneider Electric cable with 2 pairs of shielded twisted conductors (reference: TSXCSA100, TSXCSA200, and TSXCSA500).
- Keep the Modbus cable separated from the power cables (30 cm (11.8 in.) minimum).
- Make any crossovers of the Modbus cable and the power cables at right-angles, if necessary.

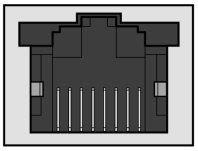
Accessories Presentation

Connection accessories should be ordered separately (see the catalog for more details).

Connection to the drive

Connect the RJ45 cable connector to the device connector.

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



Pin	Signal
1	Reserved
2	
3	
4	D1 (1)
5	D0 (1)
6	Reserved
7	VP, 10 Vdc(2)
8	Common (1)

(1) Modbus signals

(2) Supply for RS232 / RS485 converter or a remote terminal

RS485 Bus Schematic

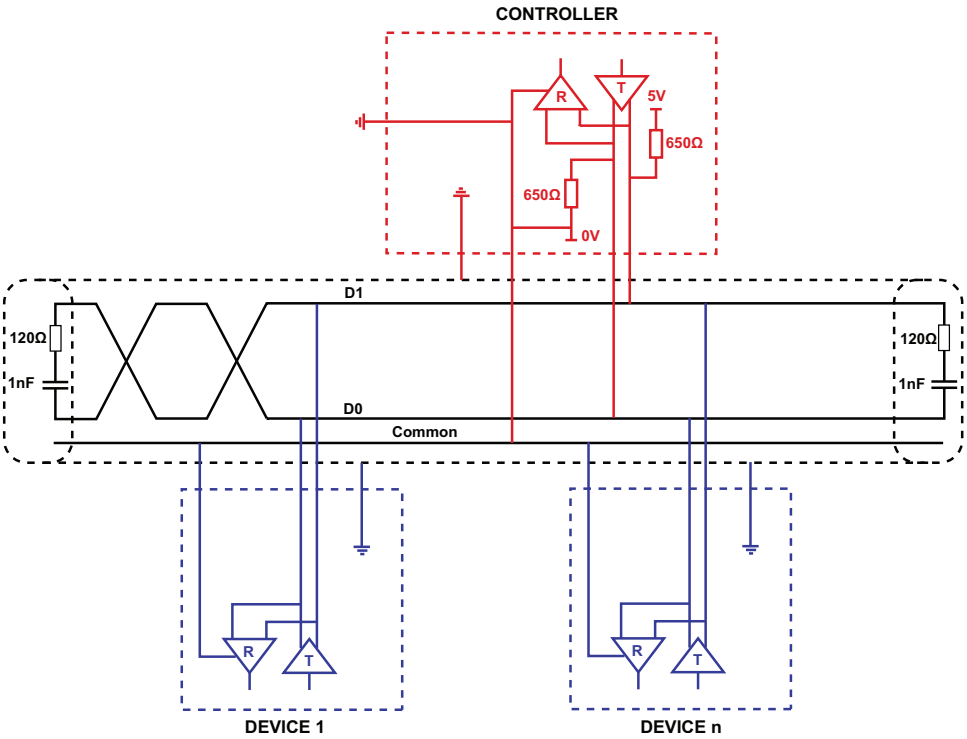
The RS485 standard allows variants of different characteristics:

- 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 trunk cable	Shielded cable with 1 twisted pair and at least a third conductor
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.
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.

Cyber Security

What's in This Part

Overview

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

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

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

The basic components of this approach are:

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

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

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

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

Defense in depth measures expected in the environment

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

⚠WARNING

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

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

Security Policy

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

⚠WARNING

CYBERSECURITY HAZARD

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

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

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

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

Potential Risks and Compensating Controls

Address potential risks using these compensating controls:

Area	Issue	Risk	Compensating controls
User accounts.	Default account settings are often the source of unauthorized access by malicious users.	If you do not change default password or disable the user access control, unauthorized access can occur.	Help to ensure user access control is enabled on all the communication ports and change the default passwords to help reduce unauthorized access to your device.
Secure protocols.	The device does not have the capability to transmit data encrypted using these protocols: • Bacnet MS/TP • Bacnet IP • Modbus serial	If a malicious user gained access to your network, they could intercept communication.	For transmitting data over internal network, physically or logically segment your network. For transmitting data over external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.

Data Flow Restriction

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

Firewall Product

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

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

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

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

Backing-up and Restoring the Software Configuration

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

Remote Access to the Drive

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

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

⚠WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

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

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

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

Deactivation of Unused Functions

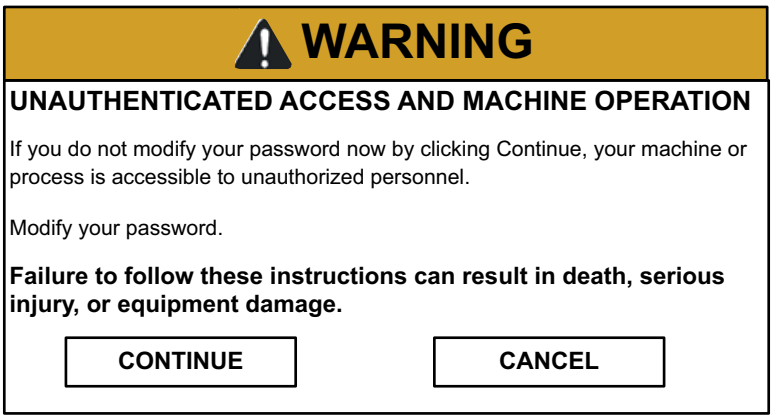
To avoid unauthorized access, it is advisable to deactivate unused functions.

Account Management Guidelines

The ATH200 password must contain:

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

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



Schneider Electric recommends to:

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

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

Software Setup

What's in This Part

[Modbus Fieldbus] Md1

Switch mode between Modbus and BACnet MS/TP

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.

[Modbus Address] Add

This parameter is used to set the Modbus address.

NOTE: The modification of communication parameters is taken into account after a power cycle of the drive.

The table presents the parameter settings:

Settings	Code	Value	Factory settings	Access	Logic address
[OFF]	oFF	0	oFF	R/W	16#1771 = 6001
[1 to 247]	1...247	1...247			

[Modbus Baud Rate] tbr

This parameter defines the baud rate at which data is transferred.

NOTE: The modification of communication parameters is taken into account after a power cycle of the drive.

The table presents the parameter settings:

Settings	Code	Value	Factory settings	Access	Logic address
[4800 bps]	4K8	24	19.2 Kbps	R/W	16#1773 = 6003
[9600 bps]	9K6	28			
[19200 bps]	19K2	32			
[38.4 Kbps]	38K4	36			

[Modbus Format] tFo

This parameter is used to define the data format.

NOTE: The modification of communication parameters is taken into account after a power cycle of the drive.

The table presents the parameter settings:

Settings	Code	Value	Description	Factory settings	Access	Logic address
[8-O-1]	8o1	2	8 data bits, odd parity, 1 stop bit	8E1	R/W	16#17734 = 6004
[8-E-1]	8E1	3	8 data bits, even parity, 1 stop bit			
[8-N-1]	8n1	4	8 data bits, no parity, 1 stop bit			
[8-N-2]	8n2	5	8 data bits, no parity, 2 stop bits			

[ModbusTimeout] tto

This parameter is used to set the Modbus timeout.

NOTE: The modification of communication parameters is taken into account after a power cycle of the drive.

The table presents the parameter settings:

Settings	Code	Value	Factory settings	Access	Logic address
[0.1...30.0]	0.1...30.0	1...300	10 s	R/W	16#17735 = 6005

Communication Scanner

Local Configuration of the Communication Scanner

The communication scanner is useful when used in combination by the Modbus 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 Modbus functions.

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]** ➡ **[Modbus network diag]**.

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, **[Mdb Com Interrupt]** `SLF1` or **[Fdbus Com Interrupt]** `CNF` is trigger.
- Drive control only takes effect once the drive has received the reference and the command from the active channels.

Command and Reference Channels

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

Parameter Name	Parameter Code		
	Taken Into Account by the Drive	Embedded	BACnet IP
Control word	CMd	CMd1	CMd3
Extended control word	CN1	CN11	CN13
Reference speed (rpm)	LFrd	LFd1	LFd3
Reference frequency (0.1 Hz)	LFr	LFr1	LFr3
Reference for torque control mode (0.1% of the normal torque))	Ltr	Ltr1	Ltr3
Reference value supplied by PI controller	P1SP	P1r1	P1r3
Reference value supplied by analog multiplier function	MFr	MFr1	MFr3

Diagnostics and Troubleshooting

What's in This Part

Fieldbus Status LEDs

LED Indicators

The fieldbus monitoring LED is displayed on the graphic display terminal. This LED is located in **[MONITORING]** menu **[Communication map]** -submenu, **[Modbus network diag]** - submenu.

LED Description

LED	Description
COM LED	Indicates the Modbus serial link connection status

COM LED : Link Activity

The table provides the LED status for Modbus serial connection

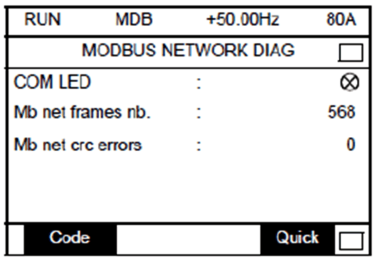
Color & Status	Description
OFF	No link
flashing	Fieldbus active

Communication Diagnostics

These parameters are visible only with the graphic display terminal.

On the terminal, in the **[MONITORING]** menu (**[Communication map]** submenu,

The **[Modbus network diag]** submenu can be used to display the status of the Modbus network communications.



⊗ Indicates a LED, which is not lit.

Modbus Counters

- **[Mdb Frame Nb]** indicate the number of Modbus frames received. The counter counts both correct and incorrect frames.
- **[Mdb CRC errors]** indicate the number of Modbus frames containing checksum errors.

In the case of these two counters, only frames that are destined for the drive and whose Modbus address is supplied by the **[Modbus Address]** parameter are counted. Broadcast frames are not counted.

[Mdb Frame Nb] nICt is modulo 65 536 counters, this means that, the value is reset to zero once the value of 65 535 is reached.

By contrast, the **[Mdb CRC errors]** nIEC remain at 65 535 once this value is reached.

Each Modbus counter corresponds to a drive parameter:

Menu	Parameter Name	Code	Logical Address
[Modbus network diag] Mnd	**[Mdb Frame Nb]**	nICt	6011
	[Mdb CRC errors]	nIEC	6010

Modbus Communication State

This can be accessed from the menu:

[Configuration] CONF / **[Full]** FULL / **[Communication]** COM / **[Modbus Fieldbus]** Md1 / **[Modbus stat]** COM1

[R0T0] r0t0: Modbus no reception, no transmission = communication idle

[R0T1] r0t1: Modbus no reception, transmission

[R1T0] r1t0: Modbus reception, no transmission

[R1T1] r1t1: Modbus reception and transmission

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 **[ModbusTimeout]** parameter

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

Value	Meaning
triggers a drive detected error [Mdb Com Interrupt] `SLF1` **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 **[Modbus Com Warn]** `SLLA` 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]**, Modbus 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 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. **[ModbusTimeout]** is activated.
2. After the end of the delay of **[ModbusTimeout]**, the motor is stopped following the value set on **[Modbus Error Resp]**.
3. An error **[Mdb Com Interrupt]** `SLF1` is triggered, and depending of **[Auto Fault Reset]**, **[R1 Assignment]** is deactivated (if set to **[Operating State Fault]** following the value set on **[Modbus Error Resp]**).

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.

[Incorrect Config] CFF

Incorrect configuration error

Probable Cause	• Option module changed or removed. • Control block replaced by a control block configured on a drive with a different rating. • The current configuration is inconsistent.
Remedy	• Check that there are no detected module errors. • In the event of the option module being changed/removed deliberately, see the remarks below. • Return to factory settings or retrieve the backup configuration, if it is valid.
Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Invalid Configuration] CF1

Invalid configuration error

Probable Cause	Invalid configuration. The configuration loaded in the drive via the bus or communication network is inconsistent.
Remedy	• Check the configuration loaded previously. • Load a compatible configuration.
Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Conf Transfer Error] CF12

Configuration transfer error

Probable Cause	Invalid configuration. The configuration loaded in the drive via the bus or communication network is inconsistent.
Remedy	• Check the configuration loaded previously. • Load a compatible configuration.
Clearing the Error Code	This detected error is cleared as soon as its cause has been removed.

[Ch Switch Error] CSF

Channel switching detected error

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

[Modb Com Interrupt] SLFI

Modbus communication interruption error

Probable Cause	Communication interruption on the Modbus 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 **[ModbusTimeout]** ETO meets the requirements of your application.
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*).

Annex

What's in This Part

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
- PROFIDRIVE
- CIP AC Drive

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

I/O Profile

Using the I/O profile simplifies PLC programming.

The I/O profile mirrors the use of the terminal strip for control by utilizing 1 bit to control a function.

The I/O profile for the drive can also be used when controlling via a fieldbus. The drive starts up as soon as the `run` command is sent.15 bits of the control word (bits 1...15) can be assigned to a specific function.

This profile can be developed for simultaneous control of the drive via:

- The terminals
- The Modbus control word
- The fieldbus module control word

The I/O profile is supported by the drive itself and therefore in turn by all the communication ports.

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.]** `SnSn`,

Functional Description

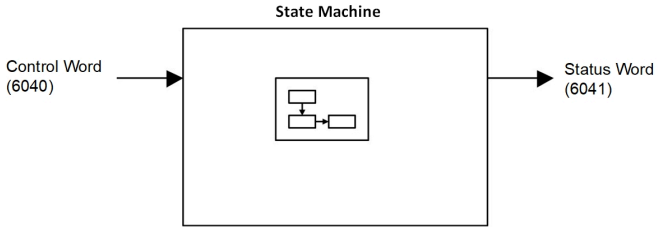
Introduction

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

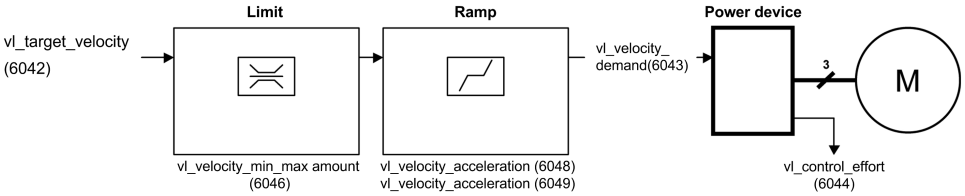
CiA402

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:



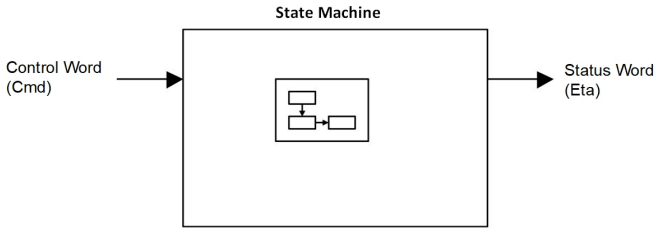
Simplified diagram for speed control in *Velocity* mode:



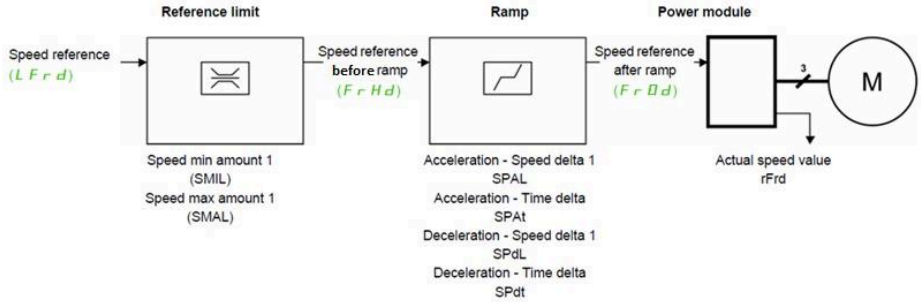
Altivar HVAC Drive

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:

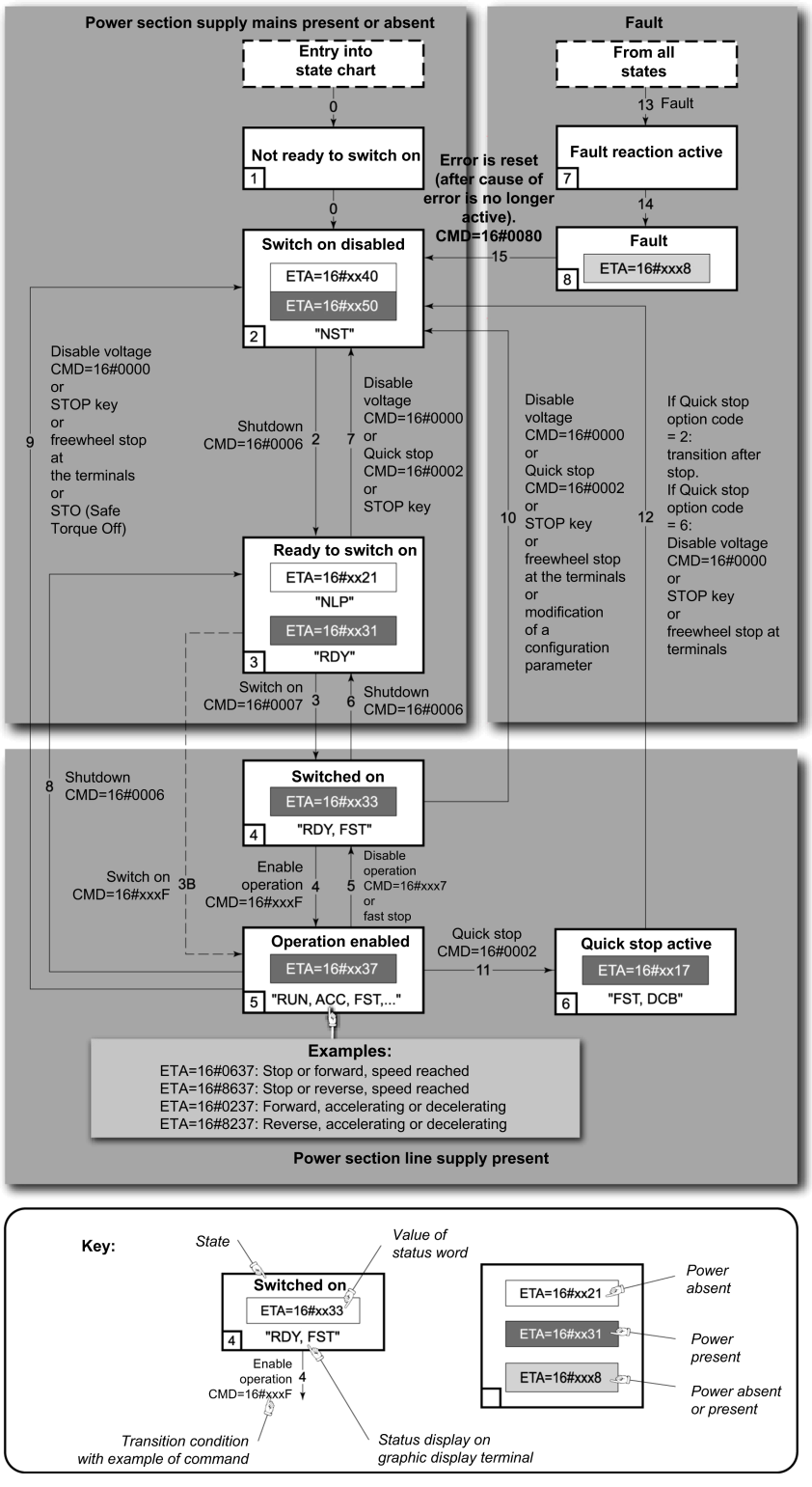


CIA402 Operating State Diagram

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 0 = Forward direction asked 1= Reverse direction asked	Reserved (=0)	Reserved (=0)	Halt Halt

Command	State Transition	Final Operating State	Bit 7 Fault Reset	Bit 3 Enable Operation	Bit 2 Quick Stop	Bit 1 Enable Voltage	Bit 0 Switch On	Example Value
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	Modbus Serial
Bit 11	C111
Bit 12	C112
Bit 13	C113
Bit 14	C114
Bit 15	C115

For example, to assign the DC injection braking to bit13 of Modbus serial, simply configure the **[DC injection]** `DCI` parameter with the **[C113]** `C113` 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	–
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.

I/O Profile

I/O Profile via **[Control Mode]** is set to **[I/O profile]**.

As well as physical digital inputs commanding the device in terminal command, the device can be commanded by line channel and each bit of the control word can be assigned to a dedicated function if the bit is free. **[I/O profile]** makes it possible to go from 4 physical digital inputs to 16 virtual digital inputs.

NOTE: The customer must monitor the **[Device State]** `HMIS`.

A function input can be assigned to:

- A virtual input (Cd00 to Cd15) according to the active command channel, corresponding bit of the control word or digital input of the terminal must be used to activate / deactivate the function.
- A terminal input (DI1 to DI6) irrespective of the active command channel, the function can be activated / deactivated using the corresponding digital input (exception for some function that requires to have the terminal as active command channel to activate / deactivate the function).

The function **[Command Switching]** can be activated / deactivated, irrespective of the active command channel, using the corresponding bit of a terminal input or of the control word **[Cy●●]**:

- A modbus control word (**[C100]** to **[C115]**)
- A fieldbus module control word (**[C300]** to **[C315]**).

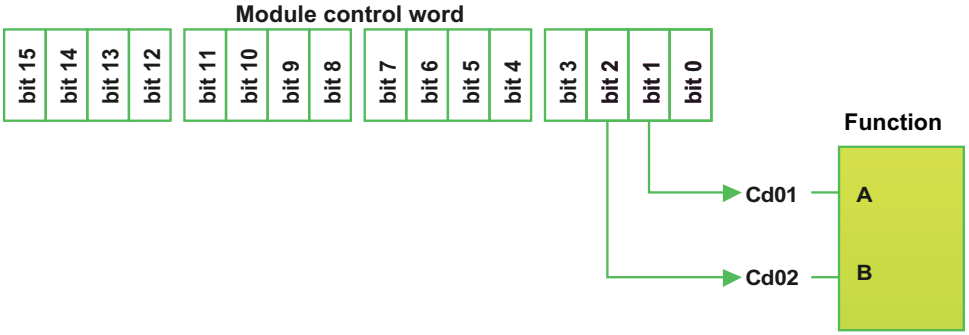
Bit	Fixed assignments		
	Virtual Inputs	Terminals	Modbus
bit 0	Cd00	DI1	C100
bit 1	Cd01	DI2	C101
bit 2	Cd02	DI3	C102
bit 3	Cd03	DI4	C103
bit 4	Cd04	DI5	C104
bit 5	Cd05	DI6	C105
bit 6	Cd06	-	C106
bit 7	Cd07	-	C107

Bit	Fixed assignments		
	Virtual Inputs	Terminals	Modbus
bit 8	Cd08	-	C108
bit 9	Cd09	-	C109
bit 10	Cd10	-	C110
bit 11	Cd11	-	C111
bit 12	Cd12	-	C112
bit 13	Cd13	-	C113
bit 14	Cd14	-	C114
bit 15	Cd15	-	C115

Schematic diagrams

Example:

- The function **A** is assigned to the bit 1 by set this function **A** to Cd01.
- The function **B** is assigned to the bit 2 by set this function **B** to Cd02.



NOTE: No matter which command channel is active, the function can always be activated.

Switched assignment

⚠WARNING

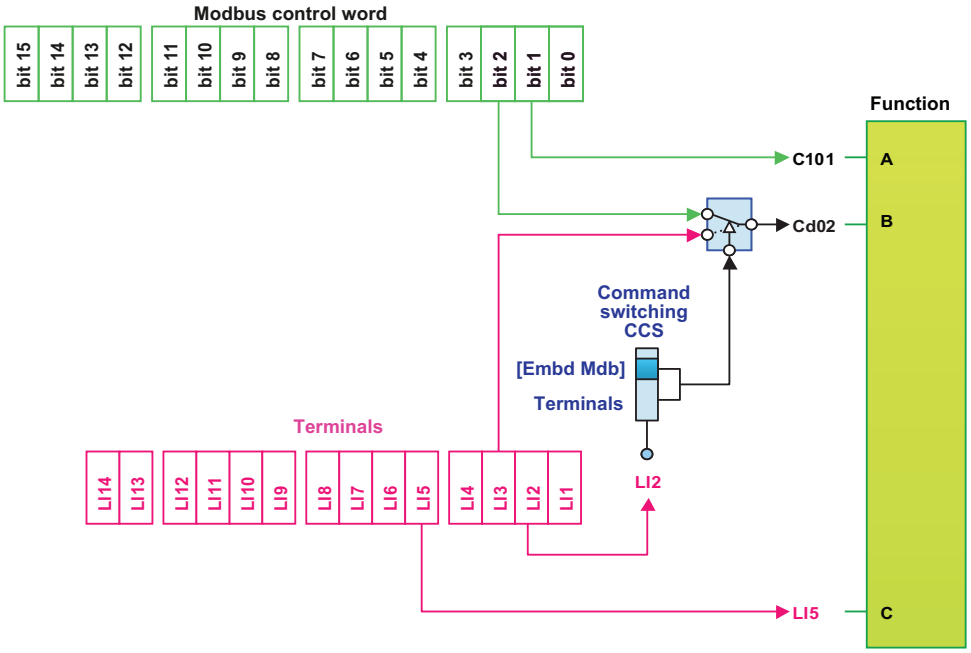
UNANTICIPATED EQUIPMENT OPERATION

- Verify that this behavior does not result in unsafe conditions by performing extensive commissioning tests.
- If the start on transition is not desired, the bits corresponding to the run command must always be reset before switching the active command channel to fieldbus.

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

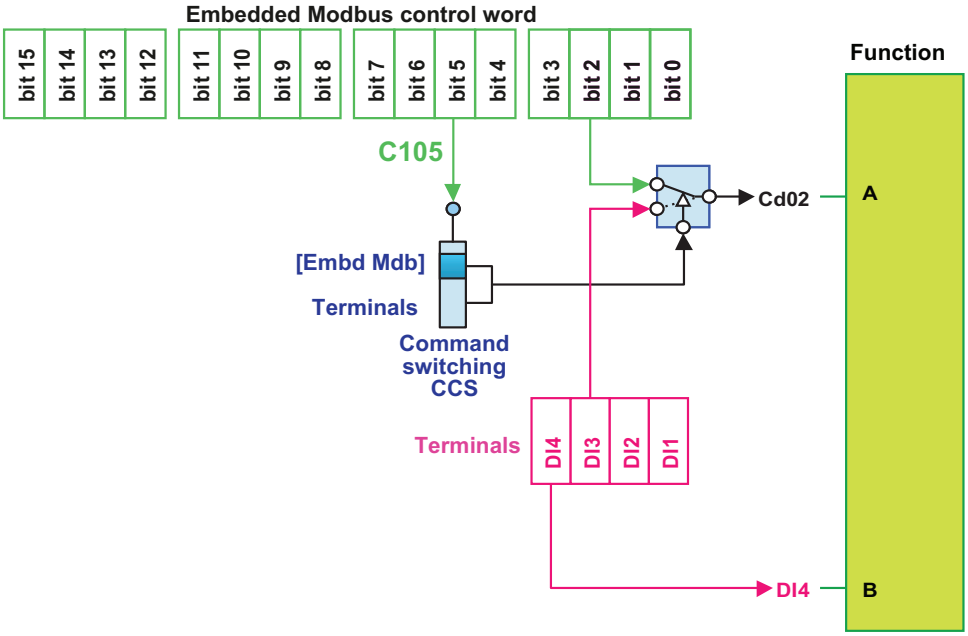
Example with:

- **[Command Switching]** managed by digital input.
- A function assigned to a control (here **C101**).
- B function assigned to a switched bit (here **CD02**).
- C function assigned to a digital input (here **DI5**).
- **[Cmd channel 1]** = **[Embd Mdb]**.
- **[Cmd channel 2]** = **[Terminal]**.



Example with:

- **[Command Switching]** managed by control word (here **C105**).
- A function assigned to a switched bit (here **CD02**).
- B function assigned to a digital input (here **DI4**).
- **[Cmd channel 1]** = **[Embd Mdb]**.
- **[Cmd channel 2]** = **[Terminal]**.



When a function is assigned to a switched bit (Cd00 to Cd15), the function can be activated via Terminals or selected communication channel according to the active command channel. To switch between Terminals and communication modules, use **[Command Switching]** function.

NOTE: A single function can be assigned to a bit at the same time, here as **[C105]** is assigned to **[Command Switching]**, Cd05 cannot be assigned to another function.

Extended Control Word

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

⚠WARNING

LOSS OF PARAMETER CONFIGURATION AFTER A POWER CYCLE

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

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

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

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

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

Code	Settings	
[Extended Ctrl Word] 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	***Factory setting asked***	***Memorize current configuration in EEPROM***	***Read current configuration in EEPROM***	***External error***	***Reserved***			
Bit at 0	Active on rising edge when motor is powered off. 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 ...)***	***Reserved***			***Drive locked in STOP***	***Serial link error inhibition***	***Parameter coherence deactivated and drive locked in STOP***
Bit at 0		in 0.1Hz				Deactivate.	Deactivate.	Deactivate. All parameters are validated.
Bit at 1		in internal unity (32767 = TFR)				Activate.	Activate.	Activate. No check of parameter consistency and device is locked when stopped.

Internal State register

	Bit 0	Bit 1	Bit 2	Bit 3
Function	***EEPROM access running***	***Parameter consistency checked***	***No more error present and drive in error state***	***Reserved***
Bit at 0	Access to the non-volatile memory stopped.	Not active.	The device: • is not in operating state "Error" • is in operating state "Error" and the error is active.	
Bit at 1	Access to the non-volatile memory in progress.	Active.	The device is in operating state "Error" and the error is no longer active (not reset).	

	Bit 4	Bit 5	Bit 6	Bit 7
Function	***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.

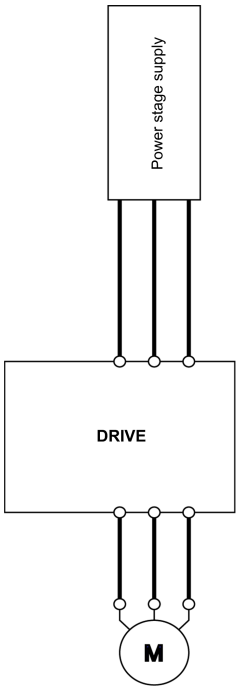
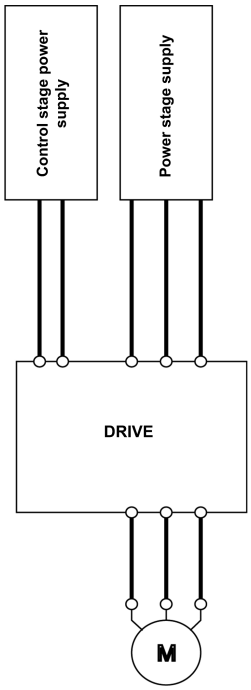
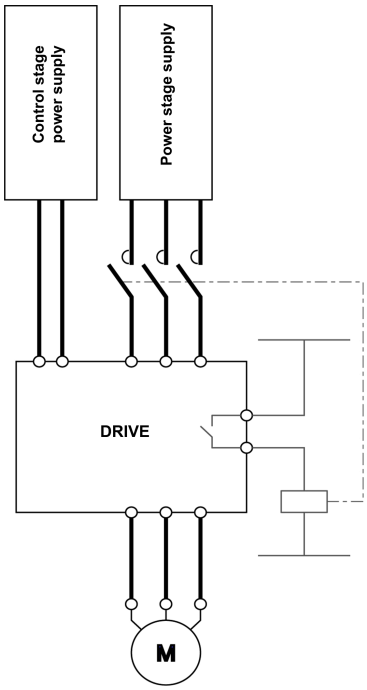
Starting Sequence

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

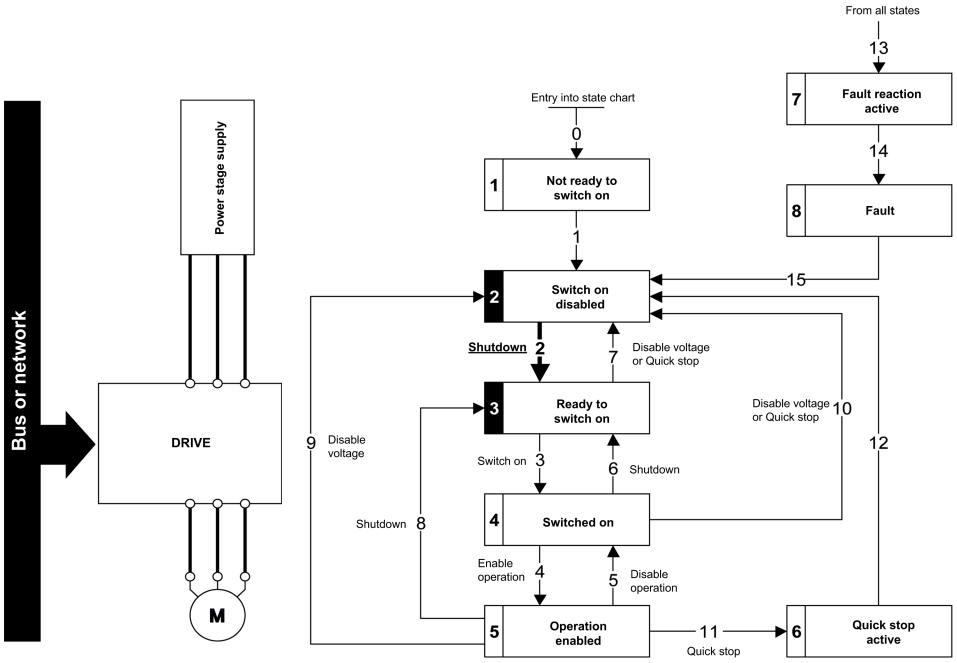
Both the power and control stages are powered by the power stage supply.

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:

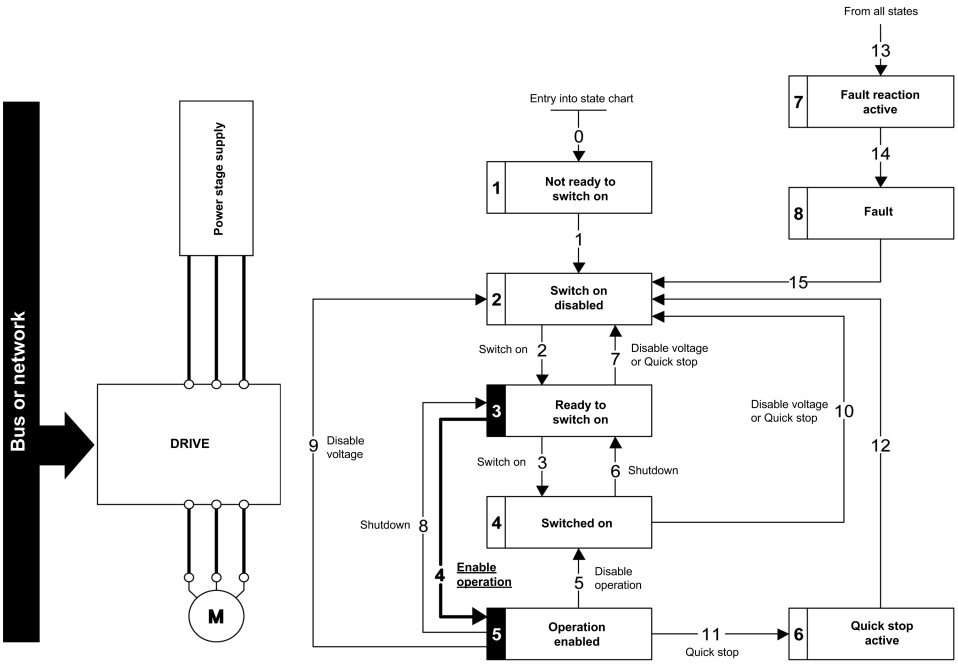
Step 1

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

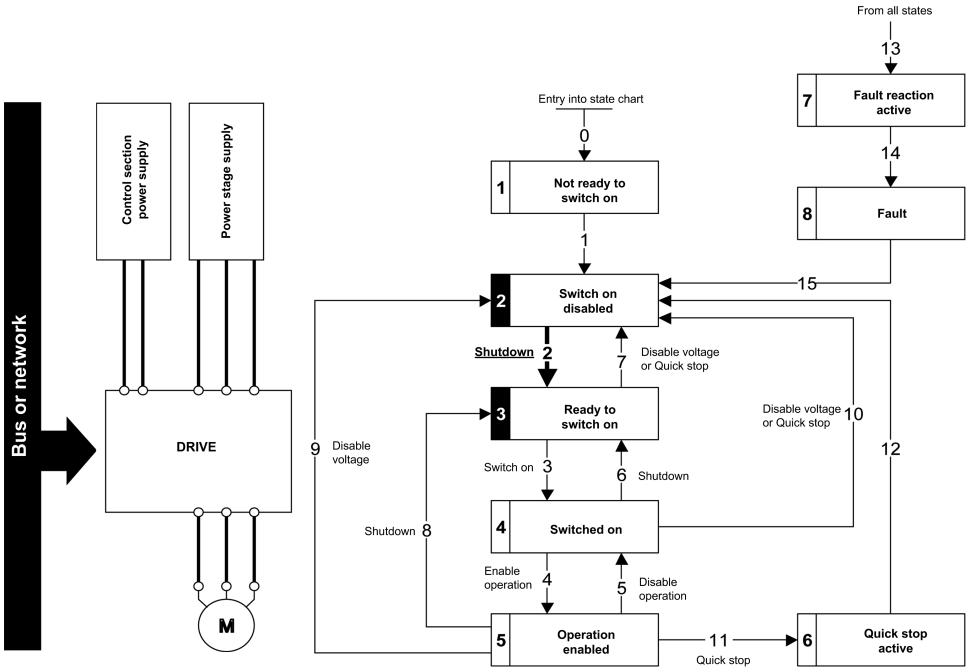
Power is supplied separately to the power and control stages.

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

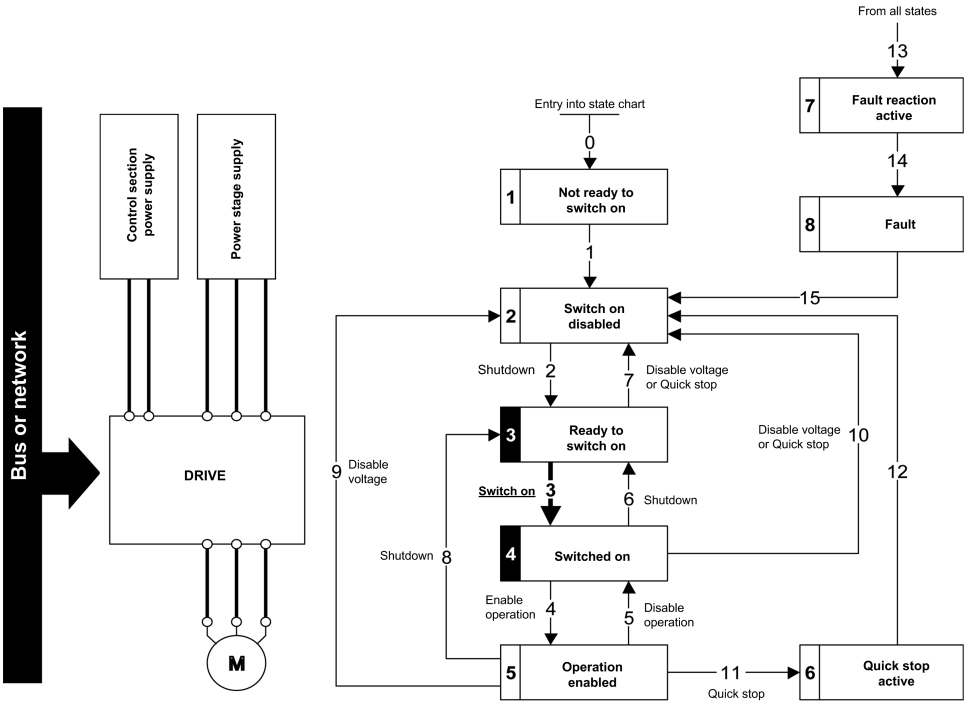


Step 2

- 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).

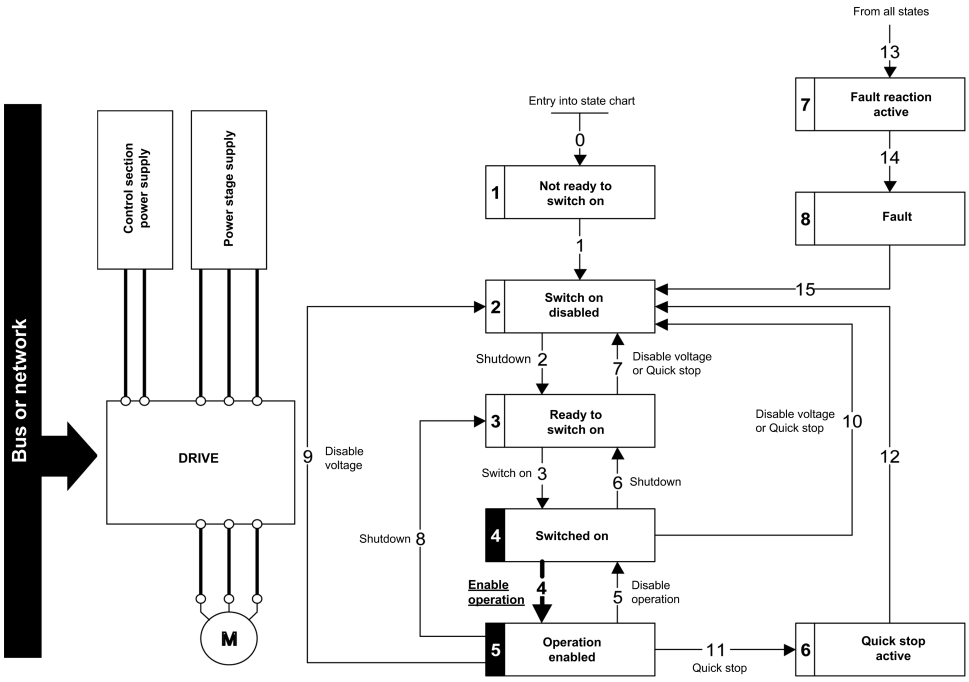
Power Stage Supply	HMI Panel	Status Word
Not present	**[No Mains Voltage]** NLP	21 hex
Present	**[Ready]** RDY	31 hex

- 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

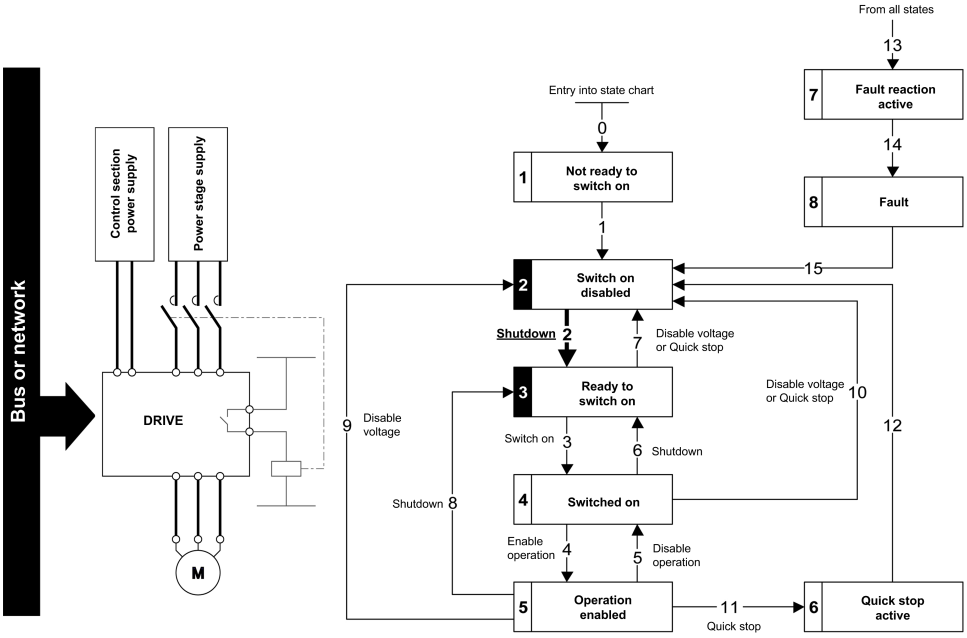
Power is supplied separately to the power and control stages.

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:

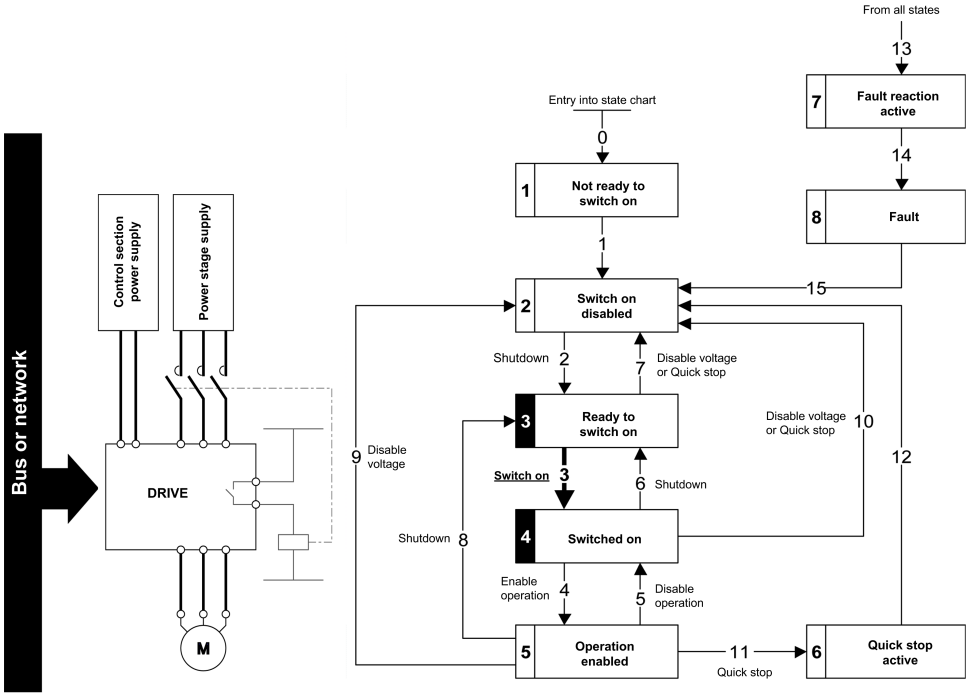
Step 1

- 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

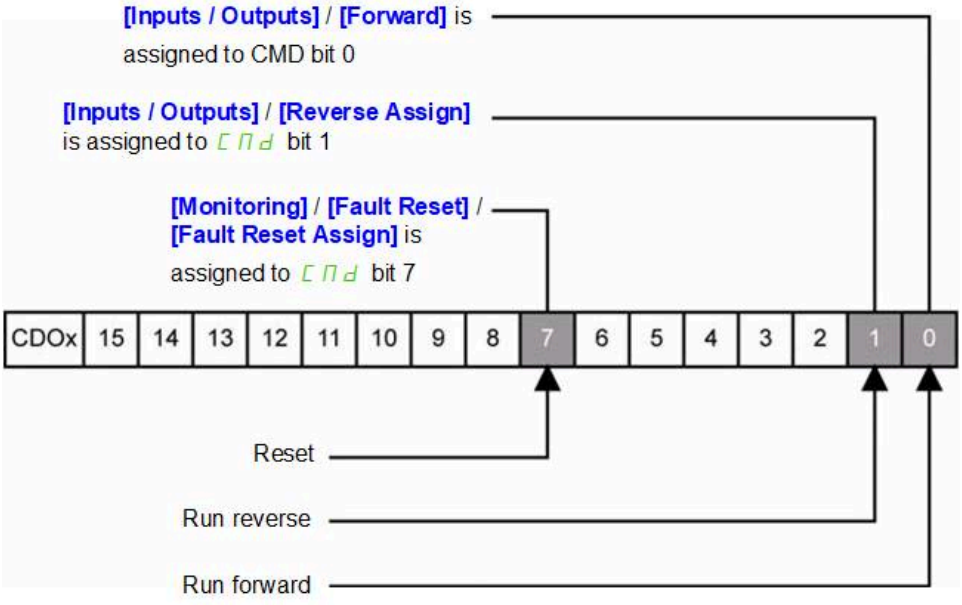
Configuring the Control Channel

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

- I/O mode - a simple command word (based on forward, reverse, and reset binary commands).
- 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 in I/O Profile

For the I/O profile, here is a simple example, which can be extended with additional features. The command word is made of run forward (bit 0 of CMd), run reverse (bit 1 of CMd), and the function fault reset (bit 7 of CMd).



The settings are the following:

[Ref Freq 1 Config] FR1	**[AI virtual 1]** AIU1
[Reverse Disable] RIN	Default
[Stop Key Enable] PST	Default
[Control Mode] CHCF	**[Separate]** SEP
[Command Switching] CCS	Default
[Cmd channel 1] CD1	**[Modbus]** Mbd

The bits of the command word can now be configured.

In the **[Inputs / Outputs]** menu, configure:

[Forward] Frd	**[CD00]** Cd00
[Reverse Assign] rrS	**[CD01]** Cd01

In the **[Monitoring]** menu, **[Fault reset]** submenu, configure:

[Fault Reset Assign] rSF	**[CD07]** Cd07

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

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

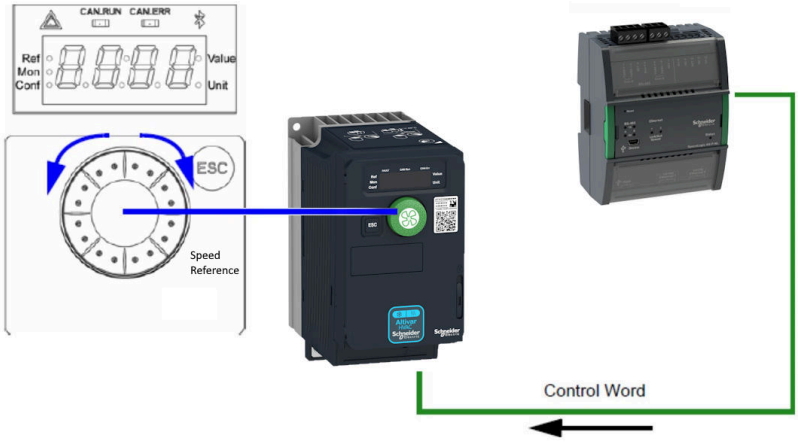
In the **[Command]** CtL - menu:

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

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

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

For example:



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

The settings are as shown in the table:

[Ref Freq 1 Config] FR1	**[AI virtual 1]** AIU1
[Reverse Disable] RIN	Default
[Stop Key Enable] PST	Default
[Control Mode] CHCF	**[Separate]** SEP
[Command Switching] CCS	Default
[Cmd channel 1] CD1	**[Modbus]** Mbd

Modbus Functions

What's in This Chapter

Modbus Protocol

Introduction

The transmission mode used is RTU. The frame does not contain message header and end of message bytes.

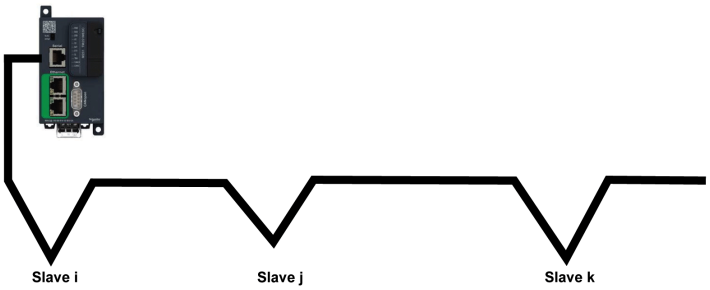
Device address	Request code	Data	CRC16

The data is transmitted in binary code.

The end of the frame is detected on a silence greater than or equal to three characters.

Principle

The Modbus protocol is a controller/device protocol



Only one device can transmit on the line at any time.

The controller manages the exchanges and only it can take the initiative.

It interrogates each of the devices in succession

No device can send a message unless it is invited to do so.

The controller repeats the question when there is an incorrect exchange, and declares the interrogated device absent if no response is received within a given time period.

If a device does not understand a message, it sends an exception response to the controller. The controller may or may not repeat the request.

Direct device-to-device communications are not possible.

For device-to-device communication, the application software must therefore be designed to interrogate a device and send back data received to the other device.

The 2 types of dialogue are possible between controller and devices:

- The controller sends a request to a device and waits for its response
- The controller sends a request to all devices without waiting for a response (broadcasting principle)

Addresses

Address specification:

- The device Modbus address can be configured from 1 to 247.
- Address 0 coded in a request sent by the controller is reserved for broadcasting. Devices take account of the request, but do not respond to it.

Supported Modbus Functions

Introduction

The drive supports the following Modbus functions:

Function Name	Code		Description	Remarks
	Dec.	Hex		
Read Holding Registers	03	03 hex	Read N output words	Maximum PDU length: 125 words
Write One Output Word	06	06 hex	Write 1 output word	–
Write Multiple Registers	16	10 hex	Write N output word	Maximum PDU length: 123 words
Read/write Multiple Registers	23	17 hex	Read/write multiple registers	Maximum PDU length: 20 words (W), 20 words (R)
(Subfunction) *Read Device Identification*	43/14	2B hex/ 0E hex	Encapsulated interface transport/ Read device identification	–
Diagnostics	08	08 hex	Diagnostics	–

Read Holding Registers (03 hex)

This function code is used to read the contents of a contiguous block of holding registers in a remote device.

The Request PDU specifies the starting register address and the number of registers. In the PDU Registers are addressed starting at zero. Therefore registers numbered 1-16 are addressed as 0-15.

The register data in the response message are packed as two bytes per register, with the binary contents right justified within each byte. For each register, the first byte contains the high order bits and the second contains the low order bits.

Request

Function code	1 byte	03 hex
Starting address	2 bytes	0000 hex...FFFF hex
Quantity of registers	2 bytes	1 to 63 (0x3F)

Response

Function code	1 byte	03 hex
Byte count	1 byte	2 x N(1)
Register value	N(1) x 2 bytes	–
(1) N: Quantity of registers		

Detected error

Detected error code	1 byte	83 hex
Exception code	1 bytes	01...04

Then, here an example of a request to read registers @3102 to @3105:

Code	Name	Logic Address
SFr	Switching frequency (Hz)	0C1E hex= 3102
tFr	Maximum output frequency (Hz)	0C1F hex= 3103
HSP	High speed (Hz)	0C20 hex= 3104
LSP	Low speed (Hz)	0C21 hex= 3105

Read these 4 words in device address 02 hex, using function 03 hex:

Request

device no.	Function Code	Number of first word	Number of words	CRC16
02	03	0C1E	004	276C

Response

device no.	Function Code	Number of bytes read	First word value	Second word value	Third word value	Last word value	CRC16
02	03	08	0028	0258	01F4	0000	52B0
	Value of:	–	@3102	@3103	@3104	@3105	–
	Parameters:	–	IN	LCS	BST	TBS	–

Analyzed:

Code	Read		Result
	hex	dec.	
SFr	0028 hex	40	Switching frequency at 40 Hz.
tFr	0258 hex	600	Maximum output frequency at 600 Hz.
HSP	01F4 hex	500	High speed at 500 Hz.
LSP	0000 hex	0	Low speed at 0 Hz.

Write 1 Output Word (06 hex)

This function code is used to write a single holding register in a remote device.

The Request PDU specifies the address of the register to be written. Registers are addressed starting at zero. Therefore register numbered 1 is addressed as 0.

The normal response is an echo of the request, returned after the register contents have been written.

Request

Function code	1 byte	06 hex
Register address	2 bytes	0000 hex...FFFF hex
Register value	2 bytes	0000 hex...FFFF hex

Response

Function code	1 byte	06 hex
Register address	2 bytes	0000 hex...FFFF hex
Register value	2 bytes	0000 hex...FFFF hex

Detected error

Detected error code	1 byte	86 hex
Exception code	1 bytes	01...04

Then, here an example of a request to write register @9001:

Write on:

Code	Name	Logic Address
ACC	Acceleration ramp time (s)	2329 hex= 9001

Write value 000D hex in device address 02 hex:

Code	Write	
	hex	dec.
ACC	000D hex	13

Request:

device no.	Function Code	Word number	Value of word	CRC16
02	06	2329	000D	9270

Response:

device no.	Function Code	Word number	Value of word	CRC16
02	06	2329	000D	9270

Analyzed:

Code	**Read**		**Result**
	hex	**dec.**	
ACC	000D hex	13	ACC = 13 s

Write Multiple Register (10 hex)

This function code is used to write a block of contiguous registers (1 to 123 registers) in a remote device.

The requested written values are specified in the request data field. Data is packed as two bytes per register.

The normal response returns the function code, starting address, and quantity of registers written.

Request

Function code	1 byte	10hex
Register address	2 bytes	0000 hex...FFFF hex
Register value	2 bytes	0000 hex...FFFF hex

Response

Function code	1 byte	10 hex
Register address	2 bytes	0000 hex...FFFF hex
Register value	2 bytes	0000 hex...FFFF hex

Detected error

Detected error code	1 byte	90 hex
Exception code	1 bytes	01...04

Then, here an example of a request to write registers @9001 and @9002:

Write on:

Code	Name	Logic Address
ACC	Acceleration ramp time (s)	2329 hex= 9001
DEC	Deceleration ramp time (s)	2330 hex= 9002

Write values on device address 02 hex:

Code	Write	
	hex	dec.
ACC	0014 hex	20
DEC	001E hex	30

Request

device no.	Request code	No. of first word	Number of words	Number of bytes	Value of first word	Value of Second word	CRC16
02 hex	10 hex	2329 hex	0002 hex	04 hex	0014 hex	001E hex	B60D hex

Response

device no.	Response code	No. of first word	No. of words	CRC16
02 hex	10 hex	2329 hex	0002 hex	0BA0 hex

Analyzed:

Code	Read		Result
	hex	dec.	
ACC	0014 hex	20	ACC = 20 s
DEC	001E hex	30	DEC = 30 s

Read/Write Multiple Registers (17 hex)

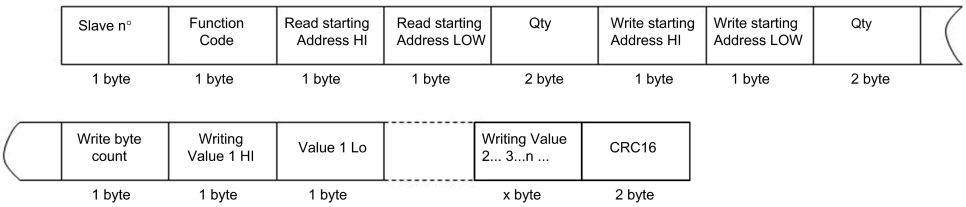
This function code performs a combination of one read operation and one write operation in a single MODBUS transaction. The write operation is performed before the read. Holding registers are addressed starting at zero. Therefore holding registers 1-16 are addressed in the PDU as 0-15.

The request specifies the starting address and number of holding registers to be read as well as the starting address, number of holding registers, and the data to be written. The byte count specifies the number of bytes to follow in the write data field.

The normal response contains the data from the group of registers that were read. The byte count field specifies the quantity of bytes to follow in the read data field.

For example

Description	Length in Byte	Value	Comment
Function code	1	17 hex	–
Read starting address	2	XXXX hex	Modbus address
Quantity	2	03 hex	Contain number of holding registers to be read
Write starting address	2	XXXX hex	Modbus address
Quantity	2	03 hex	Contain number of holding registers to be written
Write byte count	1	06 hex	The byte count specifies the number of bytes to follow in the field write register value
Write registers value	6	XXXXXX XXXXXX hex	Address to be written respectively in NCA1 to NCA3. For example: CMD, LFRD, CMI



Read Device Identification (2B hex/0E hex)

This function code allows reading the identification and additional information relative to the physical and functional description of a remote device, only.

The Read Device Identification interface is modeled as an address space composed of a set of addressable data elements. The data elements are called objects and an object Id identifies them.

The interface consists of 3 categories of objects :

- Basic Device Identification:

  All objects of this category are mandatory : VendorName, Product code, and revision number.
- Regular Device Identification:

  In addition to Basic data objects, the device provides additional and optional identification and description data objects. All of the objects of this category are defined in the standard but their implementation is optional.
- Extended Device Identification:

  In addition to regular data objects, the device provides additional and optional identification and description private data about the physical device itself. All of these data are device dependent.

The table provides the device identification details:

ID	Name / Description	Type
00 hex	`VendorName`	ASCII String
01 hex	`ProductCode`	ASCII String
02 hex	`MajorMinorRevision`	ASCII String
06 hex	`ProductName`	ASCII String

Request

device no.	Function Code (2B)	Type of MEI 0E	Read Device Id 01	Object Id 00	CRC16	
					Lo	Hi
1 byte	1 byte	1 byte	1 byte	1 byte	2 bytes	

Response

device no.	2B	Type of MEI 0E	Read Device Id 01	Degree of conformity 02
1 byte	1 byte	1 byte	1 byte	1 byte

Example

Number of additional frames 00	Next object Id 00	Number of objects 03
1 byte	1 byte	1 byte

Id of object number 1 00	Length of object number 1 12	Value of object number 1 **Schneider Electric**
1 byte	1 byte	18 bytes

Id of object number 2 01	Length of object number 2 0B	Value of object number 2 **ATV320 ATH230xxxxxx**
1 byte	1 byte	11 bytes

Id of object number 3	Length of object number 3	Value of object number 3
02	04	**0201**
1 byte	1 byte	4 bytes

CRC16	
Lo	Hi
1 byte	1 byte

The total response size equals 49 bytes

The three objects contained in the response correspond to the following objects:

- Object number 1: Manufacturer name (always **Schneider Electric**, that is 18 bytes).
- Object number 2: Device reference (ASCII string; for example, **ATV320 ATH230xxxxxx**, that is 11 bytes).
- Object number 3: Device version, in **MMmm** format where **MM** represents the determinant and **mm** the subdeterminant (4-bytes ASCII string; for example,: **0201** for version 2.1).

NOTE: The response to function 43 may be negative; in this case, the response located at the top of the next page is sent by the drive rather than the response described above.

Diagnostics (08 hex)

The function (08 hex) provides a series of tests for checking the communication system between a controller device and a device, or for checking various internal error conditions within a device.

The function uses a two–byte sub-function code field in the query to define the type of test to be performed. The device echoes both the function code and sub-function code in a normal response. Some of the diagnostics cause data to be returned from the remote device in the data field of a normal response.

In general, issuing a diagnostic function to a remote device does not affect the running of the user program in the remote device. User logic, like discrete and registers, is not accessed by the diagnostics. Certain functions can optionally reset error counters in the remote device.

A device device can, however, be forced into ‘Listen Only Mode’ in which it will monitor the messages on the communications system but not respond to them. This can affect the outcome of your application program if it depends upon any further exchange of data with the remote device. Generally, the mode is forced to remove a malfunctioning remote device from the communications system.

Subcode 00 hex: Echo

This function asks the device being interrogated to echo (return) the message sent by the controller in its entirety.

Subcode 0A hex: Counter reset

This function resets all the counters responsible for monitoring a device exchanges.

Subcode 0C hex: Read message counter responsible for counting messages received with checksum errors.

Subcode 0E hex: Read message counter responsible for counting messages addressed to device. Read a word indicating the total number of messages addressed to the device, regardless of type (excluding broadcast messages).

Request and response (the frame format is identical)

device no.	Function Code (08)	Subcode		Data		CRC16	
		Hi	Lo	Hi	Lo	Lo	Hi
1 byte	1 byte	2 bytes		N bytes		2 bytes	

Subcode	Request Data	Response Data	Function Executed
00	XX YY	XX YY	Echo
0A	00 00	00 00	Counter reset
0C	00 00	XX YY (= counter value)	Read message counter responsible for counting messages received with checksum errors
0E	00 00	XX YY (= counter value)	Read message counter responsible for counting messages addressed to device

Example

Values 31 hex and 32 hex echoed by device address 04 hex.

Request and response (the frame format is identical)

device no.	Request code or response code	Subcode		Value of first byte	Value of second byte	CRC16	
		Hi	Lo			Lo	Hi
02 hex	08 hex	00 hex	00 hex	31 hex	32 hex	74 hex	1B hex

Glossary

A

Abbreviations:

Req. = Required

Opt. = Optional

AC:

Alternating Current

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

C

Client:

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

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

CRC16:

Cyclical Redundancy Check.

D

DC:

Direct Current

dec.:

Decimal

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

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.

Q

Quick Stop:

The quick Stop function can be used for fast deceleration of a movement as a response to a detected error or via a command.

R

R/WS:

Read and write (write only possible when the drive is not in RUN mode). It is not possible to write these parameters in "5-Operation enabled" or "6-Quick stop active" states. If the parameter is written in the "4-Switched on" state, transition to "2-Switch on disabled" is activated.

S

Server:

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

SF: Switch Frequency

V

VSD:

Variable Speed Drive

W

Warning:

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

Z

Zone of operation:

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

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

JPS43217.01