

Altivar HVAC ATH600

Variable Speed Drives for Synchronous and Asynchronous Motors

Modbus Serial Link Manual

JPS89286.01
04/2026



Legal Information

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

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

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

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

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

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

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

Table of Contents

Safety Information.....	5
About the document	7
Hardware Setup	15
Modbus Serial Communication Port	16
Firmware Version	17
Electrical Data	18
Cybersecurity Generalities	20
Overview	21
Security Policy.....	25
Product Defense-in-Depth.....	26
ATH600 Security Policy.....	29
Potential Risks and Compensating Controls	32
Data Flow Restriction.....	33
Device Recovery and Reconstitution.....	34
Upgrades Management.....	35
Port Hardening	36
Security Functionality Verification.....	37
Software Setup.....	39
[Modbus Fieldbus] MD1	40
Most Common parameters	42
Communication Scanner.....	48
Monitoring of Communication Channel.....	52
Diagnostics and Troubleshooting	54
Fieldbus Status LEDs	55
Configuring Communication Error Response	57
Communication troubleshooting	59
Warning Codes.....	60
Communication error codes.....	61
Annex.....	64
Operation.....	65
Profile	66
Functional Profiles Supported by the Drive.....	67
Functional Description.....	68
CIA402 Operating State Diagram	69
Description of Operating States.....	70
Device Status Summary	71
Command Register <small>CMD</small>	72
Stop Commands.....	73
Assigning Control Word Bits	73
[CIA402 State Reg] <small>ETA</small>	74
I/O Profile	75
Extended Control Word	78
Internal State register	79
Starting Sequence	80
Starting Sequence for a Drive Powered by the Power Stage	
Supply	81
Starting Sequence for a Drive with Separate Control Stage	83

Starting Sequence for a Drive with Mains Contactor Control	86
Operating Modes	88
Configuring the Control Channel	89
Configuration of the Drive for Operation in I/O Profile	89
Configuration of the Drive for Operation with CiA 402 Profile in Combined Mode	90
Configuration of the Drive for Operation with CiA 402 Profile in Separate Mode	90
Modbus Functions	91
Modbus Protocol	92
Supported Modbus Functions	93
Glossary	103

Safety Information

Important Information

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



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



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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

Please Note

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

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

Qualification of Personnel

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

Intended Use

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

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

About the document

Document Scope

The purpose of this document is to show you how to configure the Altivar HVAC ATH630 and ATH650 to use 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 ATH600 drives: ATH630 and ATH650.

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

Product Related Information

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

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

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

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

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

DANGER

ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION

Do not use damaged products or accessories.

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

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

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

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

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

⚠ WARNING

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

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

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

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

⚠ WARNING

UNANTICIPATED EQUIPMENT OPERATION

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

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

⚠ WARNING

LOSS OF CONTROL

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

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

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

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

⚠ WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

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

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

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

⚠ WARNING

LOSS OF CONTROL

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

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

General Cybersecurity Information

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

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

Schneider Electric provides additional information and assistance:

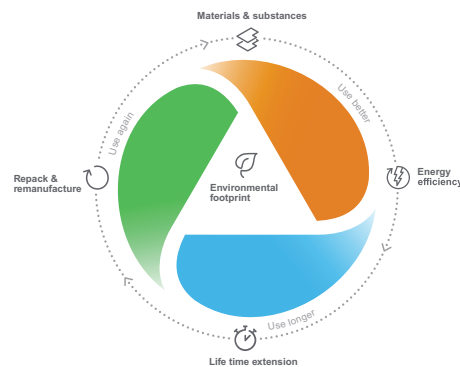
- [Subscribe to the Schneider Electric security newsletter.](#)
- [Visit the Cybersecurity Support Portal web page to:](#)
 - [Find Security Notifications.](#)
 - [Report vulnerabilities and incidents.](#)
- [Visit the Schneider Electric Cybersecurity and Data Protection Posture web page to:](#)
 - [Access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

Environmental Data

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

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

Five data categories across the product lifecycle



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

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

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

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

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

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

Related Documents

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

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

- The whole catalog for detailed characteristics and selection guides,
- The CAD files to help design your installation, available in over 20 different file formats,
- All software and firmware to maintain your installation up to date,
- A large quantity of White Papers, Environment documents, Application solutions, Specifications... to gain a better understanding of our electrical systems and equipment or automation,
- And finally all the User Guides related to your drive, listed below:

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

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

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

Information on Non-Inclusive or Insensitive Terminology

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

Terminology used in this document

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

Among others, these standards include:

- ISO 13849: The Foundation of Functional Safety in the Machinery
- IEC/UL 60204-1: Safety of machinery - Electrical equipment of machines – Part 1: General requirements.
- IEC/UL 61010: Safety requirements for electrical equipment for measurement, control, and laboratory use.
- IEC 61158 series: Industrial communication networks - Fieldbus specifications
- IEC/UL 61508 Ed.2 series: Functional safety of electrical/electronic/programmable electronic safety-related.
- IEC 61784 series: Industrial communication networks - Profiles.
- IEC 61784-5-3: Industrial communication networks - Profiles - Part 5-3: Installation of fieldbuses - Installation profiles for CPF 3
- IEC/UL 61800 series: Adjustable speed electrical power drive systems.
- IEC 61918: Industrial communication networks - Installation of communication networks in industrial premises.
- IEC 62443 /UL 2900: Security for industrial automation and control systems.

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

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

Also see the Glossary at the end of this manual.

Contact us

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

Schneider Electric

1884 Boulevard de la Défense

92000 Nanterre

France

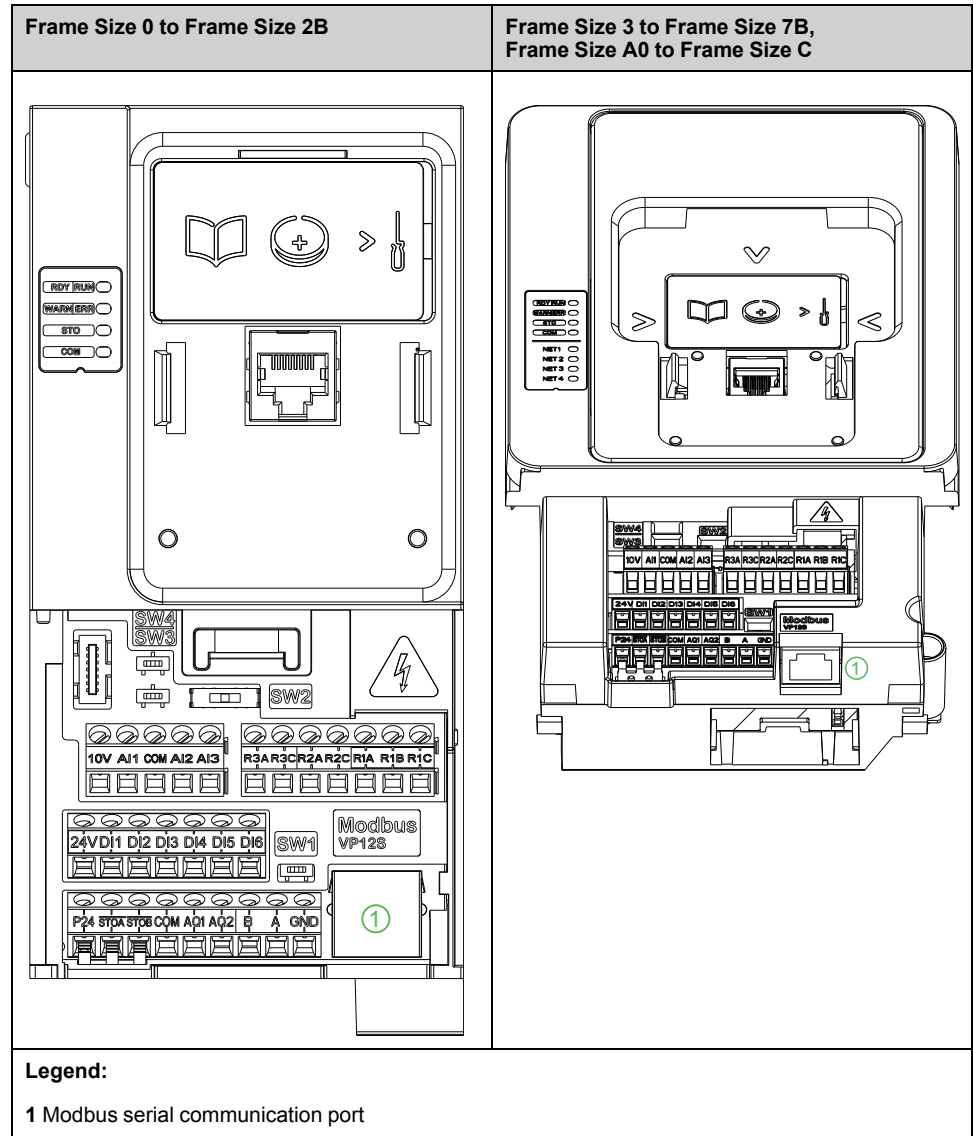
Hardware Setup

What's in This Part

Modbus Serial Communication Port.....	16
Firmware Version	17
Electrical Data.....	18

Modbus Serial Communication Port

The following figure shows the terminal view of the ATH630 drive:



Firmware Version

Compatibility

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

Firmware update

The firmware update can be updated directly via Ecostruxure Automation Device Maintenance (EADM) or SoMove. **It is recommended to use the Flashing Cordset (VW3A8127) when flashing the product.**

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

www.se.com/CCC.

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.

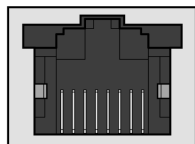
Accessories Presentation

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:



8 7 6 5 4 3 2 1

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

RS485 Bus Schematic

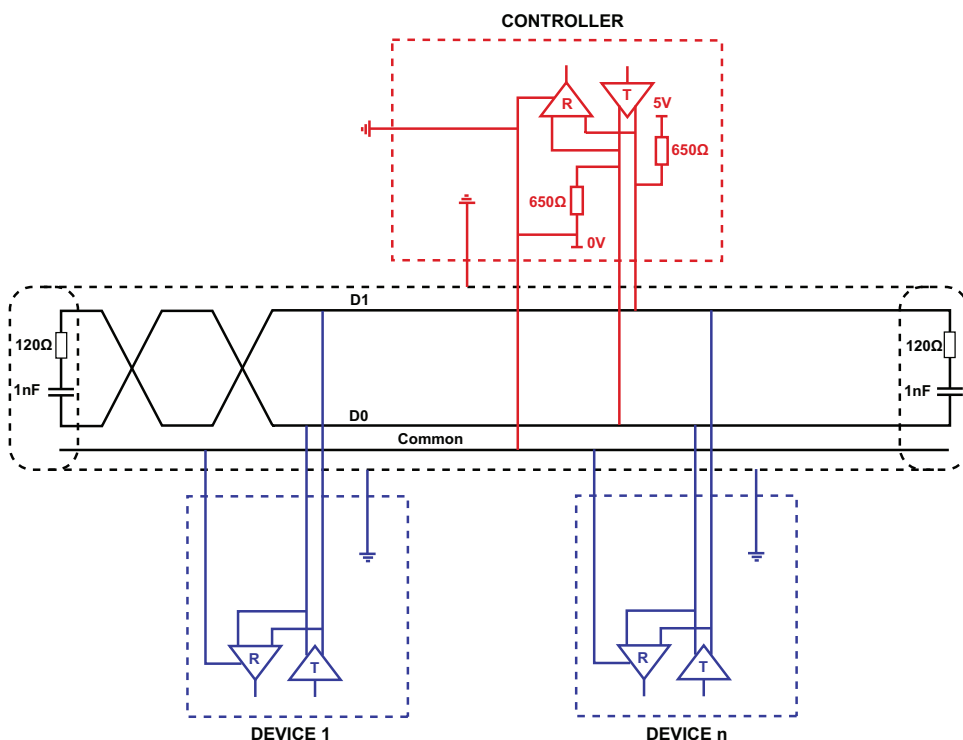
The RS485 standard allows variants of different characteristics:

- 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	<ul style="list-style-type: none"> • 20 m for 1 tape link • 40 m divided by the number of tape links on a multiple junction box
Bus polarization	<ul style="list-style-type: none"> • One 450...650 Ω pull-up resistor at 5 V (650 Ω recommended) • One 450...650 Ω pull-down resistor at the common (650 Ω recommended) 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: <ul style="list-style-type: none"> • 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.

Cybersecurity Generalities

What's in This Part

Overview	21
Security Policy	25
Product Defense-in-Depth.....	26
ATH600 Security Policy	29
Potential Risks and Compensating Controls	32
Data Flow Restriction	33
Device Recovery and Reconstitution.....	34
Upgrades Management	35
Port Hardening.....	36
Security Functionality Verification	37

Overview

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

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

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

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

The basic components of this approach are:

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

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

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

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

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

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

▲ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

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

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

Protected Environment Assumptions

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

▲ WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

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

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

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

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

Control System - Cybersecurity policy

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

Physical perimeter security

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

Physical network segmentation

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

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

Logical isolation of critical networks

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

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

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

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

Information disclosure prevention

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

Control against malware

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

Resource & control system availability

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

Security Policy

⚠ WARNING

ACCESSIBILITY LOSS

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

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

Cybersecurity helps to provide:

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

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

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

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

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

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

⚠ WARNING

CYBERSECURITY HAZARD

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

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

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

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

Product Defense-in-Depth

ATH600 offers the following security features:

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

Confidentiality

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

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

Device Integrity Protection

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

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

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

Availability

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

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

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

Authentication and Authorization

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

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

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

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

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

The ATH600 controls the access through :

- SoMove DTM (Serial and through Option Board connection)

Port Hardening

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

Security Event Logging

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

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

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

ATH600 Security Policy

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

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

Security Policy “Minimum”

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

Security Policy “Advanced”

This policy presets the device security by enabling security features. The user access control is enabled across various software tools and platforms used for system configuration. When activating the "Advanced" security policy, the user is identified as ADMIN and is requested to create a password unique to the device. During the initial setup, the user is invited to define a new password even if a default password is proposed .

If initial setup is done on DTM, there is no use of default password

Refer to the following cybersecurity features summary per security policy:

ATH600 security feature	Open for configuration (activation or settings)	Preset security policy	
		Minimum	Advanced
Password encrypted in a non-reversible way	-	-	✓
User access control	-	-	✓
Cryptographic signature of firmware package	-	✓	✓
Secure root of trust	-	✓	✓
Device backup	ADMIN or SecAdmin only	✓	✓
Device restore	ADMIN or SecAdmin only	✓	✓
Security Save	ADMIN or SecAdmin only	-	✓
Security Restore	ADMIN or SecAdmin only	✓	✓
User management	ADMIN or SecAdmin only	-	✓
Strong password/pin code policy	ADMIN or SecAdmin only	-	✓
Brute force and session timeout	ADMIN or SecAdmin only	-	✓
System use notification	ADMIN or SecAdmin only	-	✓
Access control: <ul style="list-style-type: none"> • Display terminal • Commissioning tools (Modbus Serial and Option Module) 	For all users	✓	✓
Secure events recorded	ADMIN or SecAdmin only	✓	✓
Port hardening	ADMIN or SecAdmin only	-	✓

Import / Export Security Policy

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

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

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

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

Potential Risks and Compensating Controls

Address potential risks using these compensating controls:

Area	Issue	Risk	Compensating controls
User accounts.	Default account settings are often the source of unauthorized access by malicious users.	If you do not change default password or disable the user access control, unauthorized access can occur.	Ensure User access control is enabled on all the communication ports and change the default passwords to help reduce unauthorized access to your device.
Secure protocols.	The device does not have the capability to transmit data encrypted using these protocols: <ul style="list-style-type: none"> • Modbus Serial • BACNet MS/TP • BACNet IP • Modbus TCP 	If a malicious user gained access to your network, they could intercept communication.	For transmitting data over internal network, physically or logically segment your network. For transmitting data over external network (Option module), encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution. See Protected Environment Assumptions , page 23.
Security banners	The local display terminal cannot display the security banner.	The users connecting to the ATH600 will not be able to be warned about potential security notifications.	If such security notification shall be shared with users, then a local message shall be added close to the ATH600. <u>Example:</u> A sticker on the electrical cabinet or the electrical room can inform user about specific security considerations

Data Flow Restriction

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

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

Device Recovery and Reconstitution

Control system backup – available and up-to-date backups for recovery from a control system failure.

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

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

NOTE:

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

Upgrades Management

When the Altivar HVAC ATH600 firmware and option fieldbuses are upgraded, security configuration remains the same until changed, including usernames and passwords.

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

Port Hardening

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

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

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

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

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

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

BACnet IP Services

BACnet IP Services	Settings
Modbus TCP	ON / OFF

Security Functionality Verification

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

Human User Access Control

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

Interface	Step	Action	✓
<ul style="list-style-type: none"> Commissioning tools connected on the Modbus Serial interface Commissioning tools connected on the option module. 	1	Try to connect to the selected interface	
	2	Confirm the security banner is displayed prior authentication is requested	
		Confirm security banner message is in conformity with the message to be displayed for your organization.	
	3	Try to log in to ATH600 with no password or wrong password. Result: access denied.	
	4	Try to login with more than the MaxLoginAttempts (Default value : 5) with wrong password Result: The account is locked during Lock Duration (Default value 240s)	
Confirm the account is locked as well on other interfaces (SoMove (DTM))			
5	During this Lock Duration, connect another account with the right password. Result: access granted.		
Display Terminal access control (if enabled)	1	Try to log in to the Display Terminal with no PIN code or a wrong PIN code Result: access denied.	
	2	Try to log in with more than the MaxLoginAttempts (Default value : 5) with wrong PIN code Result: The account is locked during Lock Duration (Default value : 240s)	
	3	During this Lock Duration, connect another account with the right password. Result: access granted.	

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

Password & PIN code Policy

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

Timeout Session

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

Audit

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

Firmware Update

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

Disabling Communication Ports

Step	Action	✓
1	For each individual port disabled by configuration	
2	Confirm the ports are no longer usable No data flow detected as output and no data accepted as input	
3	For each individual port disabled by configuration, confirm the protocol refuses communication according to the column verification of chapter Port Hardening , page 36	

Software Setup

What's in This Part

[Modbus Fieldbus] MD1	40
Most Common parameters.....	42
Communication Scanner.....	48
Monitoring of Communication Channel.....	52

[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]	0 F F	0	0 F F	R/W	16#1771 = 6001
[1 to 247]	1...2 4 7	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]	4 K B	24	19.2 Kbps	R/W	16#1773 = 6003
[9600 bps]	9 K B	28			
[19200 bps]	1 9 K 2	32			
[38.4 Kbps]	3 8 K 4	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]	<i>B o 1</i>	2	8 data bits, odd parity, 1 stop bit	<i>B E 1</i>	R/W	16#17734 = 6004
[8-E-1]	<i>B E 1</i>	3	8 data bits, even parity, 1 stop bit			
[8-N-1]	<i>B n 1</i>	4	8 data bits, no parity, 1 stop bit			
[8-N-2]	<i>B n 2</i>	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]	<i>0 . 1 ... 3 0 . 0</i>	1...300	10 s	R/W	16#17735 = 6005

Most Common parameters

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

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

Base Monitoring

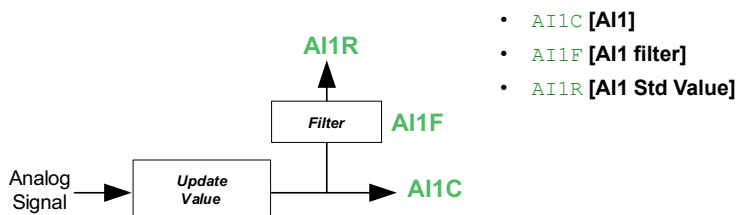
Code	Settings	
[Motor Current] LCR	Logic address: 0C84 hex = 3204	Type: UINT (Unsigned16) Read/write: R
Motor current RMS Motor current. Average of the three line currents based on the measurement of the fundamental of the motor line currents.		
[Motor Therm State] THR	Logic address: 259E hex = 9630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

Digital I/O


Code	Settings	
[Logic Inputs States] IL1R	Logic address: 1452 hex = 5202	Type: WORD (BitString16) Read/write: R Unit: -
<p>Logic inputs states This parameter is used to monitor the real value of the [Logic Inputs States].</p> <ul style="list-style-type: none"> • Bit0 : "DI1" Digital inputs real image • Bit1 : "DI2" Digital inputs real image • Bit2 : "DI3" Digital inputs real image • Bit3 : "DI4" Digital inputs real image • Bit4 : "DI5" Digital inputs real image • Bit5 : "DI6" Digital inputs real image • Bit10: "DI11" Digital inputs real image (with VW3A3203) • Bit11: "DI12" Digital inputs real image (with VW3A3203) • Bit12 : "DI13" Digital inputs real image (with VW3A3203) • Bit13 : "DI14" Digital inputs real image (with VW3A3203) • Bit14 : "DI15" Digital inputs real image (with VW3A3203) • Bit15 : "DI16" Digital inputs real image (with VW3A3203) <p>NOTE: The status of inputs can be read via [Logic Inputs States] IL1R to which a position or level sensor has been wired.</p>		
[Logic Outputs States] OL1R	Logic address: 145C hex = 5212	Type: WORD (BitString16) Read/write: R/W Unit: -
<p>Logic outputs states This parameter is used to write output value or monitor the value depending on if a function is assigned to the corresponding output:</p> <ul style="list-style-type: none"> • Bit0 : "R1" relay real image • Bit1 : "R2" relay real image • Bit2 : "R3" relay real image • Bit3 : "R4" relay real image (with VW3A3204) • Bit4 : "R5" relay real image (with VW3A3204) • Bit5 : "R6" relay real image (with VW3A3204) • Bit12 : "DQ11" Digital outputs real image (with VW3A3203) • Bit13 : "DQ12" Digital outputs real image (with VW3A3203) <p>NOTE: To write an output through communication, no function should be assigned to the corresponding output. Otherwise, writing on the bit linked to the corresponding output has no impact. If an error is triggered, outputs written through communication returns to 0.</p> <p>NOTE: It is only possible to write the output through the active command channel. Consequently, forced outputs can not be disabled on local channel (such as display terminal).</p>		

Analog input

The following diagram explains how the analog input works:



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

Code	Settings	
[AI1] AI1C	Logic address: 147A hex = 5242	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI1 This parameter is used to monitor the real value of the [AI1]. <ul style="list-style-type: none"> • (AI1T == "0A"): 0.001 mA • (AI1T == "10U"): 0.001 V • (AI1T == "LEVEL"): 0.01 kOhm • else : 0.001 V 		
 [AI1 filter] AI1F	Setting range: 0...10 s Factory setting: 0 s Logic address: 1164 hex= 4452	Type: UINT (Signed16) Read/write: R/W Unit: seconds
AI1 filter This parameter sets the cutoff time of the low filter for PTC1/AI1. The low pass filter aims to suppress electrical noise and avoid interference issue in the input signal.		
[AI1 Std Value] AI1R	Logic address: 1470 hex= 5232	Type: INT (Signed16) Read/write: R Unit: -
Analog input 1 standardized value Real image of AI1 consumed by functions.		
[AI2] AI2C	Logic address: 147B hex = 5243	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI2 AI2 customer image (1mV, 0.001mA) <ul style="list-style-type: none"> • (AI2T == "0A"): 0.001 mA • (AI2T == "10U"): 0.001 V • (AI2T == "PTC"): 0.01 kOhm • (AI2T == "KTY"): 1 Ohm • (AI2T == "1PT3"): 1 Ohm • (AI2T == "1PT2"): 0.1 Ohm • (AI2T == "LEVEL"): 0.01 kOhm • else : 0.001 V 		

Code	Settings	
[AI2 Std Value] AI2R	Logic address: 1471 hex = 5233	Type: INT (Signed16) Read/write: R Unit: -
Analog input 2 standardized value AI2 real application image		
[AI3] AI3C	Logic address: 147C hex = 5244	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI3 AI3 customer image (1mV, 0.001mA) <ul style="list-style-type: none"> • (AI3T == "0A") : 0.001 mA • (AI3T == "10U") : 0.001 V • (AI3T == "PTC") : 0.01 kOhm • (AI3T == "KTY") : 1 Ohm • (AI3T == "1PT3") : 1 Ohm • (AI3T == "1PT2") : 0.1 Ohm • (AI3T == "LEVEL") : 0.01 kOhm • else : 0.001 V 		
[AI3 Std Value] AI3R	Logic address: 1472 hex = 5234	Type: INT (Signed16) Read/write: R Unit: -
Analog input 3 standardized value AI3 real application image		
[AI4] AI4C	Logic address: 147D hex = 5245	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI4 AI4 customer image (1mV, 0.001mA) <ul style="list-style-type: none"> • (AI3T == "0A") : 0.001 mA • (AI3T == "10U") : 0.001 V • (AI3T == "PTC") : 0.01 kOhm • (AI3T == "KTY") : 1 Ohm • (AI3T == "1PT3") : 1 Ohm • (AI3T == "1PT2") : 0.1 Ohm • (AI3T == "LEVEL") : 0.01 kOhm • else : 0.001 V 		
[AI4 Std Value] AI4R	Logic address: 1473 hex = 5235	Type: INT (Signed16) Read/write: R Unit: -
Analog input 4 standardized value AI4 real application image		

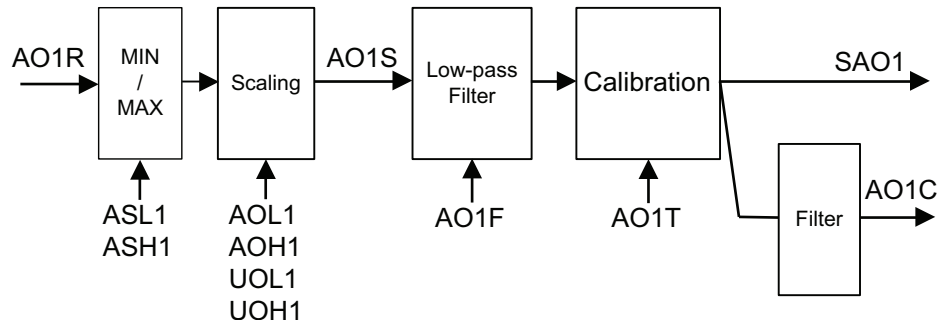
Analog outputs

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

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

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

The following diagram explains how the analog output works:



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

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

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

Communication Scanner

Local Configuration of the Communication Scanner

The communication scanner is useful when used in combination by the 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 communication scanner **[Com. scanner input]** and **[Com. scanner output]** are accessible via the following menus: **[Communication] COM-** → **[Comm parameters] CMP** → **[Bacnet MS/TP] EBM-** and **[BACnet IP Config] BAIP-**.

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

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

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

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

Fast Task of the Communication Scanner

Only the following parameters are available for the fast tasks:

Fast read	Parameters
n P A 1...n P A 4	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
n C A 1...n C A 4	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.] n C 1** to **[Com Scan Out8 val.] n C 8** and **[Com Scan In1 val.] n P 1** to **[Com Scan In8 val.] n P 8**.

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

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

Monitoring of Communication Channel

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

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

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

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

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

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

Enabling of Communication Channels

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

Example:

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

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

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

On exiting *forced local* mode:

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

Command and Reference Channels

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

Parameter Name	Parameter Code			
	Taken Into Account by the Drive	Modbus Serial	Fieldbus Module	BACnet MSTP
<i>Control word</i>	CMD	CMD1	CMD3	CMD9
<i>Extended control word</i>	CMI	CMI1	CMI3	CMI9
<i>Reference speed (rpm)</i>	LFRD	LFRD1	LFRD3	LFRD9
<i>Reference frequency (0.1 Hz)</i>	LFR	LFR1	LFR3	LFR9
<i>Reference value supplied by PI controller</i>	PISP	PISP1	PISP3	PISP9
<i>Reference value supplied by analog multiplier function</i>	MFR	MFR1	MFR3	MFR9
(1): If available				

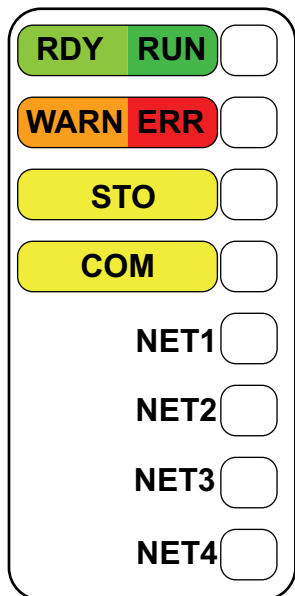
Diagnostics and Troubleshooting

What's in This Part

Fieldbus Status LEDs	55
Configuring Communication Error Response	57
Communication troubleshooting	59
Warning Codes	60
Communication error codes	61

Fieldbus Status LEDs

LED Description



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

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

Communication Diagnostics

These parameters are visible only with the graphic display terminal.

On the terminal, in the **[Display] MON** menu (**[Communication map] CMM** submenu,

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

RUN	MDB	+50.00Hz	80A
MODBUS NETWORK DIAG <input type="checkbox"/>			
COM LED	:		⊗
Mb net frames nb.	:		568
Mb net crc errors	:		0
Code		Quick	<input type="checkbox"/>

⊗ Indicates a LED, which is not lit.

Modbus Counters

- **[Mdb Frame Nb] M1CT** indicate the number of Modbus frames received. The counter counts both correct and incorrect frames.
- **[Mdb CRC errors] M1EC** 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]** *ADD* parameter are counted. Broadcast frames are not counted.

[Mdb Frame Nb] *M1CT* 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]** *M1EC* 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] <i>MND</i>	[Mdb Frame Nb]	<i>M1CT</i>	6011
	[Mdb CRC errors]	<i>M1EC</i>	6010

Modbus Communication State

This can be accessed from the menu:

[Configuration] *CONF* / **[Full]** *FULL* / **[Communication]** *COM* / **[Modbus Fieldbus]** *MD1* / **[Modbus stat]** *COM1*

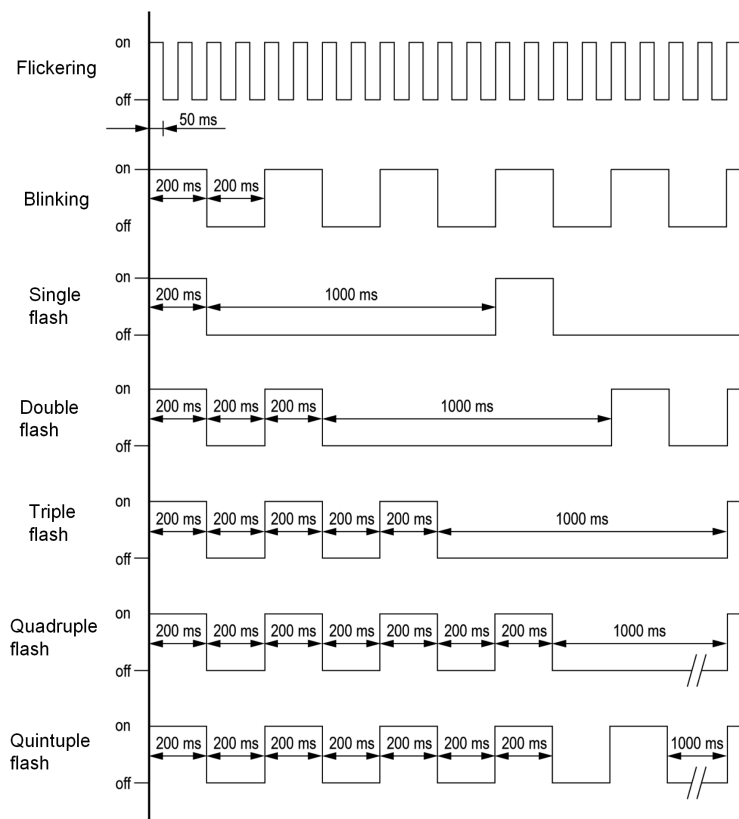
[R0T0] *R0T0*: Modbus no reception, no transmission = communication idle

[R0T1] *R0T1*: Modbus no reception, transmission

[R1T0] *R1T0*: Modbus reception, no transmission

[R1T1] *R1T1*: Modbus reception and transmission

LED Behavior



Configuring Communication Error Response

⚠ WARNING
<p>LOSS OF CONTROL</p> <p>Perform a comprehensive commissioning test to verify that communication monitoring properly detects communication interruptions.</p> <p>Failure to follow these instructions can result in death, serious injury, or equipment damage.</p>

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]** **SLL** 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
<p>LOSS OF CONTROL</p> <p>If this parameter is set to [Ignore], Modbus communication monitoring is disabled.</p> <ul style="list-style-type: none"> • 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. <p>Failure to follow these instructions can result in death, serious injury, or equipment damage.</p>

▲ WARNING

LOSS OF CONTROL

If this parameter is set to **[Fallback Speed]** *LEF* 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]**).

Warning Codes

List of Available Warnings Messages

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

Communication error codes




What's in This Chapter

[Incorrect Config] CFF	62
[Invalid Config] CFI	62
[Conf Transfer Error] CFI2	62
[Channel Switch Error] CSF	63
[Mdb Com Interrupt] SLF1	63

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

 Probable Cause	<p>At power on, the device proceeds to a self-test and checks its configuration. If the configuration is not correct, the error [Incorrect Config] CFF is triggered.</p> <ul style="list-style-type: none"> Option module changed or removed.
 Remedy	<ul style="list-style-type: none"> Verify that all option modules are inserted correctly into the option module slot. Verify that there is no detected error on the option module. Return to factory settings or retrieve the backup configuration if it is valid.
 Clearing the Error Code	<p>This detected error is cleared as soon as its cause has been removed.</p>




[Invalid Config] CFI

Invalid configuration

 Probable Cause	<p>Invalid configuration. The configuration loaded in the device via the commissioning tool or fieldbus is inconsistent.</p> <ul style="list-style-type: none"> Invalid parameter value. BACnet IP option module is plugged and [Control Mode] CHCF is set to [I/O profile] IO.
 Remedy	<ul style="list-style-type: none"> Verify the loaded configuration. Load a valid configuration.
 Clearing the Error Code	<p>This detected error is cleared as soon as its cause has been removed.</p>




[Conf Transfer Error] CFI2

Configuration transfer error

 Probable Cause	<ul style="list-style-type: none"> The configuration transfer to the device was not successful or interrupted. The configuration loaded is not compatible with the device.
 Remedy	<ul style="list-style-type: none"> Verify the configuration loaded previously. Load a compatible configuration. Use PC software commissioning tool to transfer a compatible configuration. Perform a factory setting.
 Clearing the Error Code	<p>This detected error is cleared as soon as its cause has been removed.</p>




[Channel Switch Error] CSF

Channel switching detected error

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

[Mdb Com Interrupt] SLF1

Modbus communication interruption

	Probable Cause	Communication interruption on the Modbus port if the command and/or reference value is given by Modbus.
	Remedy	<ul style="list-style-type: none"> • Verify the Modbus communication wiring. • Verify the Modbus communication parameter settings. • Verify the timeout. • Refer to the Modbus user manual.
	Clearing the Error Code	This detected error can be cleared with the [Auto Fault Reset] <i>ATR</i> or manually with the [Fault Reset Assign] <i>RSE</i> parameter after its cause has been removed. This also possible to reset with the command word 0080 hex (<i>Fault reset</i>).

Annex

What's in This Part

Operation	65
Starting Sequence.....	80
Operating Modes	88
Modbus Functions	91

Operation

What's in This Chapter

Profile.....	66
Functional Profiles Supported by the Drive	67
Functional Description	68
CIA402 Operating State Diagram	69
Description of Operating States	70
Device Status Summary	71
Command Register <small>CMD</small>	72
Stop Commands	73
Assigning Control Word Bits.....	73
[CIA402 State Reg] <small>ETA</small>	74
I/O Profile	75
Extended Control Word.....	78
Internal State register	79

Profile

There are 3 types of profile:

- Communication profiles
- Functional profiles
- Application profiles

Communication Profile

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

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

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

Functional Profile

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

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

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

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

- CiA402

Application Profile

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

Interchangeability

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

Functional Profiles Supported by the Drive

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.**] `SEP,`

Functional Description

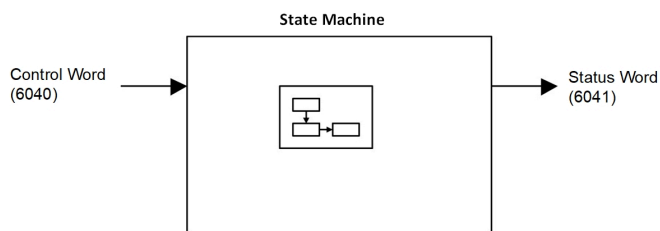
Introduction

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

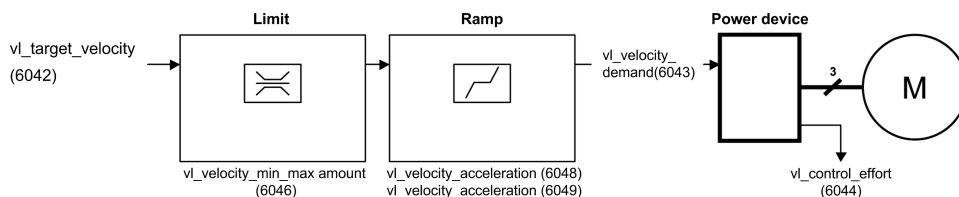
CiA402

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

The following figure shows the control diagram for drive operation:



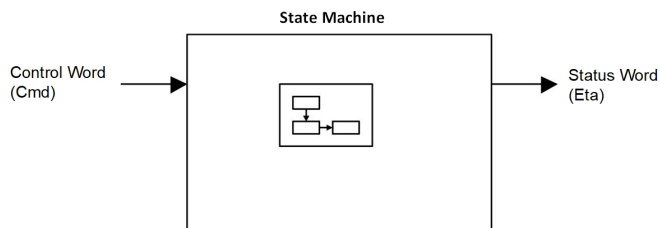
Simplified diagram for speed control in *Velocity* mode:



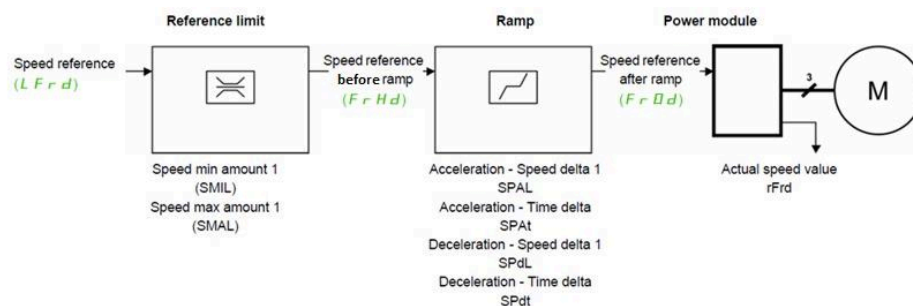
Altivar HVAC Drive

These diagrams translate as follows for the Altivar HVAC drive.

The following figure shows the control diagram for drive operation:



Simplified diagram for speed control in *Velocity* mode:

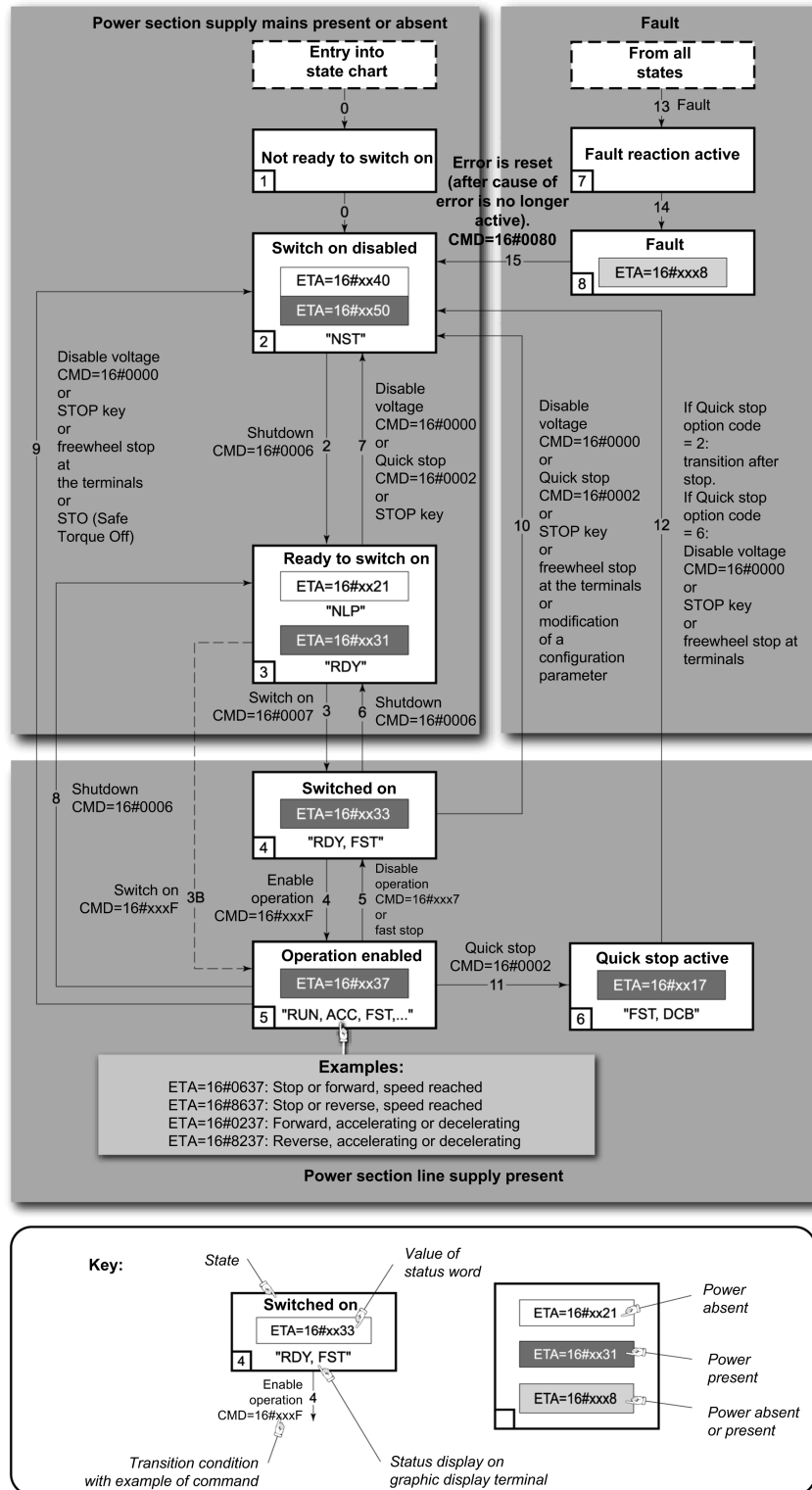


CIA402 Operating State Diagram

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

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

The following figure shows the CIA402 state diagram:



Description of Operating States

Each state represents an internal reaction by the drive.

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

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

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

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

Device Status Summary

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

NOTE:

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

Command Register CMD

Bit Mapping of the Control Word

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

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Manufacturer specific assignable	Manufacturer specific assignable	Manufacturer specific assignable	Manufacturer specific assignable	Manufacturer specific assignable	Reserved (=0)	Reserved (=0)	Halt
				0 = Forward direction asked 1 = Reverse direction asked			0 = run asked 1 = stop asked

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

X: Value is of no significance for this command.

0→1: Command on rising edge.

Stop Commands

Halt Command

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

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

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

Fast Stop Command

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

Freewheel Command

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

Assigning Control Word Bits

Function Codes

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

Bit	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]** `113` value.

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

[CIA402 State Reg] ETA**Bit Mapping of the Status Word**

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

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

Operating State	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	ETA Masked by 006F H ⁽¹⁾
	Switch On Disabled	Quick Stop	Voltage Enabled	Fault	Operation Enabled	Switched On	Ready to Switch On	
1 -Not ready to switch on	0	X	X	0	0	0	0	-
2 -Switch on disabled	1	X	X	0	0	0	0	0040 hex
3 -Ready to switch on	0	1	X	0	0	0	1	0021 hex
4 -Switched on	0	1	1	0	0	1	1	0023 hex
5 -Operation enabled	0	1	1	0	1	1	1	0027 hex
6 -Quick stop active	0	0	1	0	1	1	1	0007 hex
7 -Fault reaction active	0	X	X	1	1	1	1	002F hex
8 -Fault	0	X	X	1	0	0	0	0008 hex ⁽²⁾ ... 0028 hex

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

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

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

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]** **HMISS**.

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]**).

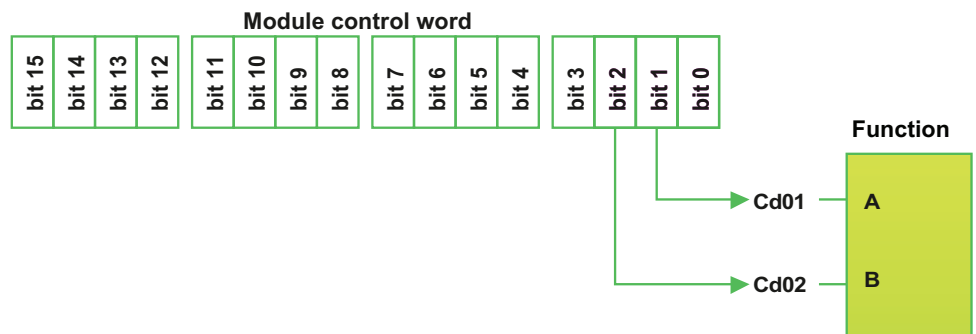
Bit	Fixed assignments		
	Virtual Inputs	Terminals	Modbus
bit 0	Cd00	DI1	C100
bit 1	Cd01	DI2	C101
bit 2	Cd02	DI3	C102
bit 3	Cd03	DI4	C103
bit 4	Cd04	DI5	C104
bit 5	Cd05	DI6	C105
bit 6	Cd06	-	C106
bit 7	Cd07	-	C107

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

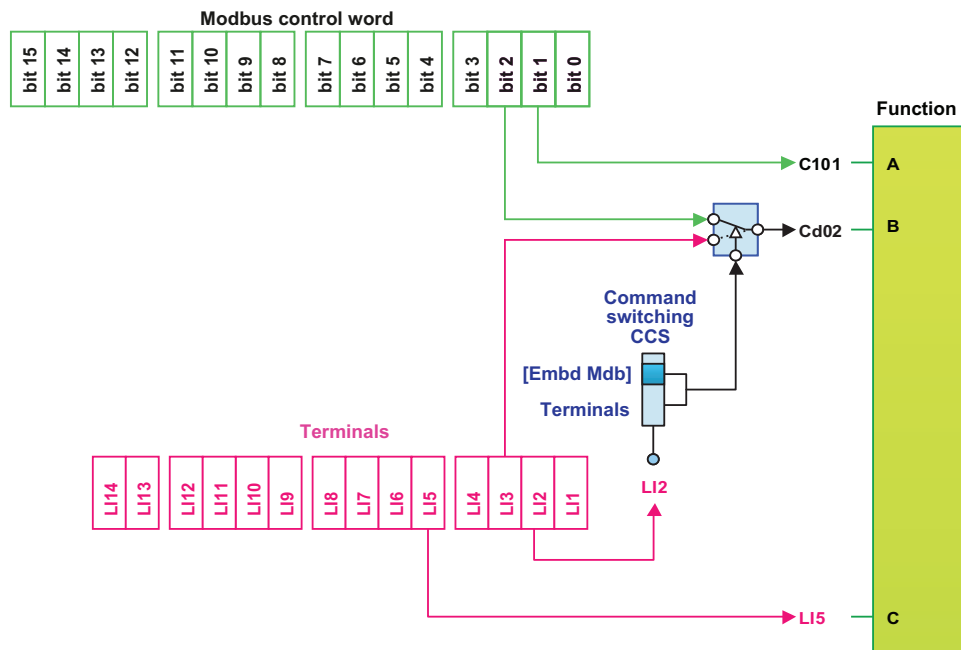
UNANTICIPATED EQUIPMENT OPERATION

- 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.

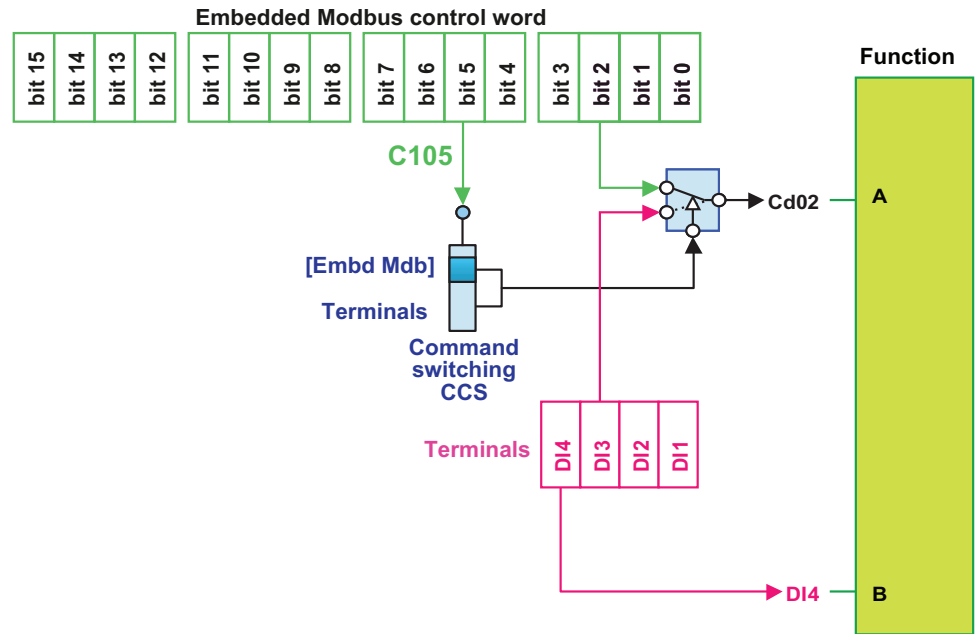
Example with:

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

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

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

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

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

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

	Bit 8	Bit 9	Bit 10	Bit 11	Bit 12	Bit 13	Bit 14	Bit 15
Function	Reserved	Frequency reference (FRH, LFR, RFR ...)	Reserved			Drive locked in STOP	Serial link error inhibition	Parameter coherence deactivated and drive locked in STOP
Bit at 0		in 0.1Hz				Deactivate.	Deactivate.	Deactivate.
Bit at 1		in internal unity (32767 = TFR)				Activate.	Activate.	Activate.

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: <ul style="list-style-type: none"> is not in operating state "Error" is in operating state "Error" and the error is active. 	
Bit at 1	Access to the non-volatile memory in progress.	Active.	The device is in operating state "Error" and the error is no longer active (not reset).	

	Bit 4	Bit 5	Bit 6	Bit 7
Function	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.	<ul style="list-style-type: none"> Bit 13 = 0 + Bit 14 = 0: Device controlled by terminal Bit 13 = 1 + Bit 14 = 0: Device controlled by the display terminal Bit 13 = 0 + Bit 14 = 1: Device controlled by Embedded Modbus Bit 13 = 1 + Bit 14 = 1: Device controlled by fieldbus card 		Forward operation applied before the ramp.
Bit at 1	Active.			Reverse operation applied before the ramp.

Starting Sequence

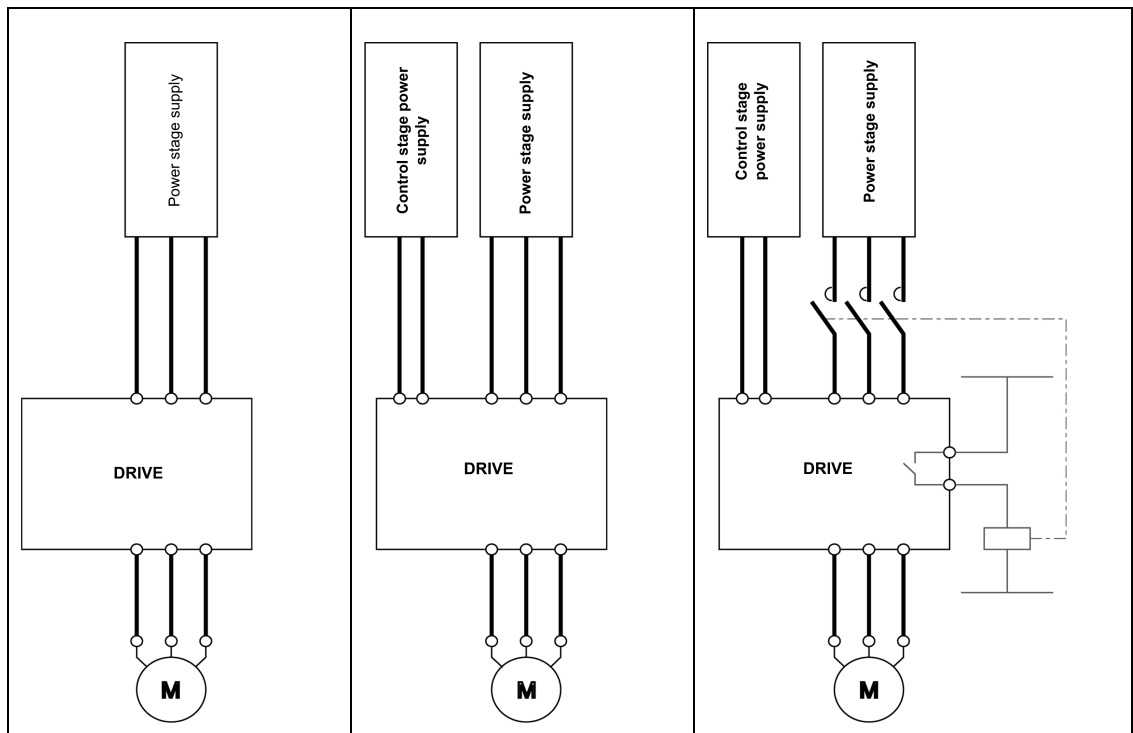
What's in This Chapter

Starting Sequence for a Drive Powered by the Power Stage Supply 81
 Starting Sequence for a Drive with Separate Control Stage 83
 Starting Sequence for a Drive with Mains Contactor Control 86

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

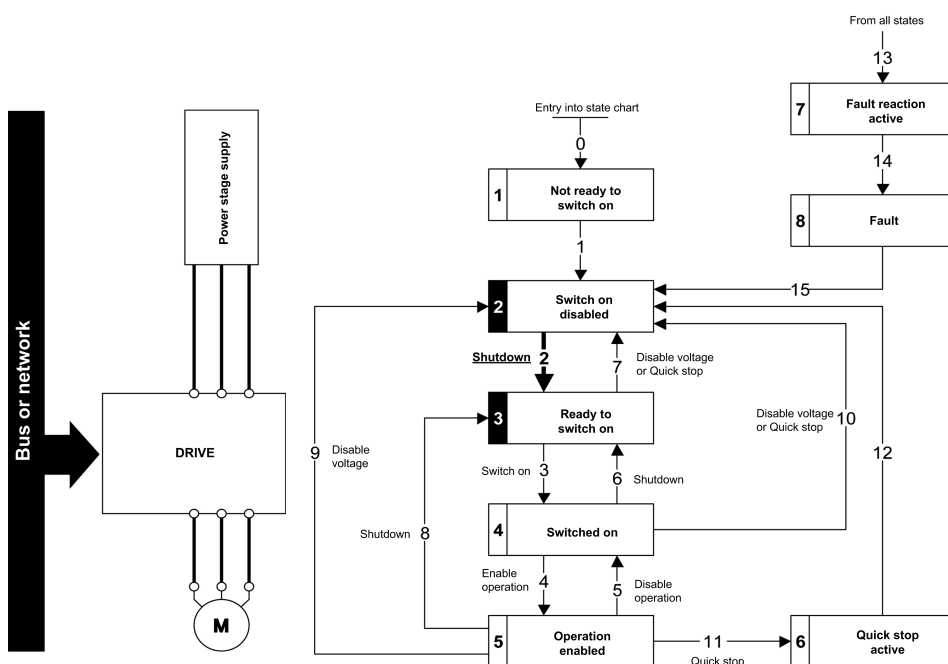
Both the power and control stages are powered by the power stage supply.

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:

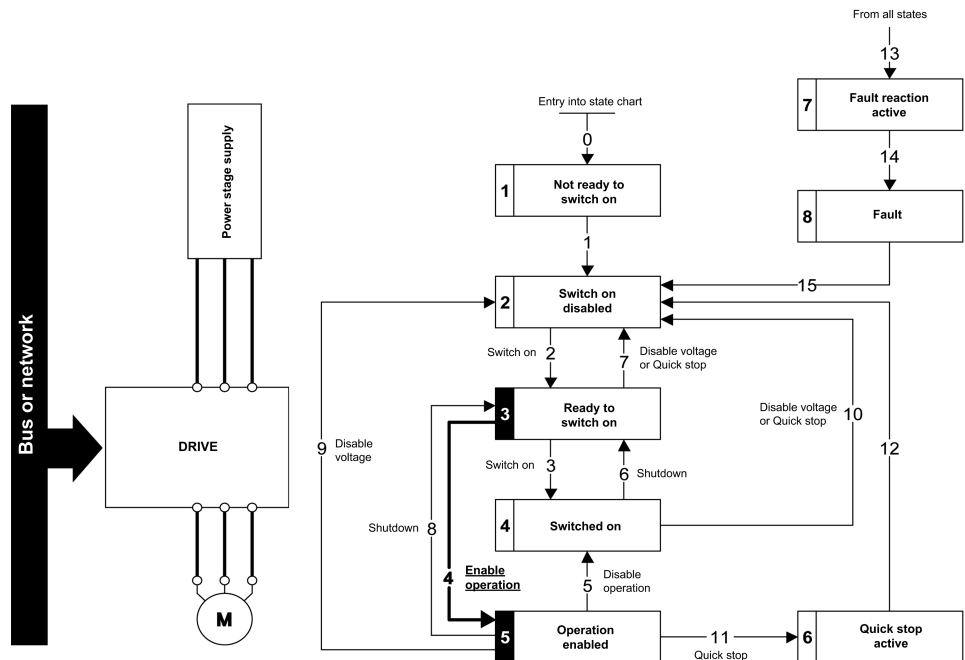
Step 1

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

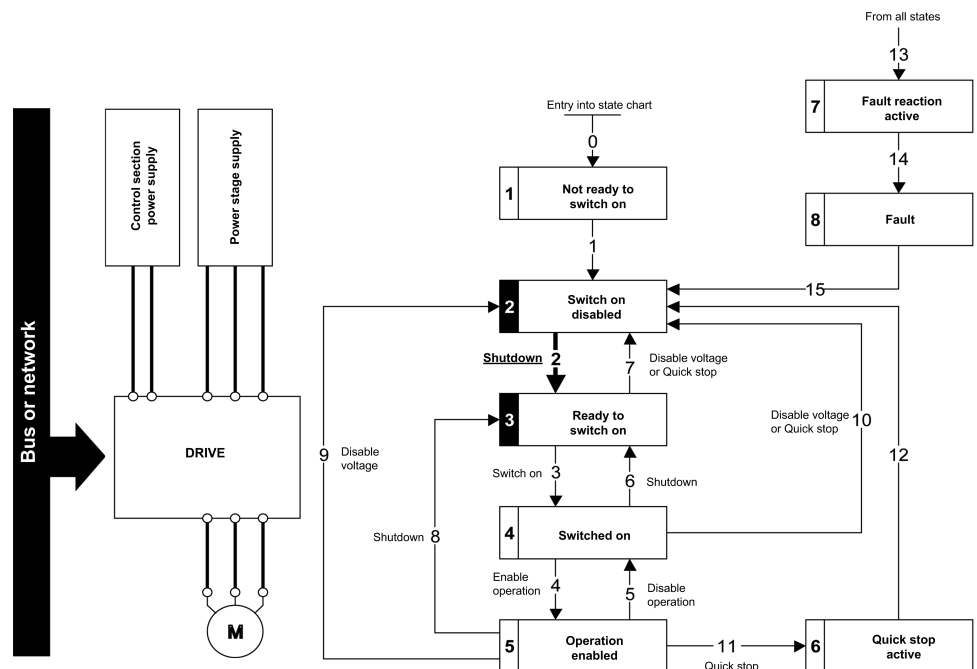
Power is supplied separately to the power and control stages.

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

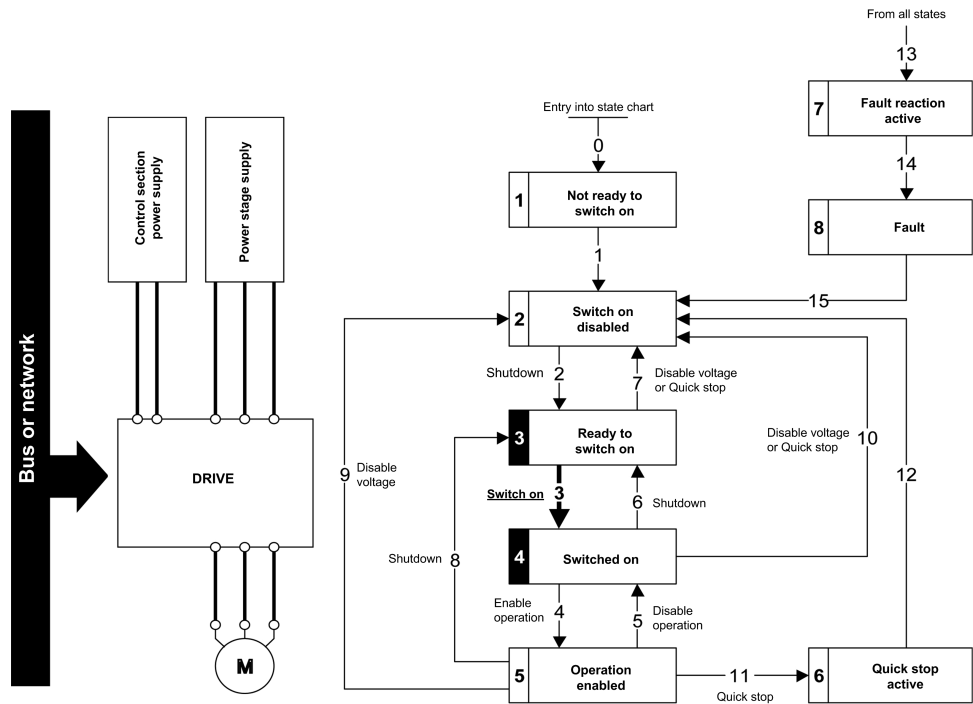


Step 2

- 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).

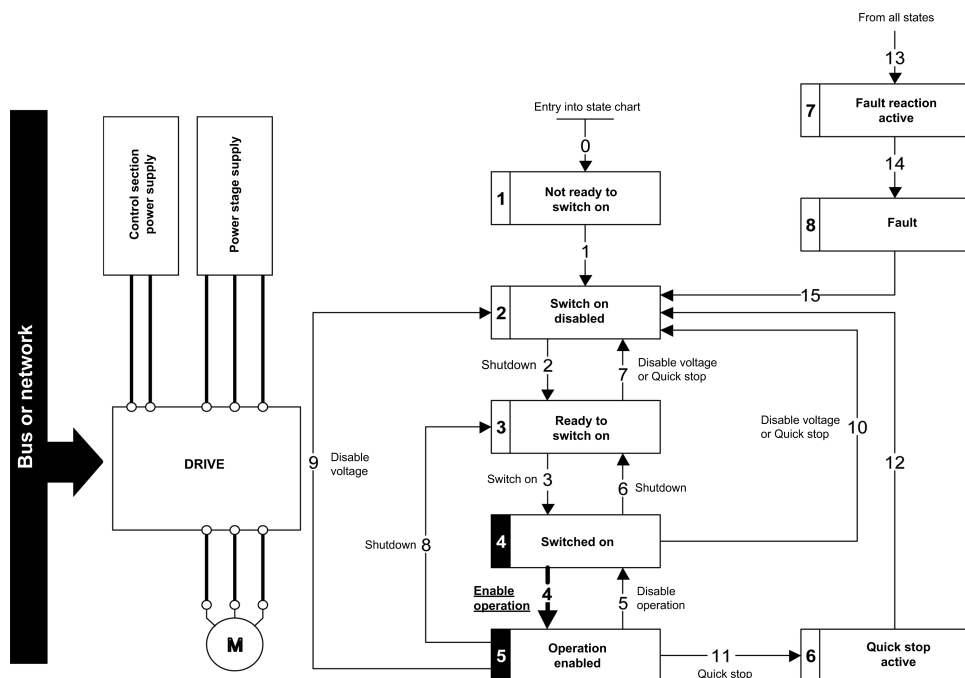
Power Stage Supply	HMI Panel	Status Word
Not present	[No Mains Voltage] <i>NLP</i>	21 hex
Present	[Ready] <i>RDY</i>	31 hex

- 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

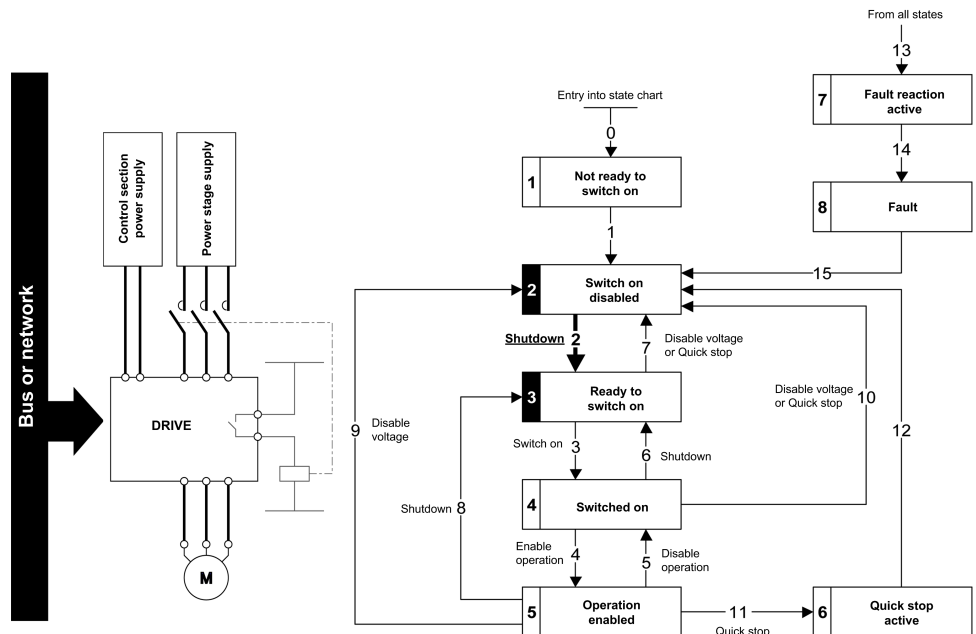
Power is supplied separately to the power and control stages.

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:

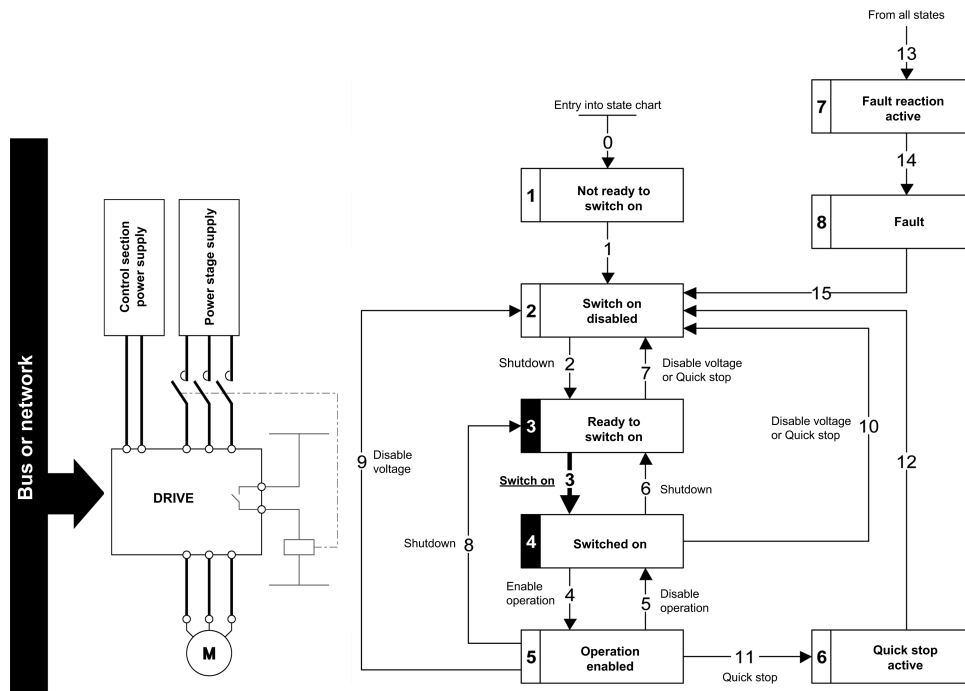
Step 1

- 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.....	89
Configuration of the Drive for Operation in I/O Profile	89
Configuration of the Drive for Operation with CiA 402 Profile in Combined Mode.....	90
Configuration of the Drive for Operation with CiA 402 Profile in Separate Mode.....	90

Configuring the Control Channel

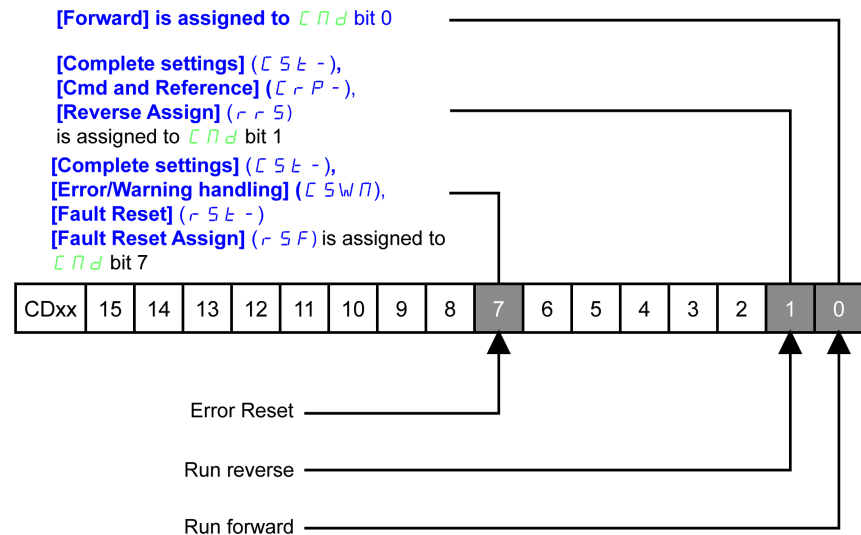
This chapter explains how to configure the drive for operation from the communication network through three following examples.

- 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 reference frequency is given by Graphic Display Terminal.



The settings are the following:

[Ref Freq 1 Config] FR1	[HMI] LCC
[Reverse Disable] RIN	Default
[Stop Key Enable] PST	Default
[Control Mode] CHCF	[Separate] SEP
[Command Switching] CCS	Default
[Cmd channel 1] CD1	[Modbus] Mod

The bits of the command word can now be configured.

In [Cmd and Reference] **CRP-**, configure:

[Reverse Assign] RRS	[CD01] CD01
-----------------------------	--------------------

In [Error/Warn handling] **CSWM-** → [Fault reset] **RST-**, configure:

[Fault Reset Assign] RSEF	[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 **[Complete settings] CST-** menu → **[Cmd and Reference] CRP-** submenu :

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

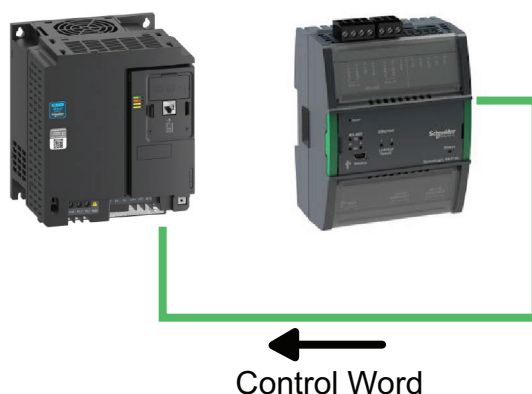
For the current example, **[Control Mode] CHCF** is adjusted to **[Not separ.] SIM** as reference and control are originated from the communication network.

Profile	Ref1 Channel setting
CiA 402 combined mode	[Not separ.] SIM
CiA 402 separate mode	[Separate] SEP
I/O profile	[I/O profile] IO

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

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

For example:



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

The settings are as shown in the table:

[Ref Freq 1 Config] FR1	[HMI] LCC
[Reverse Disable] RIN	Default
[Stop Key Enable] PST	Default
[Control Mode] CHCF	[Separate] SEP
[Command Switching] CCS	Default
[Cmd channel 1] CD1	[Modbus] MDB

Modbus Functions

What's in This Chapter

Modbus Protocol	92
Supported Modbus Functions.....	93

Modbus Protocol

Introduction

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

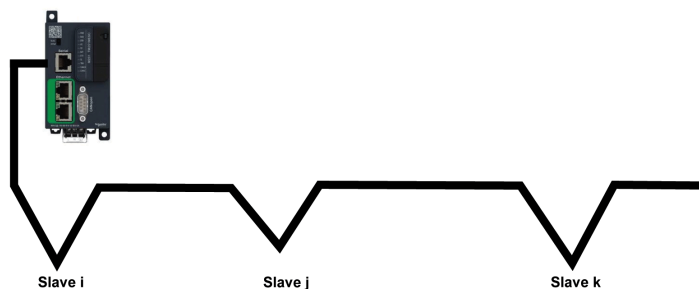
Device address	Request code	Data	CRC16
----------------	--------------	------	-------

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

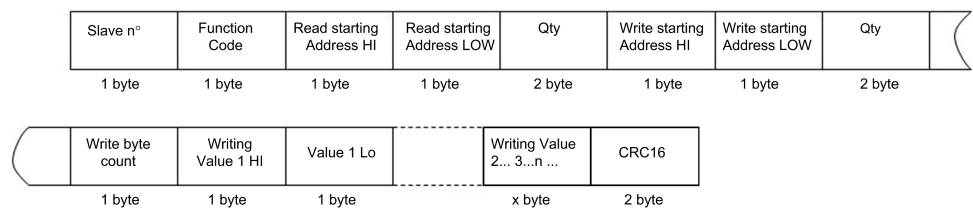
This function code performs a combination of one read operation and one write operation in a single MODBUS transaction. The write operation is performed before the read. Holding registers are addressed starting at zero. Therefore holding registers 1-16 are addressed in the PDU as 0-15.

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

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

Id of object number 2	Length of object number 2	Value of object number 2
01	0B	ATH630xxxxxx
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, **ATH630xxxxxx**, 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 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
1884 Boulevard de la Défense
92000 Nanterre
France

www.se.com

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

© 2026 Schneider Electric. All rights reserved.

JPS89286.01