

Altivar Process ATV600

Variable Speed Drives

PROFINET Manual - VW3A3647

BQT46619.01
12/2023



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
Qualification of Personnel	6
Intended Use.....	6
Product Related Information	7
About the Book.....	10
At a Glance	10
Validity Note	10
Document Scope	10
Related Documents	11
Terminology.....	12
Contact us.....	13
Cyber Security	14
Overview	14
Password.....	20
Upgrades Management.....	21
Basics	22
Introduction.....	22
Common Additional Features	23
Identification and Maintenance Data.....	23
I&M Record	23
Drive Parameters Channel	25
Acyclic drive parameters access	25
Drive profile request structure	25
Drive Parameters Access	27
Presentation.....	29
Hardware Setup	29
Hardware Presentation.....	29
Firmware Version.....	29
Installation of the fieldbus module	29
Electrical Installation	31
Cable Routing Practices	32
Software Setup.....	35
Software Overview.....	35
Basic Settings.....	36
IP Parameter Settings	38
[User authentication] SECP- menu	40
iPar Service.....	42
S2 Redundancy	47
Communication Profile	48
Operations	70
Operating States	70
Configuring Communication Error Response	70
Operating Modes.....	71
Configuring the Control Channel	71
Configuration of the Drive for Operation in I/O Profile	72
Configuration of the Drive for Operation with CiA 402 Profile in Combined Mode	73

Configuration of the Drive for Operation with CiA 402 Profile in Separate Mode	74
Diagnostics and Troubleshooting	75
Fieldbus Status LEDs	75
Connection problem with the fieldbus module	77
Fieldbus Response Test	77
Communication Interruption	78
[Fieldbus Com Interrupt] Error F	79
[Internal Error 6] Error F6	80
Diagnostic (PROFINET Service)	81
Monitoring of Communication Channel	82
Control-Signal Diagnostics	84
Glossary	86

Safety Information

Important Information

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



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



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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

Please Note

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

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

Qualification of Personnel

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

Intended Use

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

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

Product Related Information

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

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 drive 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 drive 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.

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

Before performing work on the drive system:

- Disconnect all power, including external control power that may be present. Take into account that the circuit breaker or main switch does not de-energize all circuits.
- Place a “Do Not Turn On” label on all power switches related to the drive system.
- Lock all power switches in the open position.
- Wait 15 minutes to allow the DC bus capacitors to discharge.
- Verify the absence of voltage. (1)

Before applying voltage to the drive system:

- Verify that the work has been completed and that the entire installation cannot cause hazards.
- If the mains input terminals and the motor output terminals have been grounded and short-circuited, remove the ground and the short circuits on the mains input terminals and the motor output terminals.
- Verify proper grounding of all equipment.
- Verify that all protective equipment such as covers, doors, grids is installed and/or closed.

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

(1) Refer to Verifying the Absence of Voltage in the [Installation manual of the product](#).

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.

This equipment has been designed to operate outside of any hazardous location. Only install this equipment in zones known to be free of a hazardous atmosphere.

⚠ DANGER**POTENTIAL FOR EXPLOSION**

Install and use this equipment in non-hazardous locations only.

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

Your application consists of a whole range of different interrelated mechanical, electrical, and electronic components, the drive being just one part of the application. The drive 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/manufacture 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 drive 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 cyber security 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 cyber security (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 cyber security 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](https://www.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.

About the Book

At a Glance

Validity Note

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

NOTE: The products listed in the document are not all available at the time of publication of this document online. The data, illustrations and product specifications listed in the guide will be completed and updated as the product availabilities evolve. Updates to the guide will be available for download once products are released on the market.

This documentation is valid for the Altivar Process (ATV630, ATV650, ATV660, ATV680, ATV6A0, ATV6B0, ATV6L0). drives.

Step	Action
1	Go to the Schneider Electric home page www.se.com .
2	In the Search box type the reference of the product or the name of a product range. <ul style="list-style-type: none">• Do not include blank spaces in the reference or product range.• To get information on grouping similar modules, use asterisks (*).
3	If you entered a reference, go to the Product Datasheets search results and click on the reference that interests you. If you entered the name of a product range, go to the Product Ranges search results and click on the product range that interests you.
4	If more than one reference appears in the Products search results, click on the reference that interests you.
5	Depending on the size of your screen, you may need to scroll down to see the data sheet.
6	To save or print a data sheet as a .pdf file, click Download XXX product datasheet .

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.

Document Scope

The purpose of this document is to:

- Show you how to install the PROFINET fieldbus on your drive.
- Show you how to configure the drive to use PROFINET fieldbus.


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

Related Documents

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

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

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

Title of Documentation	Catalog number
Catalog: Altivar Process ATV600 variable speed drives	DIA2ED2140502EN (English) DIA2ED2140502FR (French)
ATV600 Getting Started	EAV63253 (English) EAV63254 (French) EAV63255 (German) EAV63256 (Spanish) EAV63257 (Italian) EAV64298 (Chinese) EAV63253PT (Portuguese) EAV63253TR (Turkish)
ATV600 Getting Started Annex (SCCR)	EAV64300 (English)
Video: Getting Started with Altivar Process ATV600	FA364431 FAQ (English) 
ATV630, ATV650 Installation Manual	EAV64301 (English) EAV64302 (French) EAV64306 (German) EAV64307 (Spanish) EAV64310 (Italian) EAV64317 (Chinese) EAV64301PT (Portuguese) EAV64301TR (Turkish)
ATV600 Programming Manual	EAV64318 (English) EAV64320 (French) EAV64321 (German) EAV64322 (Spanish) EAV64323 (Italian) EAV64324 (Chinese) EAV64318PT (Portuguese) EAV64318TR (Turkish)
ATV600 Modbus Serial Link Manual (Embedded)	EAV64325 (English)
ATV600 Ethernet Manual (Embedded)	EAV64327 (English)
ATV600 Ethernet IP - Modbus TCP Manual (VW3A3720, 721)	EAV64328 (English)
ATV600 BACnet MS/TP Manual (VW3A3725)	QGH66984 (English)
ATV600 PROFIBUS DP manual (VW3A3607)	EAV64329 (English)
ATV600 DeviceNet manual (VW3A3609)	EAV64330 (English)
ATV600 PROFINET manual (VW3A3627)	EAV64331 (English)
ATV600 CANopen Manual (VW3A3608, 618, 628)	EAV64333 (English)
ATV600 POWERLINK manual (VW3A3619)	PHA99690 (English)
ATV600 Communication Parameters	EAV64332 (English)
ATV600 Embedded Safety Function manual	EAV64334 (English)

Title of Documentation	Catalog number
ATV660 Handbook	NHA37111 (English) NHA37110 (German)
ATV680 Handbook	NHA37113 (English) NHA37112 (German)
Application Note: ATV600 Multi-Drives Booster Control Optimized	QGH36060 (English)
Application Note: ATV600 Multi- Masters Booster Control Pressure Feedback with Service Continuity	QGH36061 (English)
Application Note: ATV600 Multi-Drives Standard Level Control	QGH36059 (English)
Application Note: ATV600 Multi- Masters with Optimized Level Control	EAV64367 (English)
ATV600F, ATV900F Installation Instruction sheet	NVE57369 (English)
ATV600, ATV900 ATEX manual	NVE42416 (English)
ATV61-71 to ATV600-900 Migration Manual	EAV64336 (English)
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)
ATV600: DTM	ATV6xx_DTM_Library_EN (English - to be installed first) ATV6xx_DTM_Lang_FR (French) ATV6xx_DTM_Lang_DE (German) ATV6xx_DTM_Lang_SP (Spanish) ATV6xx_DTM_Lang_IT (Italian) ATV6xx_DTM_Lang_CN (Chinese)
Recommended Cybersecurity Best Practices	CS-Best-Practices-2019-340 (English)
EcoStruxure Automation Device Maintenance	EcoStruxure Automation Device Maintenance (English)

You can download these technical publications and other technical information from our website at www.se.com/ww/en/download.

Terminology

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

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.

Among others, these standards include:

- IEC 61800 series: Adjustable speed electrical power drive systems
- IEC 61508 Ed.2 series: Functional safety of electrical/electronic/programmable electronic safety-related
- EN 954-1 Safety of machinery - safety-related parts of control systems
- ISO 13849-1 & 2 Safety of machinery - safety related parts of control systems
- IEC 61158 series: Industrial communication networks - Fieldbus specifications
- IEC 61784 series: Industrial communication networks - Profiles
- IEC 60204-1: Safety of machinery - Electrical equipment of machines – Part 1: General requirements
- IEC 62443: Security for industrial automation and control systems

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 Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

Cyber Security

Overview

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. See Device Security
- Capabilities sub-chapter for details
- Review assumptions about protected environments. See Protected
- Environment Assumptions sub-chapter for details
- Address potential risks and mitigation strategies. See Product Defense-in-Depth sub-chapter for details
- Follow recommendations to optimize cybersecurity

For detailed information on the system defense-in-depth approach, refer to the TVDA: How Can I Reduce Vulnerability to Cyber Attacks in the Control Room (STN V2) 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 cyber security 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 cyber security (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 cyber security 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](#).

Before considering cybersecurity practices on the device, please pay attention to following points:

- Cybersecurity governance – available and up-to-date guidance on governing the use of information and technology assets in your company.
- Perimeter security – installed devices, and devices that are not in service, are in an access-controlled or monitored location.

- Emergency power – the control system provides the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.
- Firmware upgrades – the ATV600 upgrades are implemented consistently to the current version of firmware available on request from Schneider Electric Customer Care Center.
- Controls against malware – detection, prevention, and recovery controls to help protect against malware are implemented and combined with appropriate user awareness.
- Physical network segmentation – the control system provides the capability to:
 - Physically segment control system networks from non-control system networks.
 - 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.
- 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.
- Encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.
- 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. If a remote site connection is needed, for example, encrypt protocol transmissions.
- Resource availability and redundancy – ability to break the connections between different network segments or use duplicate devices in response to an incident.
- 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.
- Control system backup – available and up-to-date backups for recovery from a control system failure

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)

For an efficient security, 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.

The anti-intrusion and anti-physical access to any sensitive installation should be set up.

All the security rules implemented in the ATV600 are in complement of the points above.

The device does not have the capability to transmit data encrypted using the . 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.

The access through the digital inputs is not controlled.

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

The ATV600 have 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

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.

Device Security Capabilities

ATV600 offers the following security features:

Threats	Desired security property on Embedded Device	security features
Information disclosure	Confidentiality	Password encrypted in a non-reversible way
		User access control
Denial of Service	Availability	Device backup/restore
		Achilles Level 2
Spoofing/Elevation of privilege	User Authenticity / Authorization	Strong password policy
		Access control commissioning tools Modbus TCP
		Access control commissioning tools Web Server

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

Information affecting the security policy of the device is encrypted in transit.

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 ATV600 and facilitates protected file transfer: digitally signed firmware is used to help protect the authenticity of the firmware running on the ATV600 and only allows firmware generated and signed by Schneider Electric.

- Cryptographic signature of the firmware package executed at the firmware update

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:

- Complete device backup/restore available on local HMI, DTM and FDR. Regarding the communication robustness, the ATV600 embedded Ethernet fieldbus and option module successfully passed the certification Achilles L2.

User Authenticity 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, DTM or EcoStruxure Control Expert
- Authorization managed according to channels

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 ATV600, 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 ATV600 controls the access through:

- SoMove DTM (Ethernet connection)
- The webserver
- EcoStruxure Control Expert

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.	Modbus serial, Modbus TCP, EtherNet/IP, SNMP, SNTP, HTTP protocols are insecure. The device does not have the capability to transmit data encrypted using these protocols.	If a malicious user gained access to your network, they could intercept communication.	For transmitting data over internal network, physically or logically segment your network. For transmitting data over external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution. See Protected Environment Assumptions, page 15.

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 in the Control Room (STN V2) on the Schneider Electric website.

Password

Changing Password

The user password can be changed from the DTM Admin options screen.

Reset Password

The password is accessible in the graphic display terminal by default.

The ATV600 stores password in a secure non-reversible format. It is not possible to retrieve a password that has been lost by the user.

For ADMIN user, a special operation is available with the display terminal to reset the ADMIN password to a default value unique to the device.

To reset the ADMIN password:

Step	Action
1	Navigate in the menu [Communication] COM- → [Comm parameters] CMP- → [Profinet] PNC- → [User authentication] SECE- .
2	Scroll to the parameter [Reset PNT Password] RWPP and press OK . Note: If you are using an ATV600 with an option module, you can select the parameter [Reset Eth Opt Pwd] RWPO .
3	The default password is visible on the graphic display terminal until the ADMIN modifies it.

Upon first use, the commissioning tools and webserver requests the user to change the password prior to connecting. The cybersecurity policy does not change when the password is reset.

Password Policy

By default, the password policy of the ATV600 complies with IEEE 1686–2013 as following:

- 8 characters minimum with ASCII [32 to 122] characters
- At least one digit (0-9)
- At least one special character (for example @, \$)

In addition, for password changes, the password history is saved and help prevent the reuse of a password that has been set at least once in the last 5 times.

The password policy can be customized or totally disabled to match with password policy in place in the system of which the device is part.

The following settings are available:

- Password policy: enabled/disabled. If disabled, a password is requested as authentication factor but there is no specific rule defined regarding the password robustness
- Password history: No restriction, Exclude last 3, Exclude last 5
- Special character required: YES/NO
- Numeric character required: YES/NO
- Alphabetic character required: YES/NO
- Minimum password length: any value between 6 and 20

This password policy customization can only be done with SoMove, DTM or EcoStruxure Control Expert. Please refer to DTM online help for details.

Upgrades Management

When the ATV600 firmware is 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 stand

Basics

Introduction

PROFINET

- PROFINET RT extends Ethernet by an advanced industrial protocol management as an application layer for automation applications. In this way, Ethernet protocol is suited for industrial control.
- PROFINET relies on TCP and UDP for non-RT information.
- Products from different manufacturers can be networked by using a PROFINET-compliant switch.

Modbus TCP

The Modbus application layer is standard. Many of the manufacturers are already implementing this protocol. Many have already developed a Modbus TCP/IP connection and numerous products are currently available. With the simplicity of its protocol and the fast Ethernet throughput data rate of 100 Mbit/s, Modbus TCP/IP achieves excellent performance.

The Modbus TCP channel is only used for commissioning tools (Unit ID 251: Fieldbus module, unit ID 248: Variable speed drive) and to access monitoring data related to the drive via the profinet option module.

For more details on how to connect the drive with the Profinet VW363A47 to SoMove, refer to the DTM online help or the FAQ "Connect SoMove to Altivar Process Drive via Ethernet TCP/IP or Profinet".

PROFINET and Ethernet Features

The product supports the following functions:

- Automatic IP address assignment via DHCP and DCP
- Support of MRP (Media Redundancy Protocol)
- Automatic configuration data via iPar-Server
- Commissioning via DTM-based PC software
- Support of LLDP (Link Layer Discovery Protocol)
- S2 redundancy
- I&M 0 to 5 (I&M 4 reserved for PROFIsafe)

Common Additional Features

Identification and Maintenance Data

Overview

Identification & maintenance (I&M) is established through PNO.

Supports the user during various scenarios of the device life cycle, such as:


- Configuration
- Commissioning
- Repair and update
- Operation and visualization

The access to the identification & maintenance data can be achieved using the PROFINET mechanisms (IEC 61158-6).

I&M Record

Description

The table provides the details of I&M record:

Champ	Number of Bytes	Value	Description
I&M (index AFF0)			
HEADER_MANUF_SPEC	6 bytes	String	Manufacturer-specific field
MANUFACTURER_ID	2 bytes	01 hex, 29 hex	129 hex: Schneider Electric
ORDER_ID	20 bytes	Identification object ID 1	Commercial name of the drive
SERIAL_NUMBER	16 bytes	Serial number	C1P1 to C1P8 Note: the full serial number can be viewed in the [Identification]  menu
HARDWARE_REVISION	2 bytes	10 hex, 00 hex	–
SOFTWARE_REVISION	4 bytes	'V', A, B, C	A = MSB of software version B = LSB of software version C = MSB of software revision
REVISION_COUNTER	2 bytes	xx hex, yy hex	Incremented when I&M structure is modified
PROFILE_ID	2 bytes	–	Defined by the PNO (3A00...3AFF)
PROFILE_SPECIFIC_TYPE	2 bytes	–	Profile specific number
IM_VERSION	2 bytes	01 hex, 02 hex	Version I&M: 1.2
IM_SUPPORTED	2 bytes	00 hex, 01 hex	Managed index I&M → I&M0, I&M1, I&M2, I&M3 and I&M5

Champ	Number of Bytes	Value	Description
I&M1 (index AFF1)			
<i>Tag-function</i>	32 bytes	String	Indicates the submodule's function or task
<i>Tag-location</i>	22 bytes	String	Indicates the submodule's location
I&M2 (index AFF2)			
<i>Date and time</i>	16 bytes	String	Sets the time information for the option module internally.
I&M3 (index AFF3)			
<i>Descriptor</i>	54 bytes	String	Saves local documentation specific to the option module.
I&M5 (index AFF5)			
<i>MANUFACTURER_ID</i>	2 bytes	-	Defined by the PNO same as profibus
<i>ORDER_ID (option)</i>	20 bytes	String	Commercial reference (VW3A3647)
<i>SERIAL_NUMBER (option)</i>	16 bytes	String	Unique number
<i>HARDWARE_REVISION (option)</i>	2 bytes	Uint16	Hardware revision of the option module
<i>SOFTWARE_REVISION (option)</i>	4 bytes	1 char 3 Uint8	Software version of the option module
<i>REVISION_COUNTER</i>	2 bytes	Uint16	Incremented when I&M structure is modified
<i>PROFILE_ID</i>	2 bytes	Uint16	Defined by the PNO 3A00 .. 3AFF
<i>PROFILE_SPECIFIC_TYPE</i>	2 bytes	Uint16	Profile specific code
<i>IM_VERSION</i>	2 bytes	2 Uint8	Version I&M : 1.1
<i>IM_SUPPORTED</i>	2 bytes	Uint16	1 : I&M5 supported.

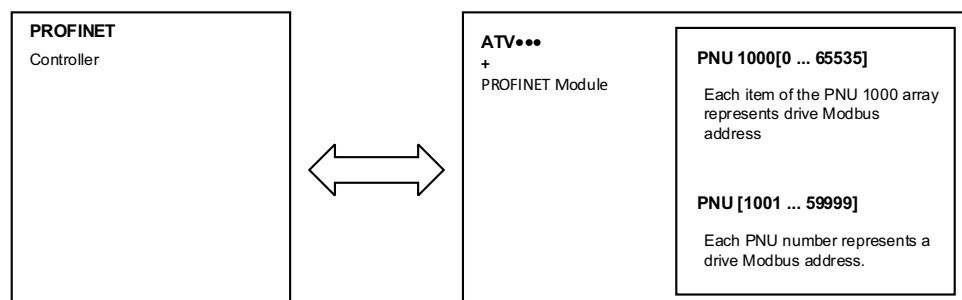
Drive Parameters Channel

Acyclic drive parameters access

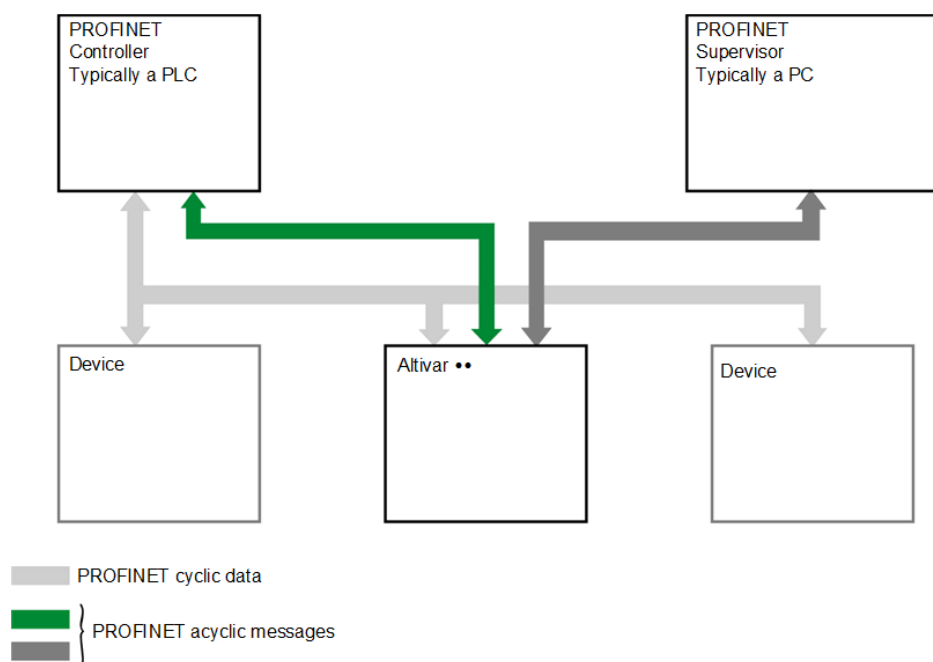
The drive parameters are organized as defined by PNU numbering and addressing modes. However, this addressing mode keeps the native structure of the device (based on Modbus addressing). PNU is numbered from 0...65535 and each PNU represents a parameter (from single type as words to complex data structure or arrays). . All others PNUs are manufacturer-specific.

In the case of this drive, parameters can be separated in two groups:

- Drive parameters which are gathered in a single PNU entry point: PNU1000 and Modbus address as subindex. It is also possible to access the parameters using the Modbus address as PNU for each parameter (1001...59999) and 0 as subindex.



When the drive is operated in drive profile, the parameter management takes benefit of the PROFINET acyclic messaging features. With PROFINET, it is possible to exchange messages of variable length between both controllers (MS0 or MS1). These messages come in addition of the periodic data exchange.



Drive profile request structure

The table describes the drive profile header as used for the drive parameters access:

DU	Byte Nr	Request
Function code	0	–
Slot_num	1	0: global parameters

DU	Byte Nr	Request
Index	2	Reserved for the drive profile: <ul style="list-style-type: none"> 47: Base Mode Parameter Access-Global 47102: Base Mode Parameter Access-Local
Length	3	Length of the drive profile parameter channel frame
Data	4...5	Drive profile parameter channel frame: check

Drive Parameter Structure

A parameter is defined with its PNU number from 1...65535.

Each parameter consists of 3 main areas:

- **PWE**: the value
- **PBE**: describes the parameter attributes
- Text area

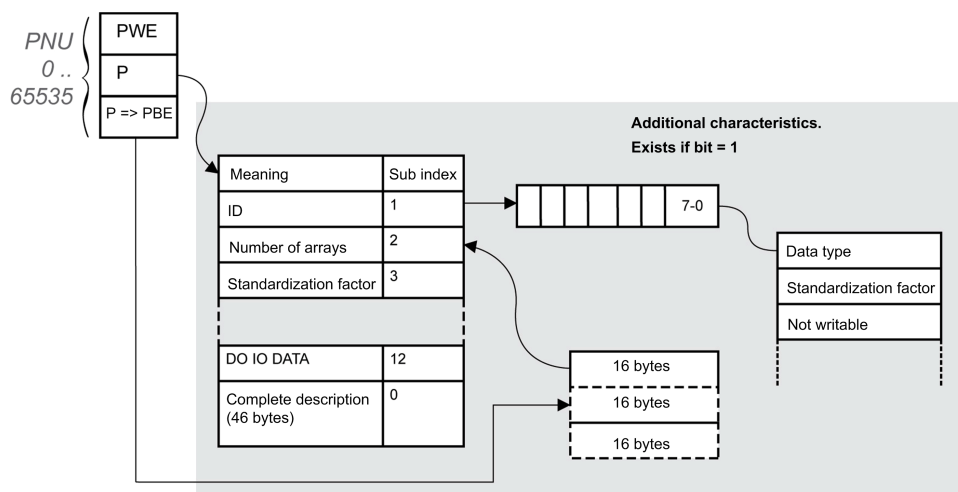
The access to the 3 different areas of a parameter is specified by the **attribute field** of the parameter request.

The parameters and their sub parts are identified as follows:

PNU number + attribute	10 hex	PWE	+ Sub index
	20 hex	PBE	+ Sub index
	30 hex	Text	+ Sub index

Detail of the PBE Attribute

The diagram describes the PBE attribute:



Drive Parameters Access

Each drive parameter can be represented according to the PNU standard structure. Drive parameters are part of the PNU 1000 or can be accessed using the Modbus address as PNU number.

The table provides the possible values of a parameter according to the PNU properties:

Parameter Property	Drive Implementation	Example
PNU number	1000	–
Sub index	Modbus address	CMD address: 8501
PWE	Value of the parameter 0...65535	–
PBE	Describes an array of 65535 words	Constant
Text	–	Drive parameter

Parameters Requests

There are 2 types of request:

- Request drive parameter
- Change drive parameter

These requests are able to manage one or more parameters or several attributes of one parameter.

Parameter Reading

Request

	Byte n+1	Byte n
Request data	Request reference = 01	Request ID = 01
	Axis = 01 hex	Number of parameters = 01
	Attribute = 10 hex *	Number of elements = 01
	PNU number = 3E8 hex	
	Drive parameter address = C81 hex (3201) ETA Modbus address	
*refers to field value (PWE), 20 hex refers to the description field (PBE) and 30 hex to the text field.		

Response

	Byte n+1	Byte n
Response header	Request reference = 01	Request ID = 01
	Axis = 01 hex	Number of parameters = 01
Response data	Format = 42 hex *	Number of elements = 01
	PNU value = xxxx hex (value of ETA)	
*format 42 hex specifies that the returned value is a WORD.		

NOTE: Format is defined by the following returned value: byte 41 hex, word: 42 hex, standard integer: 03 hex, double word: 43 hex.

Parameter Writing

Request

	Byte n+1	Byte n
Request header	Request reference = 01	Request ID = 02
	Axis = 01 hex	Number of parameters = 01
Parameter number	Attribute = 10 hex *	Number of elements = 01
	PNU number = 3E8 hex	
	Sub index = 2329 hex (9001) ACC Modbus address	
Parameter value	Format = 42 hex	Amount values = 01
	Value = 50 (ACC is set to 5 s)	
*refers to field value (PWE), 20 hex refers to the description field (PBE) and 30 hex to the text field.		

Response

	Byte n+1	Byte n
Response header	Request reference = 01	Request ID = 02
	Axis = 01 hex	Number of parameters = 01

Request for Negative Response

The table lists the items of a negative response:

	Byte n+1	Byte n
Request header	Request reference = 01	Request ID = 82*
	Axis = 01 hex	Number of parameters = 01
Parameter number	Format = error 44 hex	Number of values
Value	0x00: Impermissible PNU	0x15: Response too long
	0x01: Cannot change value	0x16: Parameter address impermissible
	0x02: Low or high limit exceeded + sub index	0x17: Illegal format
	0x03: Sub index detected error + sub index	0x18: Number of values inconsistent
	0x04: No array	0x19: Axis/DO nonexistent
	0x05: Incorrect data type	0x20: Cannot change text
	0x06: Setting not permitted + sub index	0x65: Invalid request reference
	0x07: Cannot change description + sub index	0x66: Invalid request ID
	0x09: No description	0x67: Invalid axis number / DO-ID
	0x0B: No operation priority	0x68: Invalid number of parameters
	0x0F: No text array available	0x69: Invalid attribute
	0x11: Cannot execute the request. Reason not specified	0x6B: Request too short
	0x14: Value impermissible	
*for all negative responses the ID equals to response code or 80 hex.		

With the sub index in addition to the detected error value, the total length of the answer is 10 bytes.

Presentation

Hardware Setup

Hardware Presentation

PROFINET Fieldbus Module

The figure shows a PROFINET fieldbus module with 2 RJ45 connectors:



Firmware Version

Compatibility

The VW3A3647 option module version 3.1IE08 and higher is compliant with all Altivar process product range with firmware V3.8 or higher. When the drive has a firmware version that does not support VW3A3647 option module, a **[Internal Error 6]** INF6 error (see [Internal Error 6] InF6 Error, page 80) is triggered and a firmware update of the drive is required. The firmware update can only be done by Schneider Electric Services. For more information contact your local Schneider Electric Services..

The associated GSDML is named as the following example:

GSDML-V2.4-Schneider-ATV6xx-YYYYMMDD.xml

The files are available on www.se.com.

Installation of the fieldbus module

Before starting

Verify that the catalog number printed on the label corresponds to the purchase order.

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

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.

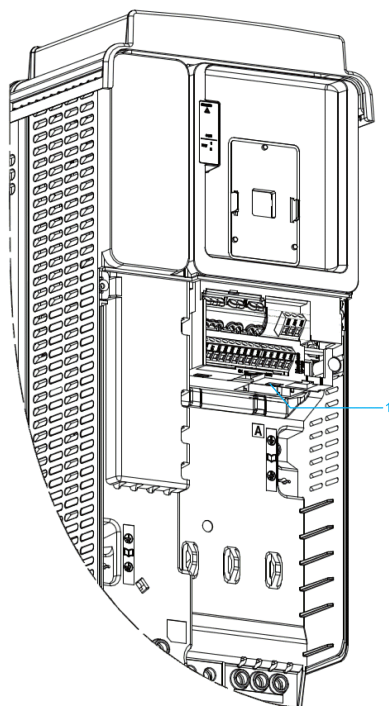
Failure to follow these instructions will result in death or serious injury.

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

Inserting the fieldbus module

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


Step	Action
1	Ensure that the power is off.
2	Locate the fieldbus module slot (A) on the bottom of the control part.
3	Insert the module.
4	Check that the module is correctly inserted and locked mechanically in the drive.
5	Wire the fieldbus module to the automate.
6	Add the corresponding sticker on the LED front panel of the drive.



1 Fieldbus Module Slot A

Removing the fieldbus module

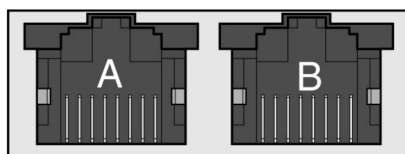
The table provides the procedure for removal of the fieldbus module from the drive:

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

Electrical Installation

Pin Layout

The VW3A3647 option module is equipped with 2 RJ45 female sockets for the PROFINET connection.



8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1

The table provides the pin out details of each RJ45 connector:

Pin	Signal	Meaning
1	Tx+	Ethernet transmit line +
2	Tx-	Ethernet transmit line –
3	Rx+	Ethernet receive line +
4	–	–
5	–	–
6	Rx-	Ethernet receive line –
7	–	–
8	–	–

Cable Specification

Cable specifications are as follows:

- Ethernet cable must be AWG24 & SF/FTP
- Minimum Cat 5e,
- Use equipotential bonding conductors (100 BASE-TX, category 5e or industrial Ethernet fast connect)
- Connector RJ45, no crossover cable
- Shield: both ends grounded
- Twisted-pair cable
- Verify that wiring, cables, and connected interfaces meet the PELV requirements.
- Maximum cable length per segment = 100 m (328 ft)

More details on cable connection in the *ATV630 installation manual*.

Cable Routing Practices

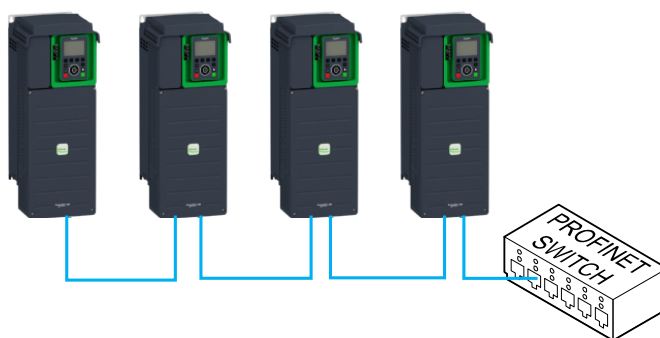
Installation Topology

The VW3A3647 option module, with its 2 RJ45 connector, enables several wiring solutions:

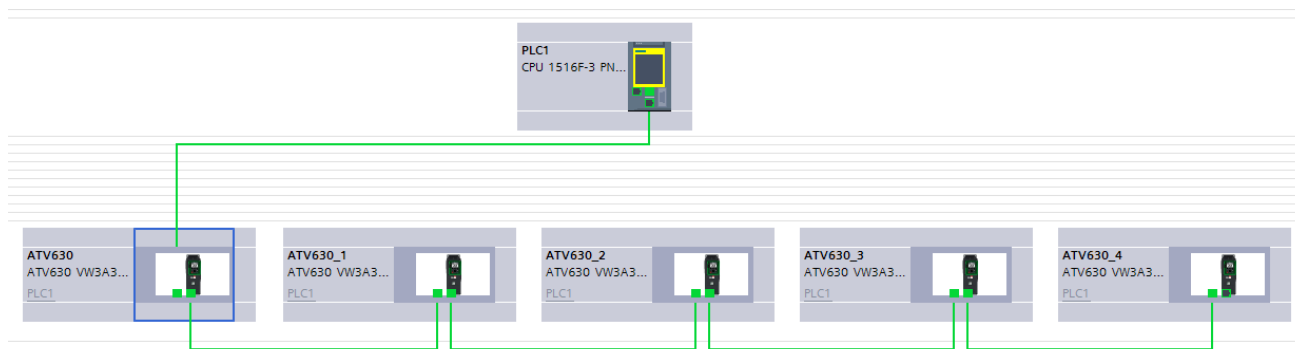
- **Daisy chain topology**
- **Star topology**
- **Ring topology**

Daisy chain Topology

- **Wiring topology:**



- **Daisy chain topology on TIA Portal:**

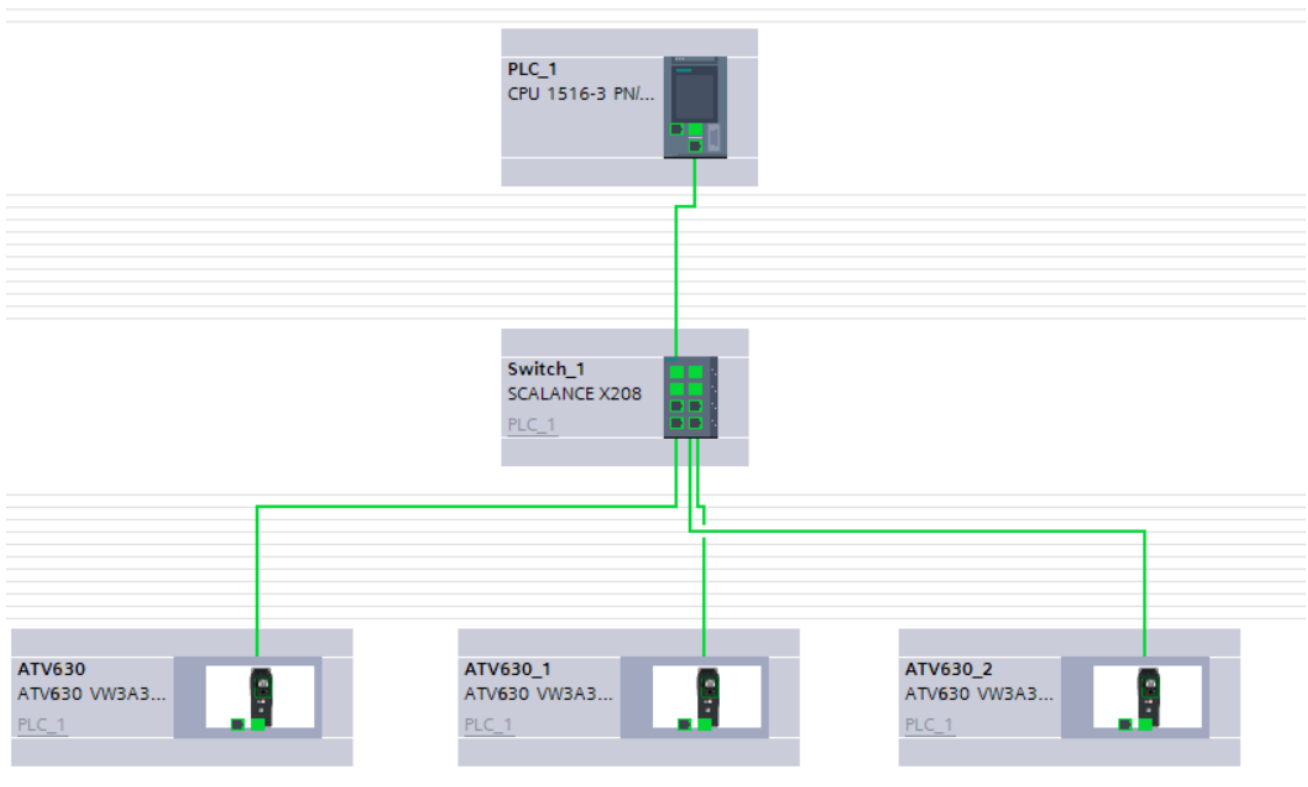


Star Topology

- **Wiring topology:**

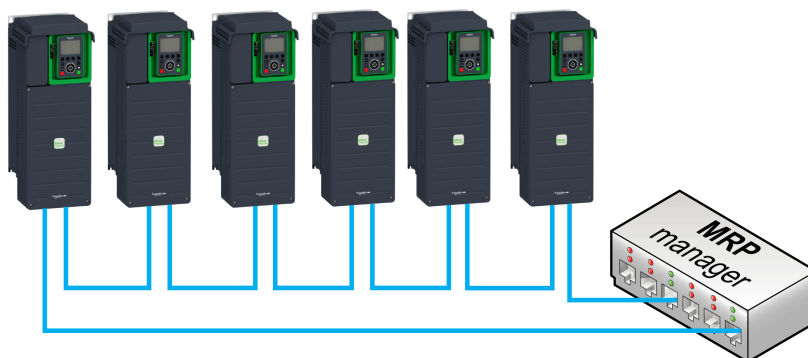


- **Star topology on TIA Portal:**

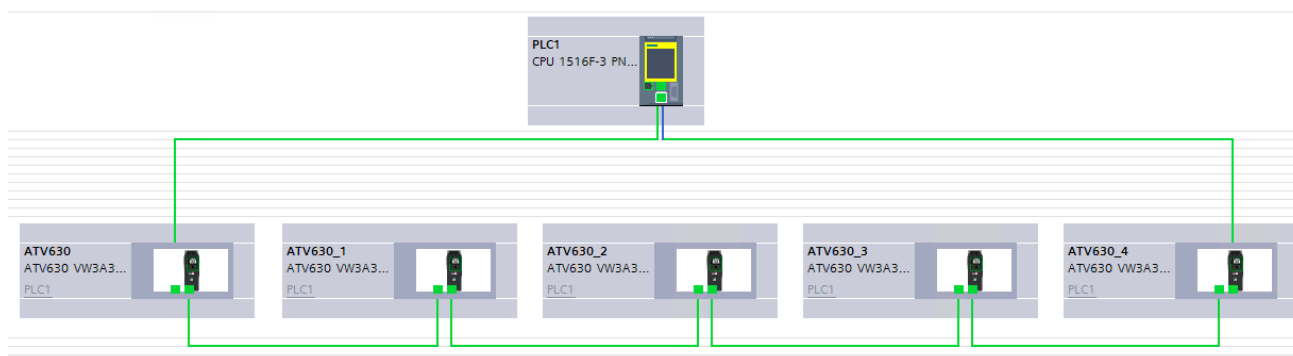


Ring Topology

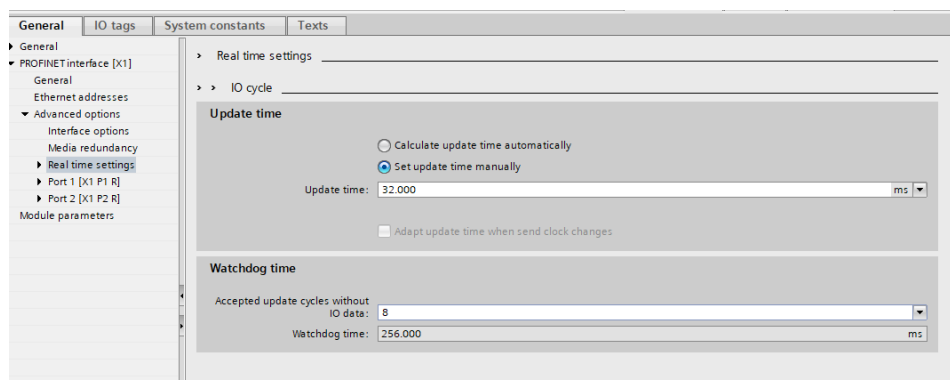
- **Wiring topology:**



- **Topology on TIA Portal:**



The ring topology can only be used with a media redundancy protocol (MRP) capable managed device. The bus watchdog shall be configured by increasing manually the "Update Time" or the "IO data" on TIA Portal when using MRP function in order to avoid triggering untimely **[Fieldbus Com Interrupt]** $\mathcal{L} \cap F$.



Software Setup

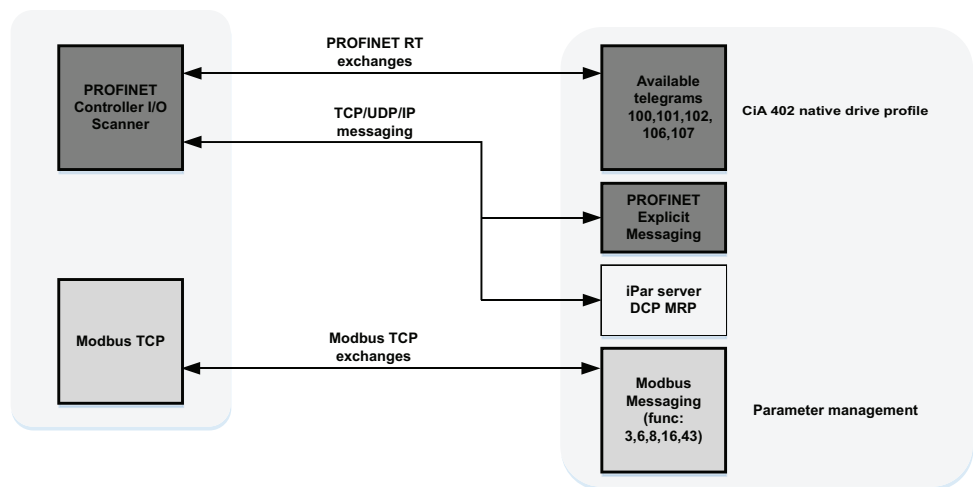
Software Overview

Simplified TCP/IP Model

The table provides the basic software overview according to the simplified TCP/IP model:

Application	Transport	Network	Link
PROFINET / IP services	TCP/UDP	IP	Ethernet
PROFINET RT	–	–	Ethernet

PROFINET Fieldbus Module Features Overview



Basic Settings

Introduction

The parameters are described according to the graphic display terminal.

These settings are also possible from commissioning software.

Access

The parameters are accessible in the **[Communication] COM- → [Comm parameters] CMP- → [Profinet] PNC-** menu.

Possible Settings

The table presents the parameter settings:

HMI label	Setting	
[Device Name] PAN	[0D0C hex= 3340] to [0D13 hex= 3347]	Type: UINT (Unsigned16) Read/write: R/W
<p>This parameter is used to set the device name.</p> <p>If [IP mode] IPM of Profinet module is set to [DHCP] DHCP, set the [Device Name] PAN as defined in the DHCP server.</p>		
[IP mode] IPM	Logic address: FBC2 hex = 64450 Factory setting: [Fixed] MANU	Type: WORD (Enumeration) Read/write: R/W
<p>IP mode This parameter is used to select the IP address assignment method:</p> <p>[Fixed] MANU: Manually set the IP address.</p> <p>[DHCP] DHCP: Automatically gets the IP address from the DHCP server using the device name.</p> <p>[DCP] DCP: Automatically gets the IP address from the DCP server using the device name.</p> <p>Note: The parameter is forced to [DCP] DCP if "Support device replacement without exchangeable medium" is selected (only available with a Siemens PLC).</p>		



HMI label	Setting	
[IPAddress] <i>IPC1, IPC2, IPC3, IPC4</i>	Logic address IPC1: FAD4 hex = 64212 Logic address IPC2: FAD5 hex = 64213 Logic address IPC3: FAD6 hex = 64214 Logic address IPC4: FAD7 hex = 64215	Type: UINT (Unsigned16) Read/write: R/W
Configured Profinet IP Address This parameter is used to set the IP address and can be edited only when the IP mode is set to fixed address. The modification of this parameter setting is only effective when you restart the drive if [IP mode] <i>IPM</i> is set to [Fixed] <i>MANU</i> .		
[IPMask] <i>IPM1, IPM2, IPM3, IPM4</i>	Logic address IPM1: FAD8 hex = 64216 Logic address IPM2: FAD9 hex = 64217 Logic address IPM3: FADA hex = 64218 Logic address IPM4: FADB hex = 64219	Type: UINT (Unsigned16) Read/write: R/W
Configured Profinet IP mask This parameter can be edited only when the IP mode is set to fixed address. The modification of the setting value is effective when you restart the drive.		
[IPGateway] <i>IPG1, IPG2, IPG3, IPG4</i>	Logic address IPG1: FADC hex = 64220 Logic address IPG2: FADD hex = 64221 Logic address IPG3: FADE hex = 64222 Logic address IPG4: FADF hex = 64223	Type: UINT (Unsigned16) Read/write: R/W
Configured Profinet IP Gate This parameter can be edited only when the IP mode is set to fixed address.		
[MonitorIPAddress] <i>IPA1, IPA2, IPA3, IPA4</i>	Logic address IPA1: FAFC hex = 64252 Logic address IPA2: FAFD hex = 64253 Logic address IPA3: FAFE hex = 64254 Logic address IPA4: FAFF hex = 64255	Type: UINT (Unsigned16) Read/write: R
Current Profinet IP Address This parameter can be accessed only when IP mode is set to fixed address. This is the current IP setting taken into account by the drive.		
[MonitorIPMask] <i>IPS1, IPS2, IPS3, IPS4</i>	Logic address IPS1: FB00 hex = 64256 Logic address IPS2: FB01 hex = 64257 Logic address IPS3: FB02 hex = 64258 Logic address IPS4: FB03 hex = 64259	Type: UINT (Unsigned16) Read/write: R
Current Profinet IP Mask This parameter can be accessed only when IP mode is set to fixed address.		
[MonitorIPGateway] <i>IPT1, IPT2, IPT3, IPT4</i>	Logic address IPT1: FB04 hex = 64260 Logic address IPT2: FB05 hex = 64261 Logic address IPT3: FB06 hex = 64262 Logic address IPT4: FB07 hex = 64263	Type: UINT (Unsigned16) Read/write: R
Profinet IP Gateway obtained from the network This parameter can be accessed only when IP mode is set to fixed address.		

HMI label	Setting	
[PPO profile used] PRFL	Logic address: 1A09 hex = 6665	Type: UINT (Unsigned16) Read/write: R
PPO profile used This parameter displays the actual profile for the device. This parameter can be accessed in [Display] MON–, [Communication map] CMM–, [PROFINET DIAG] PRN– menu. The parameter settings are: <ul style="list-style-type: none">• [0] = UNCG / not configured• [100] = Telegram 100• [101] = Telegram 101• [102] = Telegram 102• [106] = Telegram 106• [107] = Telegram 107		
[MAC @] MAC	Type: UINT (Unsigned16) Read/write: R	
This parameter displays the MAC address of the Profinet VW3A3647 option module.		

IP Parameter Settings

Assigning IP Parameters

The drive needs three IP parameters:

- The drive IP address.
- The subnet mask.
- The gateway IP address.

When the **[IP mode]** *IPM* is set to **[Fixed]** *MANU*, you can directly set the IP address using the graphic display terminal or using the commissioning software.

When the **[IP mode]** *IPM* is set to **[DHCP]** *DHCP*, you can get IP address from a DHCP server (correspondence between the device name and the IP addresses).

When the **[IP mode]** *IPM* is set to **[DCP]** *DCP*, you can use DCP (Discovery control protocol) protocol to discover PROFINET devices.

Entering IP Parameters in the Display Terminal

In the **[Communication]** *COM* → **[Comm parameters]** *CMP* → **[Profinet]** *PNC*– menu, enter the following IP parameters:

- **[COM_IPAddress]** *IPC1, IPC2, IPC3, IPC4*
- **[COM_IPMask]** *IPM1, IPM2, IPM3, IPM4*
- **[COM_IPGateway]** *IPG1, IPG2, IPG3, IPG4*

Turn off the drive and then back on again (control voltage if a separate power supply is being used), otherwise the IP parameters are not taken into account.

The new IP address is immediately displayed but will only be effective the next time the drive is turned on.

Case of Manual Switching of [IP mode] **IPM**

When switching **[IP mode] IPM** to **[DCP] DCP**

- IP settings are no longer editable
- Turn off the drive supply and then back on again, including the control voltage if a separate power supply is being used
- The new configuration is applied, the device is waiting for IP settings from the PROFINET controller

When switching **[IP mode] IPM** to **[Fixed] MANU**

- IP settings become editable
- Set IP settings with valid values
- Turn off the drive and then back on again, including the control voltage if a separate power supply is being used
- The new configuration is applied

NOTE: If the IP settings are not valid, the drive triggers **[Fieldbus Error] EPF2** after the next power-on.

When switching **[IP mode] IPM** to **[DHCP] DHCP**

- IP settings are no longer editable.
- Set the device name with a valid value.
- Turn off the drive and then back on again, including the control voltage if a separate power supply is being used.
- The new configuration is applied, the device is waiting for IP settings from DHCP server.

Case of Automatic Switching of [IP mode] **IPM** to [DCP] **DCP**

The following condition should be fulfilled:

- The option module has a station name configured and validated.
- The device is connected to a PROFINET controller.
- The PROFINET controller has the station name in its own configuration. This station name is the same as the option module's.
- The settings are in local configuration of the PROFINET controller.

If the all above mentioned conditions are fulfilled:

- **[IP mode] IPM** is automatically set to **[DCP] DCP**
- IP settings are replaced by the one set in local PROFINET controller
- The new configuration is applied immediately

[User authentication] SECP- menu

About This Menu

This menu is accessible in **[Communication] COM-** → **[Comm parameters] CMP-** → **[Profinet] PNC-** menu via the graphic display terminal if the Profinet module (VW3A3647) has been inserted. The content of this menu can also be accessed via the commissioning software.

NOTE: The drive firmware must be V3.8 or higher and the option module firmware must be V3.0IE19 or higher.

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

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

Possible Settings

The table presents the parameter settings:

HMI label	Setting
[PNT User Auth.] SCPP	Factory Setting: [Yes]
<p>Profinet user authentication This parameter is used to enable or disable the user authentication feature.</p> <p>Disabling this feature, no credentials will be required to access your process or machine. This setting is saved with the configuration and will be active if a configuration is loaded or copied.</p>	
<p>⚠ WARNING</p>	
<p>UNAUTHENTICATED ACCESS AND MACHINE OPERATION</p> <p>Do not disable the feature if your machine or process is accessible to unauthorized personnel either directly or via a network.</p> <p>Failure to follow these instructions can result in death, serious injury, or equipment damage.</p>	
<p>Set [PNT User Auth.] SCPP to:</p> <ul style="list-style-type: none"> [No] NO to disable User authentication. Connection to PC software tools provided by Schneider-Electric (such as SoMove FDT / DTM) with Modbus TCP (via VW3A3647 Profinet module) is unlocked. [Yes] YES to enable User authentication. Connection to PC software tools provided by Schneider-Electric (such as SoMove FDT / DTM) with Modbus TCP (via VW3A3647 Profinet module) is locked by a password. 	
[Reset PNT Password] RWPP	Factory Setting: [No]
<p>Reset option password (used for user authentication).</p> <p>It resets the user authentication password to the default value. Once reset, the default password can be read using [Option default password] DPW.</p> <p>If [Reset Option Pwd] RPWD is set to:</p> <ul style="list-style-type: none"> [No] NO: Password reset not requested. [Yes] YES: Password reset requested. The parameter switches back to [No] NO when the operation is done. 	

HMI label	Setting
[Option default password] DPW	-

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

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

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

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



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

iPar Service

Description

The PROFINET fieldbus module is compliant with iPar server function. The purpose of this function is to save (upload) the parameters (iParameter) of any PROFIBUS DP device, PROFINET I/O device, or module within the same host controller that is maintaining the GSD-based parameters and diagnosis messages.

The configuration can be:

- Saved:
 - manually by using **[IPAR Action]** **IPAA** parameter when set to **[Save]** **SAVE**
 - automatically by using **[iPar Autosave Act]** **IPAS** when set to **[Yes]**. **[iPar Local Conf]** **ICFG** must be set to **[Yes]**.
- Restored:
 - manually by using **[IPAR Action]** **IPAA** parameter when set to **[Restore]** **REST**
 - at each restart of the drive using **[iPar Local Conf]** **ICFG** when set to **[No]**.

The status of the Save/Restore action is viewed with the **[IPAR Action Status]** **IPAC**.

Refer to the table below for more information about the parameters.


Access

The parameters are accessible in the **[Communication]** **COM** → **[Comm parameters]** **CMP** → **[Profinet]** **PNC** menu.

Possible Settings

The table presents the parameter settings:

HMI label	Setting	
[iPar Activation] IPAV	Logic address: FB12 hex = 64274	Type: WORD (Enumeration) Read/write: R/W
iPar service activation This parameter is used to enable the iPar service. <ul style="list-style-type: none"> • [No]: Indicates that the iPar service is disabled. • [Yes]: Indicates that the iPar service is enabled. 		
[iPar Autosave Act] IPAS	Logic address: FB13 hex = 64275 Factory setting: [No]	Type: WORD (Enumeration) Read/write: R/W
iPar autosave activation This parameter is used to enable the iPar autosave service. <ul style="list-style-type: none"> • [No]: Indicates that the iPar autosave service is disabled. • [Yes]: Indicates that the iPar autosave service is enabled. 		

HMI label	Setting	
[iPar Autosave Timer] <i>IPAT</i>	0...9999 min Factory setting: 10 min Logic address: FB16 hex = 64278	Type: UINT (Unsigned16) Read/write: R/W
iPar autosave timer This parameter is used to set the interval for periodic saving of the iPar service. 0: No autosave 1...9999 min: iPar service is saved after specific interval of time.		
[iPar Error Response] <i>IPAF</i>	Logic address: FB15 hex = 64277 Factory setting: [Yes]	Type: WORD (Enumeration) Read/write: R/W
iPar response to detected error This parameter is used to enable the iPar error handling. <ul style="list-style-type: none"> • [No]: Indicates that the iPar error handling is disabled. • [Yes]: Indicates that the iPar error handling is enabled. 		
[IPAR Action] <i>IPAA</i>	Logic address: FB1C hex = 64284	Type: WORD (Enumeration) Read/write: R
IPAR action This parameter is used to transfer the configuration between the drive and the PLC. The parameter settings are: <ul style="list-style-type: none"> • [Inactive] <i>DEAC</i>: The configuration transfer through iPar is disabled (Factory setting). • [Save] <i>SAVE</i>: The configuration is transferred from the drive to the PLC. • [Restore] <i>REST</i>: The configuration is restored from the PLC. Note: When parameters requiring a restart are modified, it is essential to restart the drive for the restore to succeed.		
<div>  WARNING </div>		
UNANTICIPATED EQUIPMENT OPERATION Verify that restoring the configuration from the PLC is compatible with the type of wiring used. and perform a comprehensive commissioning test to verify correct operation. Failure to follow these instructions can result in death, serious injury, or equipment damage.		
[IPAR Action Status] <i>IPAC</i>	Logic address: FB1D hex = 64285 Factory setting: [In Progress] <i>EXEC</i>	Type: WORD (Enumeration) Read/write: R
IPAR action status This parameter shows the status of the [IPAR Action] <i>IPAA</i> . The parameter settings are: <ul style="list-style-type: none"> • [In Progress] <i>EXEC</i>: The transfer is under execution. • [Save - Success] <i>SASU</i>: Save success. • [Save - Error] <i>SAER</i>: Save error. • [Restore - Success] <i>RESU</i>: Restore success. • [Restore - Error] <i>REER</i>: Restore error. 		

HMI label	Setting	
[iPAR Config Selection] IPAM	Logic address: FB1F hex = 64287 Factory setting: [Active Drive Config] ACTI	Type: WORD (Enumeration) Read/write: R
iPAR configuration selection This parameter defines the drive configuration to be transferred. The parameter settings are: <ul style="list-style-type: none"> • [Active Drive Config] ACTI: the transfer (save and restore) is only done for the active configuration. • [All Drive Config] FULL: This setting allows to transfer multiple drive configurations selected in [File management] FMT → [Factory settings] FCS → [Save Configuration] SCSI. 		
[PNT Mdb Word Order] TWOP	Factory setting: [ON] HIGH	
Profinet ModbusTCP word order This parameter is used to invert the words order. The parameter settings are: <ul style="list-style-type: none"> • [OFF] LOW: Low word first. • [ON] HIGH: High word first. 		
[iPar Local Conf] ICFG	Logic address: FB14 hex = 64276 Factory setting: [No]	Type: WORD (Enumeration) Read/write: R/W
iPar local configuration This parameter is used to select local or server configuration. <ul style="list-style-type: none"> • [No]: Indicates that the drive configuration is downloaded from the iPar server at power-on of the drive. • [Yes]: Indicates that the drive configuration is available locally in the drive. 		
[iPar Status] IPAE	Logic address: FB17 hex = 64279	Type: WORD (Enumeration) Read/write: R
iPar service status This parameter displays the iPar service status. This parameter can be accessed in [Display] MON- → [Communication map] CMM- → [PROFINET DIAG] PRN- menu. The parameter settings are: <ul style="list-style-type: none"> • [Idle State] IDLE: Idle state • [Init] INIT: Initialization • [Configuration] CONF: Configuration • [Ready] RDY: Ready • [Operational] OPE: Operational • [Not Configured] UCFG: Not configured • [Unrecoverable Error] UREC: Unrecoverable error state 		

HMI label	Setting	
[iPar Error Code] <i>IPAD</i>	Logic address: FB18 hex = 64280 Factory setting: [iPar Error Code] <i>IPAD</i> = [0]	Type: WORD (Enumeration) Read/write: R
<p><i>iPar detected error code</i> This parameter displays the iPar service status. This parameter can be accessed in [Display] <i>MON</i>- → [Communication map] <i>CMM</i>- → [PROFINET DIAG] <i>PRN</i>- menu.</p> <p>The parameter settings are:</p> <ul style="list-style-type: none"> • [0] = No error • [1] = Stored configuration is not ok. • [2] = No configuration file on the IPAR server or configuration is not compatible. (Served configuration is not ok). • [3] = Connection error to the IPAR configuration file on the server. • [4] = Writing error the configuration file to the server. 		

Modbus TCP Settings

The Modbus channel is only used for commissioning tools (Unit ID 251: Fieldbus module, unit ID 248: Variable speed drive) and to access monitoring data related to the drive via the profinet option module.

To use standard Modbus TCP, **[PNT User Auth.]** *SCP* must be set to **NO**.

Function Name	Code		Description	Comments
	Dec	Hex		
Read Holding Register	03	03 hex	Read multiple register	Maximum PDU length: 63 words
Diagnostic	08	08 hex	Diagnostic	–
Read/write multiple registers (Unit ID 0-248)	23	17 hex	Read/write multiple registers	Max PDU length: 121 words (W), 125 words (R)
Read device Identification	43	2B hex	Schneider identification	(subfunction 14/0E hex) See the table below

The following table provides the details of device identification

Byte(s)	Meaning	With the VW3A3647 PROFINET Module	
0	Function code = 2B hex	2B hex	
1	Type of MEI	0E hex	
2	ReadDeviceId code	01 hex	
3	Degree of conformity	02 hex	
4	Number of additional frames	00 hex	
5	Next object ID	00 hex	
6	Number of objects	3 for basic 4 for regular or extended	
7	Object 1 ID	00	
8	Length of object 1 (A)	13	
9...21	Value of object 1 (A ASCII character)	Schneider Electric	
22	Object 2 ID	01 hex = Product Code	
23	Length of object 2 (B)	11 (for the following example only)	
24...23+B	Value of object 2 (B ASCII characters) ⁽¹⁾	Example: ATVxxxxxxxx	
24+B	Object 3 ID	02 hex = Major.Minor revision	
25+B	Length of object 3 (C)	4	
26+B...29+B	Value of object 3 (C ASCII characters)	Example: 0201 for version 2.1	
30+B	Object 4 ID	06 hex = Application name ⁽²⁾	For regular and extended
31+B	Length of object 4 (D)	8 (for the following example only)	
32+B...31+B +D	Value of object 4 (D ASCII characters) ⁽¹⁾	Example: Machine 4	
(1) The length of this field is variable. Use the Length of object X field associated with it to determine the length.			
(2) In the case of the drive, this data item corresponds to [DEVICE NAME] .			
The response to a drive identification request does not cause an exception response			

S2 Redundancy

Description

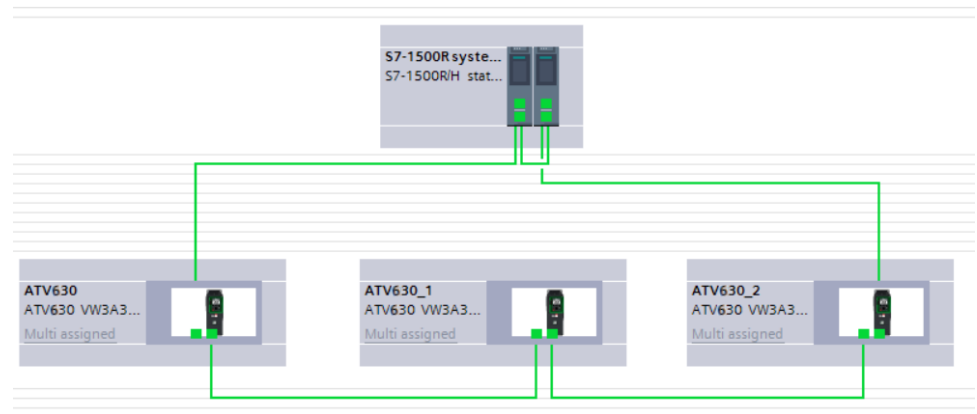
System redundancy S2 defines the concept of establishing multiple connections to a device to ensure continuous system operation in case of a communication connection interruption. The S2 redundancy functionality, integrated into the VW3A3647 option module through the GSDML file, enables two controllers, one primary and one backup, to connect to the device.

- When the primary controller is unavailable, the backup controller seamlessly takes over communication without any disruption to the network.
- Both controllers use the same configuration (submodule configuration)

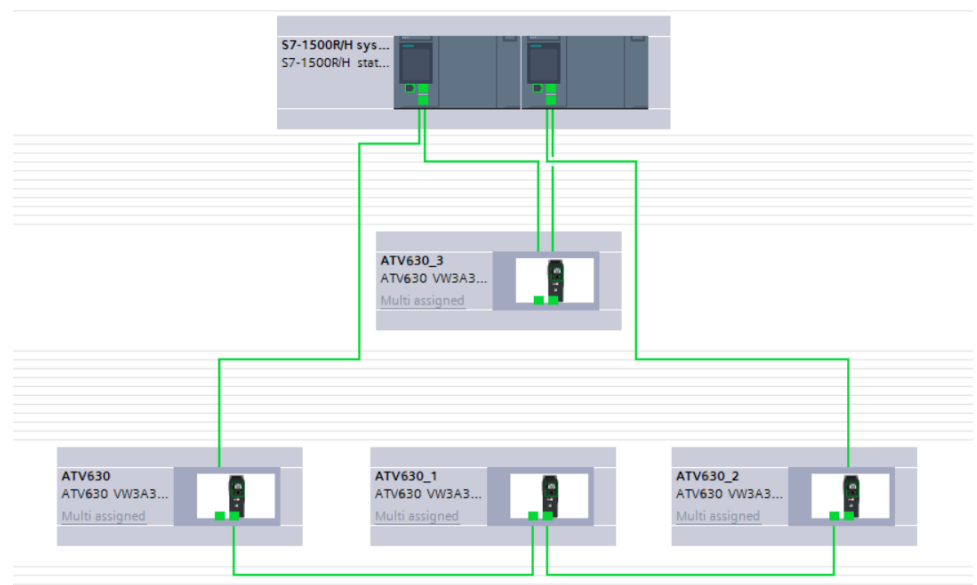
Network topology

The profinet devices (drive + VW3A3647 option module) supporting the S2 redundancy functionality can be paired to:

- R-system with S2 redundancy: the synchronization between the two controllers is done via Profinet ring. the Profinet devices are connected to the controllers in a MRP ring structure.



- H-system with S2 redundancy: the synchronization between the two controllers is done via the fiber optical.



Communication Profile

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, PROFIBUS DP, 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
- Drive profile
- CIP AC Drive

CiA402 device profile for drives and motion control represents the next stage of this standard development and is now part of the IEC 61800-7 standard.

Application Profile

Application profile defines the services to be provided by the devices on a machine. For example, CiA DSP 417-2 V 1.01 part 2: CANopen application profile for lift control systems - virtual device definitions.

Interchangeability

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

Functional Profiles Supported by the Altivar 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 CANopen control word
- Ethernet Modbus TCP embedded 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.

NOTE: when **[Control Mode]** `CHCF` is set to I/O profile, Drive profile is not supported by the Profinet option module.

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:

- **Separated channel mode** **[Separate]** `SEP`
- **Combined channel mode** **[Not separ.]** `SIM`,

Functional Description

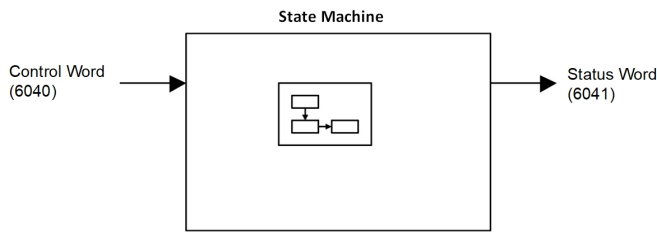
Introduction

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

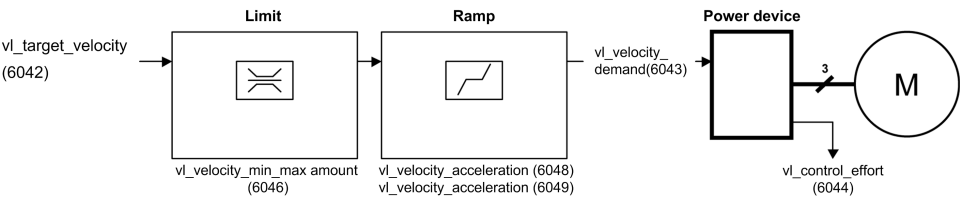
CiA402

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:



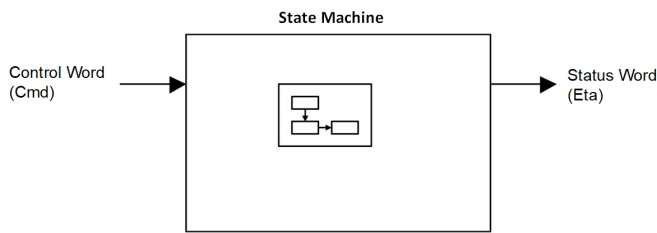
Simplified diagram for speed control in *Velocity* mode:



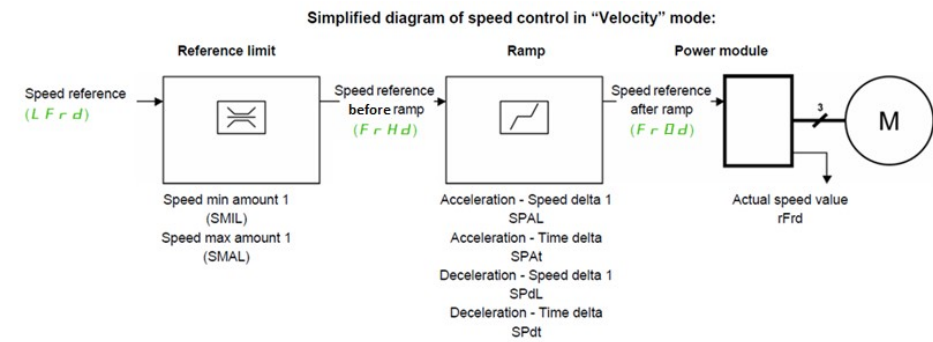
Altivar Drive

These diagrams translate as follows for the Altivar drive.

The following figure shows the control diagram for drive operation:



Simplified diagram for speed control in *Velocity* mode:

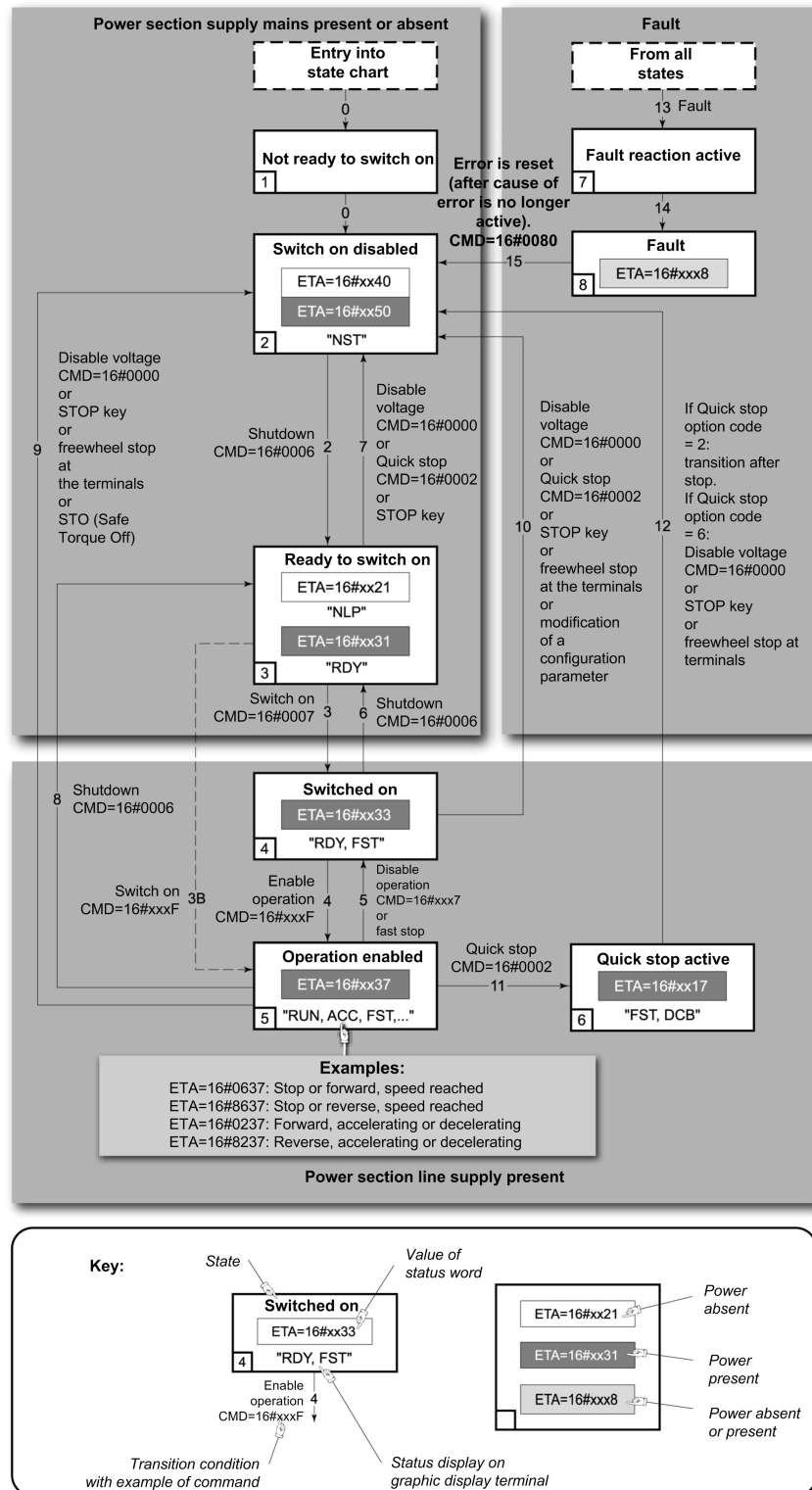


CIA402 Operating State Diagram

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](#).

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

Operating State	Description
6 - <i>Quick stop active</i>	<p>The drive performs a fast stop and remains locked in the operating state 6-<i>Quick stop active</i>. Before restarting the motor, it is required to go to the operating state 2-<i>switch on disabled</i>. During fast stop, the drive is unlocked and power is supplied to the motor.</p> <p>The configuration parameters cannot be modified.</p> <p>The condition for transition 12 to state 2 - <i>Switch on disabled</i> depends on the value of the parameter</p> <p>[Quick Stop Mode] QSTD:</p> <p>If the <i>Quick stop</i> 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 - <i>Switch on disabled</i>.</p> <p>If the <i>Quick stop</i> 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 - <i>Quick stop active</i> until:</p>
7 - <i>Fault reaction active</i>	Transient state during which the drive performs an action corresponding to the selected error response.
8 - <i>Fault</i>	<p>Error response terminated. Power stage is disabled.</p> <p>The drive is locked, no power is supplied to the motor.</p>

Device Status Summary

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

NOTE:

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

Cmd Register [0]

Bit Mapping of the Control Word

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

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

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

X: Value is of no significance for this command.

0→1: Command on rising edge.

Stop Commands

Halt Command

The **Halt** command enables movement to be interrupted without having to leave the **5 - Operation enabled** state. The stop 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 **[Fast Stop Assign] FST**, **[On Ramp] RMP**, **[Freewheel Stop] NST**, or **[DC injection] DCI**, 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	
Bit 11	C311
Bit 12	C312
Bit 13	C313
Bit 14	C314
Bit 15	C315

For example, to assign the DC injection braking to bit13 of fieldbus module, simply configure the **[DC injection]** **DCI** parameter with the **[C313]** **Ⓒ 3 1 3** value.

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

[CIA402 State Reg] E L R

Bit Mapping of the Status Word

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

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

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

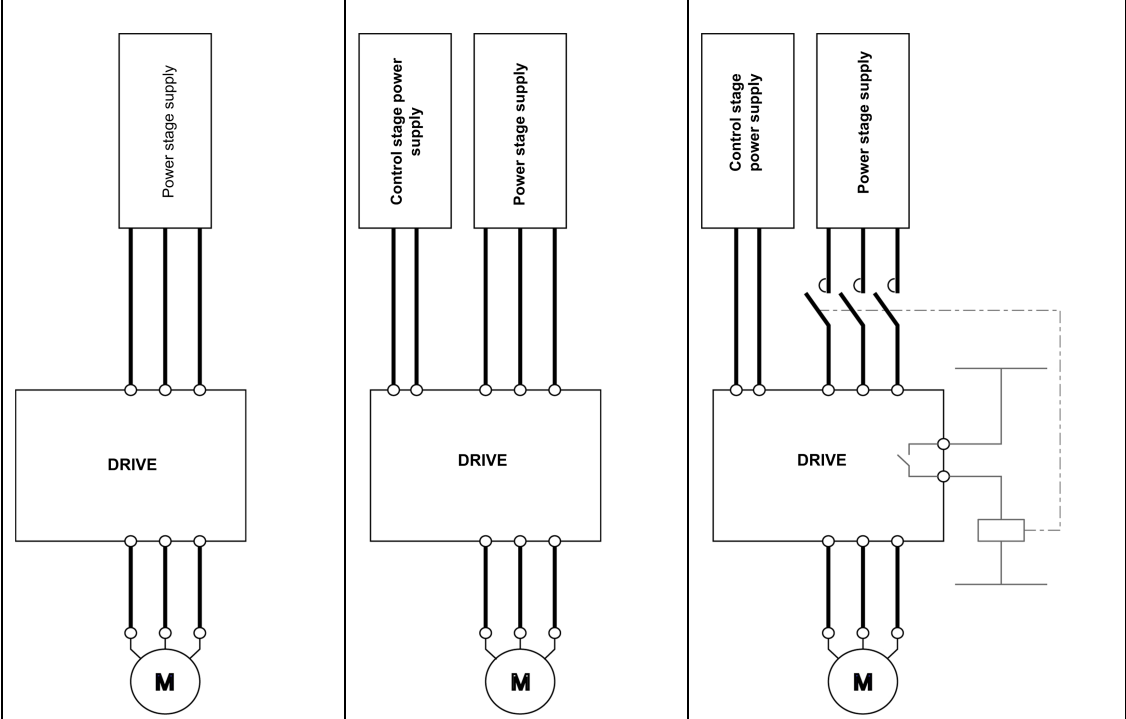
X: In this state, the value of the bit can be 0 or 1.

Starting Sequence

Description

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

There are 3 possible scenarios:

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

Starting Sequence for a Drive Powered by the Power Stage Supply

Description

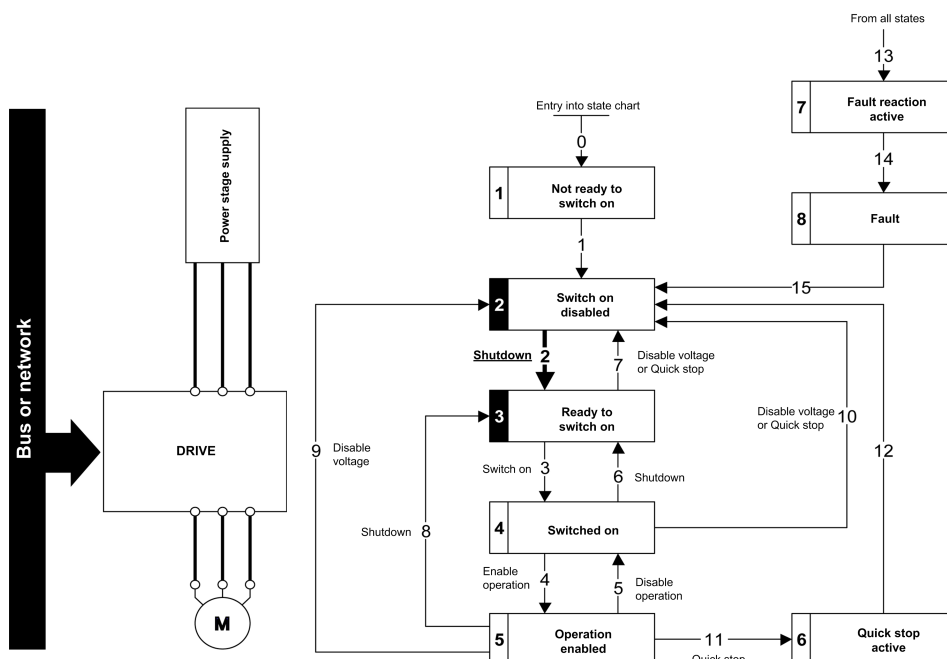
Both the power and control stages are powered by the power stage supply.

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

The following sequence must be applied:

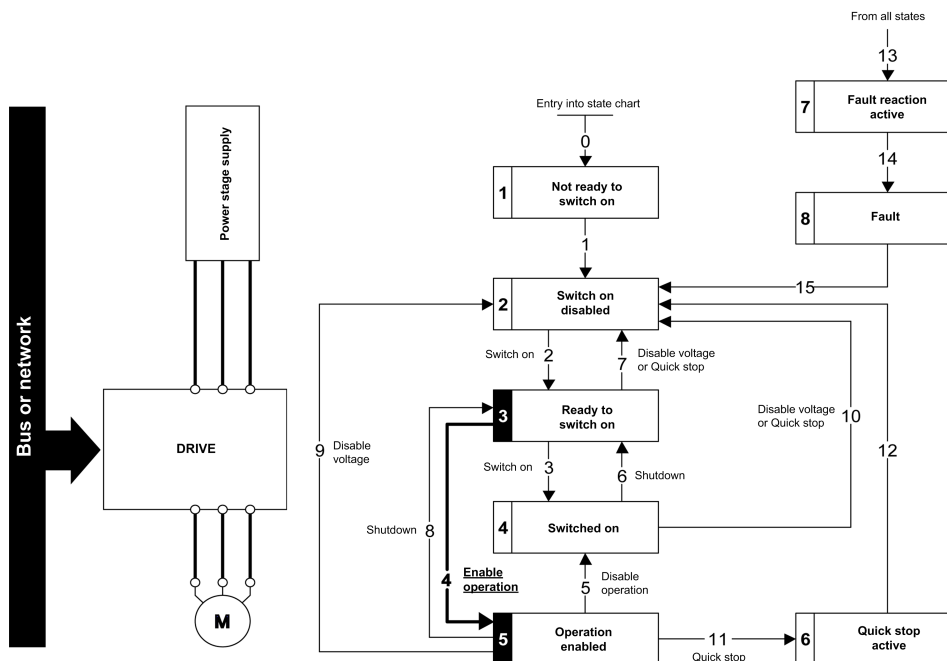
Step 1

Apply the 2 - *Shut down* command



Step 2

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



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

Starting Sequence for a Drive with Separate Control Stage

Description

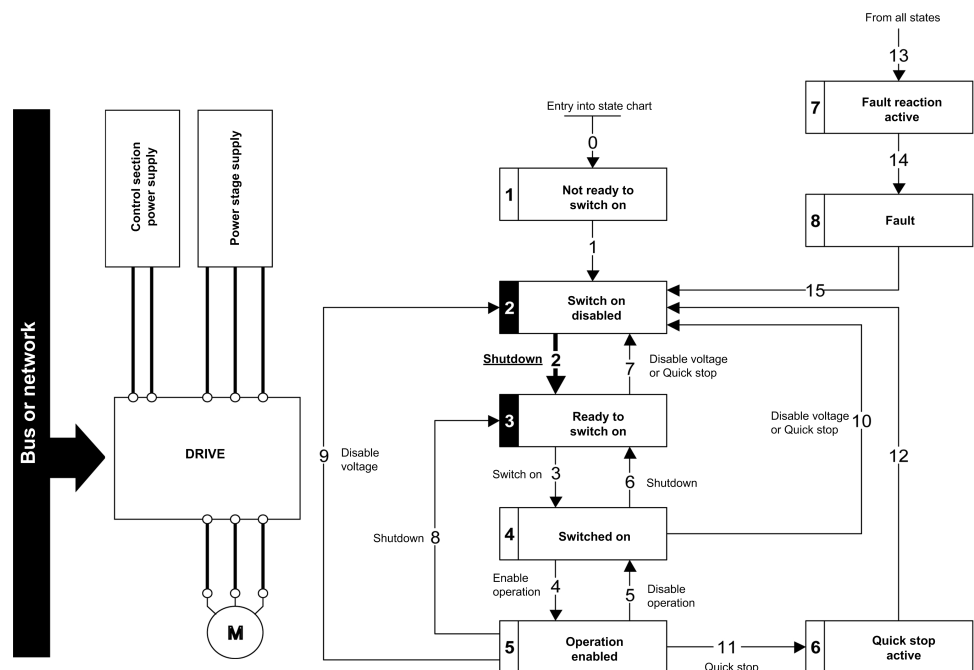
Power is supplied separately to the power and control stages.

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

The following sequence must be applied:

Step 1

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

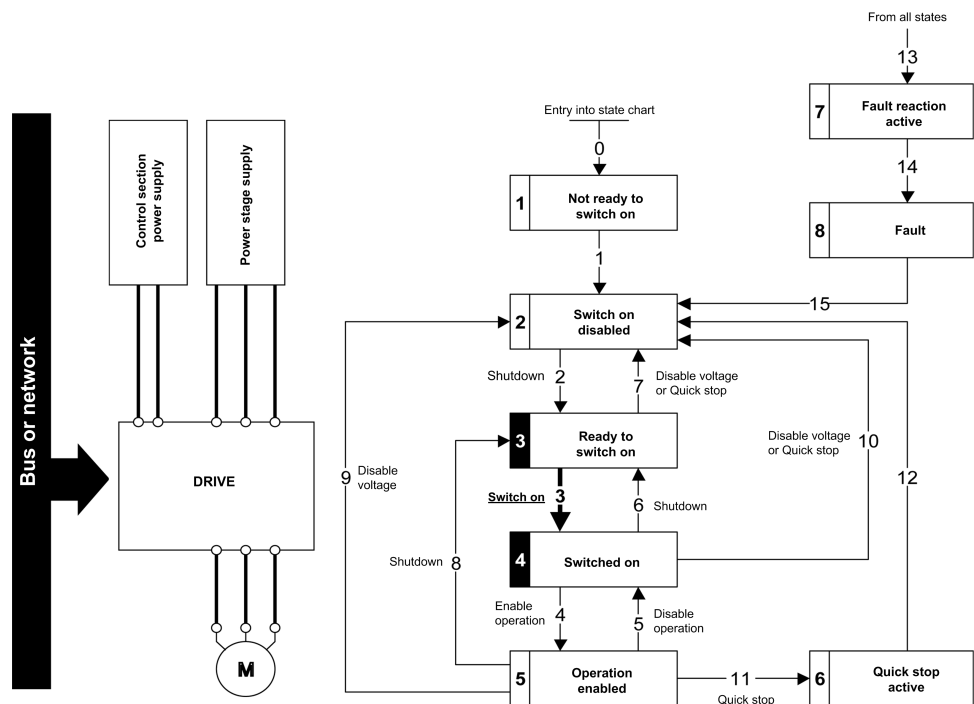


Step 2

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

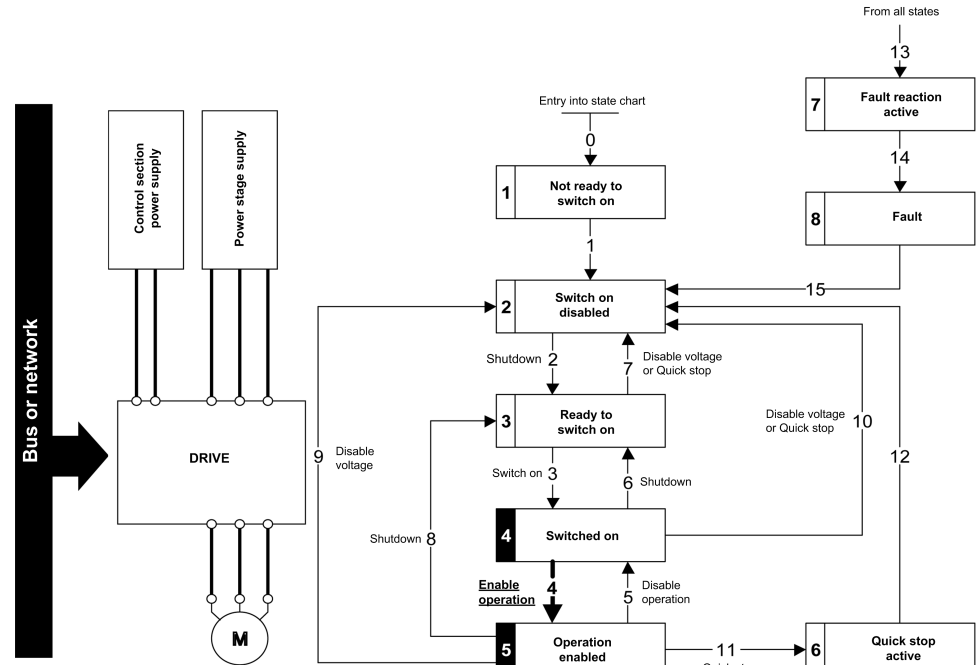
Power Stage Supply	HMI Panel	Status Word
Not present	[No Mains Voltage] NLP	21 hex
Present	[Ready] RDY	31 hex

- Apply the 3 - *Switch on* command



Step 3

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



Starting Sequence for a Drive with Mains Contactor Control

Description

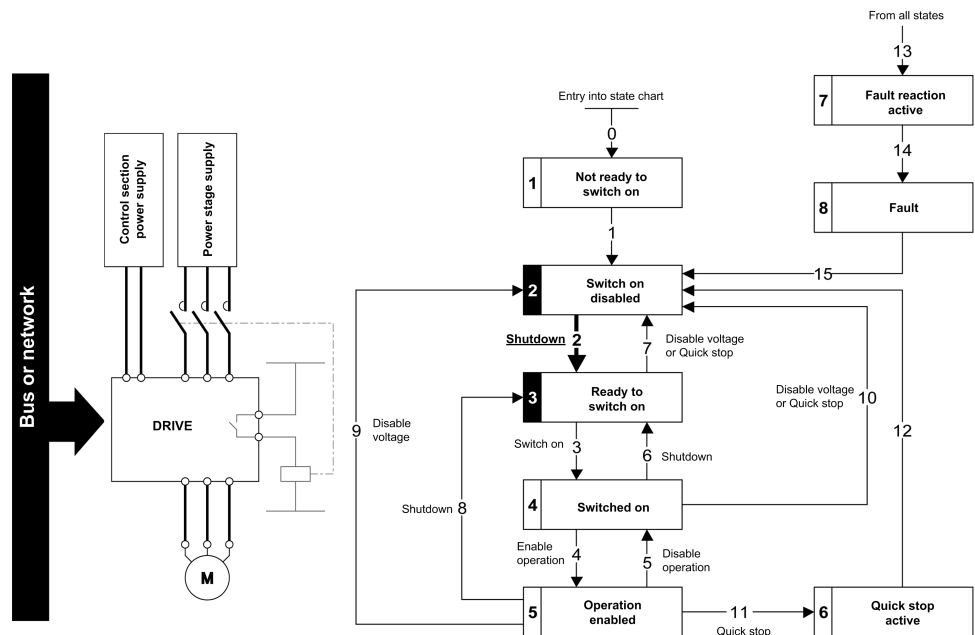
Power is supplied separately to the power and control stages.

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

The following sequence must be applied:

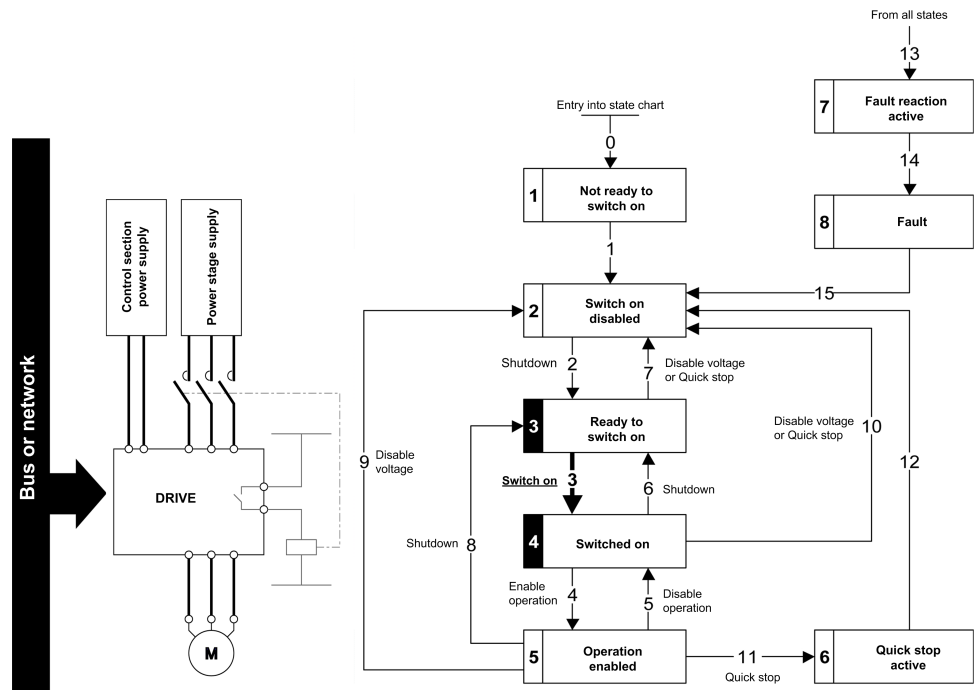
Step 1

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



Step 2

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

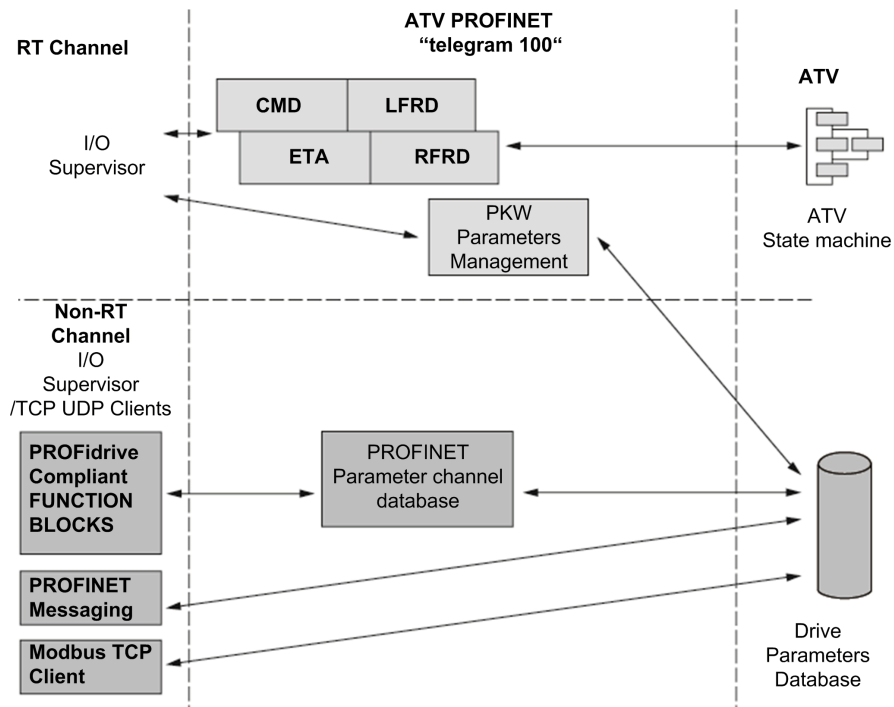


Description Telegram 100, 101, 102, 106, 107

Overview

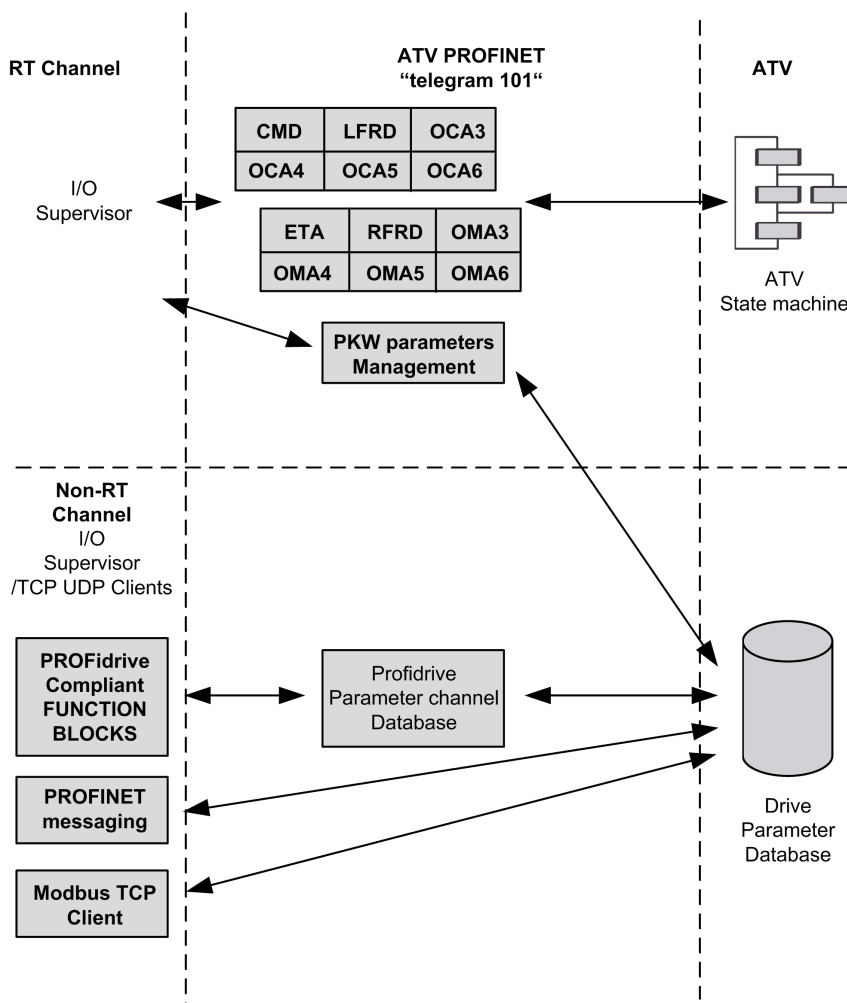
The telegrams 100,101, 102, 106, 107 are compliant with the native mode (CIA402 native drive profile).

The following diagram shows the native modes for telegram 100:

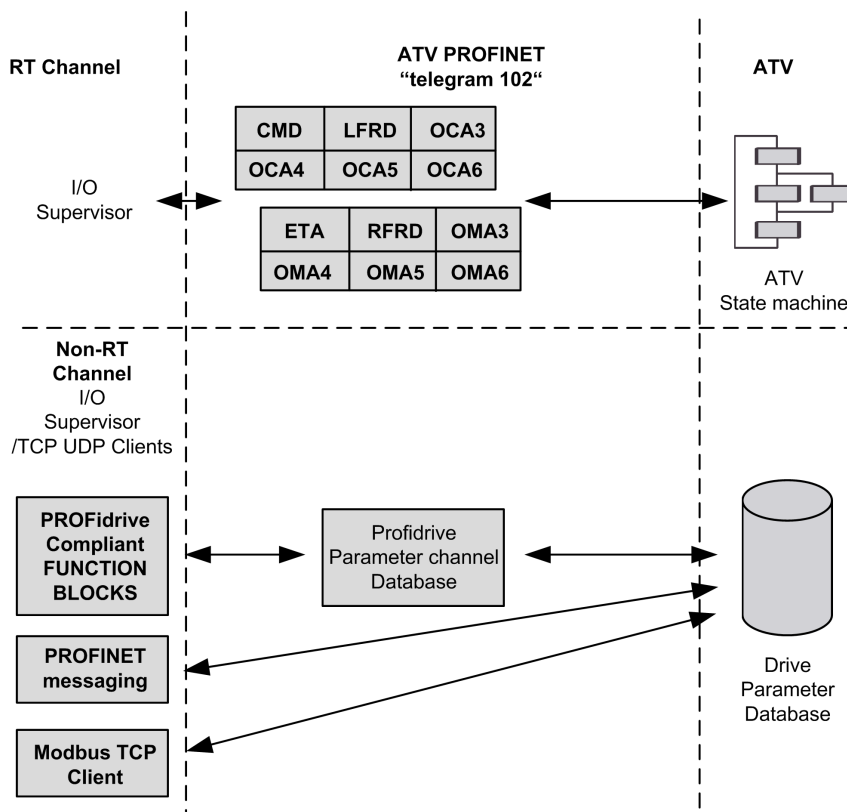


The PKW area of telegram 100, which is used for a simple parameter management, is compliant with the PKW mechanism used with the module.

The following diagram shows the native modes for telegram 101, 106, 107:



The following diagram shows the native modes for telegram 102:



Periodic Exchanges

The following table provides the details of telegram 100, 101, and 102

	Telegram 100		Telegram 101		Telegram 102	
	PLC>VSD	VSD>PLC	PLC>VSD	VSD>PLC	PLC>VSD	VSD>PLC
PKW 1	PKE	PKE	PKE	PKE	-	
PKW 2	R/W	R/W	R/W	R/W		
PKW 3	PWE	PWE	PWE	PWE		
PKW 4	PWE	PWE	PWE	PWE		
Cyclic data 1	OCA1 address of CMD =8501*	OMA1 address of ETA =3201*	OCA1 address of CMD =8501*	OMA1 address of ETA =3201*	OCA1 address of CMD =8501*	OMA1 address of ETA =3201*
Cyclic data 2	OCA2 address of LFRD =8602*	OMA2 address of RFRD =8604*	OCA2 address of LFRD =8602*	OMA2 address of RFRD =8604*	OCA2 address of LFRD =8602*	OMA2 address of RFRD =8604*
Cyclic data 3			OCA3 default =0	OMA3 default =0	OCA3 default =0	OMA3 default =0
Cyclic data 4			OCA4 default =0	OMA4 default =0	OCA4 default =0	OMA4 default =0
Cyclic data 5			OCA5 default =0	OMA5 default =0	OCA5 default =0	OMA5 default =0
Cyclic data 6			OCA6 default =0	OMA6 default =0	OCA6 default =0	OMA6 default =0
*:default Modbus address.						

The following table provides the details of telegram 106 and 107

	Telegram 106		Telegram 107	
	PLC>VSD	VSD>PLC	PLC>VSD	VSD>PLC
PKW 1	PKE	PKE	PKE	PKE
PKW 2	R/W	R/W	R/W	R/W
PKW 3	PWE	PWE	PWE	PWE
PKW 4	PWE	PWE	PWE	PWE
Cyclic data 1	OCA1 address of CMD =8501*	OMA1 address of ETA =3201*	OCA1 address of CMD =8501*	OMA1 address of ETA =3201*
Cyclic data 2	OCA2 address of LFRD =8602*	OMA2 address of RFRD =8604*	OCA2 address of LFRD =8602*	OMA2 address of RFRD =8604*
Cyclic data 3	OCA3 default =0	OMA3 default =0	OCA3 default =0	OMA3 default =0
Cyclic data 4	OCA4 default =0	OMA4 default =0	OCA4 default =0	OMA4 default =0
Cyclic data 5	OCA5 default =0	OMA5 default =0	OCA5 default =0	OMA5 default =0
Cyclic data 6	OCA6 default =0	OMA6 default =0	OCA6 default =0	OMA6 default =0
Cyclic data 7	OCA7 default =0	OMA7 default =0	OCA7 default =0	OMA7 default =0
Cyclic data 8	OCA8 default =0	OMA8 default =0	OCA8 default =0	OMA8 default =0
Cyclic data 9			OCA9 default =0	OMA9 default =0
Cyclic data 10			OCAA default =0	OMAA default =0
Cyclic data 11			OCAB default =0	OMAB default =0
Cyclic data 12			OCAC default =0	OMAC default =0
Cyclic data 13			OCAD default =0	OMAD default =0
Cyclic data 14			OCAE default =0	OMAE default =0
Cyclic data 15			OCAF default =0	OMAF default =0
Cyclic data 16			OCAG default =0	OMAG default =0
*:default Modbus address.				

The configuration of the cyclic data is made with the PROFINET IO controller configuration tool. The Modbus address of the parameter linked to each cyclic data must be defined as in the following example with the HW configuration software:

Input cyclic data 1/2 and output cyclic data 1/2 are already preconfigured to **[Cmd Register]** **CMD** (8501) and **[Speed Setpoint]** **LFRD** (8602); **[Status Register]** **ETA** (3201) and **[Output Velocity]** **RFRD** (8604).

If a null address Modbus is entered, no link between the related cyclic data and the drive is established. In any case, the 6 cyclic data are not disabled and the 6 cyclic data takes place in the I/O memory image of the controller.

Telegram 101 (4PKW/6PZD)_1 [Telegram 101 (4PKW/6PZD)]

General	IO tags	System constants	Texts																																																
<div> <div> General Catalog information Module parameters I/O addresses </div> <div> Module parameters General configuration </div> </div>																																																			
<table> <tr> <td>OCA1_TYPE:</td> <td>Output Data Word (16 Bits)</td> </tr> <tr> <td>OCA1_ADDRESS:</td> <td>8501</td> </tr> <tr> <td>OCA2_TYPE:</td> <td>Output Data Word (16 Bits)</td> </tr> <tr> <td>OCA2_ADDRESS:</td> <td>8602</td> </tr> <tr> <td>OCA3_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OCA3_ADDRESS:</td> <td>0</td> </tr> <tr> <td>OCA4_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OCA4_ADDRESS:</td> <td>0</td> </tr> <tr> <td>OCA5_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OCA5_ADDRESS:</td> <td>0</td> </tr> <tr> <td>OCA6_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OCA6_ADDRESS:</td> <td>0</td> </tr> <tr> <td>OMA1_TYPE:</td> <td>Input Data Word (16 Bits)</td> </tr> <tr> <td>OMA1_ADDRESS:</td> <td>3201</td> </tr> <tr> <td>OMA2_TYPE:</td> <td>Input Data Word (16 Bits)</td> </tr> <tr> <td>OMA2_ADDRESS:</td> <td>8604</td> </tr> <tr> <td>OMA3_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OMA3_ADDRESS:</td> <td>0</td> </tr> <tr> <td>OMA4_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OMA4_ADDRESS:</td> <td>0</td> </tr> <tr> <td>OMA5_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OMA5_ADDRESS:</td> <td>0</td> </tr> <tr> <td>OMA6_TYPE:</td> <td>Not Used</td> </tr> <tr> <td>OMA6_ADDRESS:</td> <td>0</td> </tr> </table>				OCA1_TYPE:	Output Data Word (16 Bits)	OCA1_ADDRESS:	8501	OCA2_TYPE:	Output Data Word (16 Bits)	OCA2_ADDRESS:	8602	OCA3_TYPE:	Not Used	OCA3_ADDRESS:	0	OCA4_TYPE:	Not Used	OCA4_ADDRESS:	0	OCA5_TYPE:	Not Used	OCA5_ADDRESS:	0	OCA6_TYPE:	Not Used	OCA6_ADDRESS:	0	OMA1_TYPE:	Input Data Word (16 Bits)	OMA1_ADDRESS:	3201	OMA2_TYPE:	Input Data Word (16 Bits)	OMA2_ADDRESS:	8604	OMA3_TYPE:	Not Used	OMA3_ADDRESS:	0	OMA4_TYPE:	Not Used	OMA4_ADDRESS:	0	OMA5_TYPE:	Not Used	OMA5_ADDRESS:	0	OMA6_TYPE:	Not Used	OMA6_ADDRESS:	0
OCA1_TYPE:	Output Data Word (16 Bits)																																																		
OCA1_ADDRESS:	8501																																																		
OCA2_TYPE:	Output Data Word (16 Bits)																																																		
OCA2_ADDRESS:	8602																																																		
OCA3_TYPE:	Not Used																																																		
OCA3_ADDRESS:	0																																																		
OCA4_TYPE:	Not Used																																																		
OCA4_ADDRESS:	0																																																		
OCA5_TYPE:	Not Used																																																		
OCA5_ADDRESS:	0																																																		
OCA6_TYPE:	Not Used																																																		
OCA6_ADDRESS:	0																																																		
OMA1_TYPE:	Input Data Word (16 Bits)																																																		
OMA1_ADDRESS:	3201																																																		
OMA2_TYPE:	Input Data Word (16 Bits)																																																		
OMA2_ADDRESS:	8604																																																		
OMA3_TYPE:	Not Used																																																		
OMA3_ADDRESS:	0																																																		
OMA4_TYPE:	Not Used																																																		
OMA4_ADDRESS:	0																																																		
OMA5_TYPE:	Not Used																																																		
OMA5_ADDRESS:	0																																																		
OMA6_TYPE:	Not Used																																																		
OMA6_ADDRESS:	0																																																		

Configuring the drive with TIA Portal

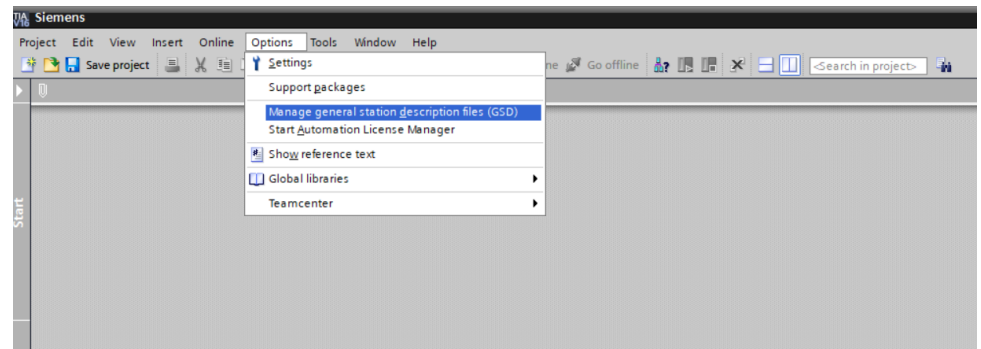
GSDML Installation

First download, and install the GSDML file of the drive in the hardware configuration tool of the TIA Portal software.

NOTE: SIMATIC STEP7® is supported by TIA Portal.

You can find the GSDML file and its associated picture on www.se.com.

From the menu > **Options > Install GSD File...**

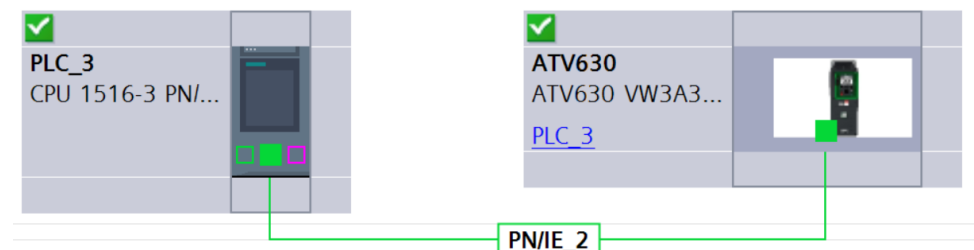


Configuration of a drive with the Telegram 100

Description

With this telegram, the drive is controlled with two process data.

Configure the PLC and its PROFINET network. Then select and place the drive from the library to the bus:



Define the addresses of the cyclic data (PZD) and PKW data in the PLC periphery:

Device overview									
Module	Rack	Slot	I address	Q address	Type	Article no.	Firmware	Comment	
ATV630	0	0			ATV630 VW3A3647	ATV630			
Interface	0	0 X1			ATV630				
Telegram 100 (4PKW2PZD)_1	0	1	0...11	0...11	Telegram 100 (4PKW2PZD)				

By default, the process data are linked to **[Cmd Register]** **CMD**, **[Speed Setpoint]** **LFRD**, **[Status Register]** **ETA** and **[Output Velocity]** **RFRD** (native CiA 402 profile of the drive).

Check that the exchanges are working properly with the **Watch and force tables**:

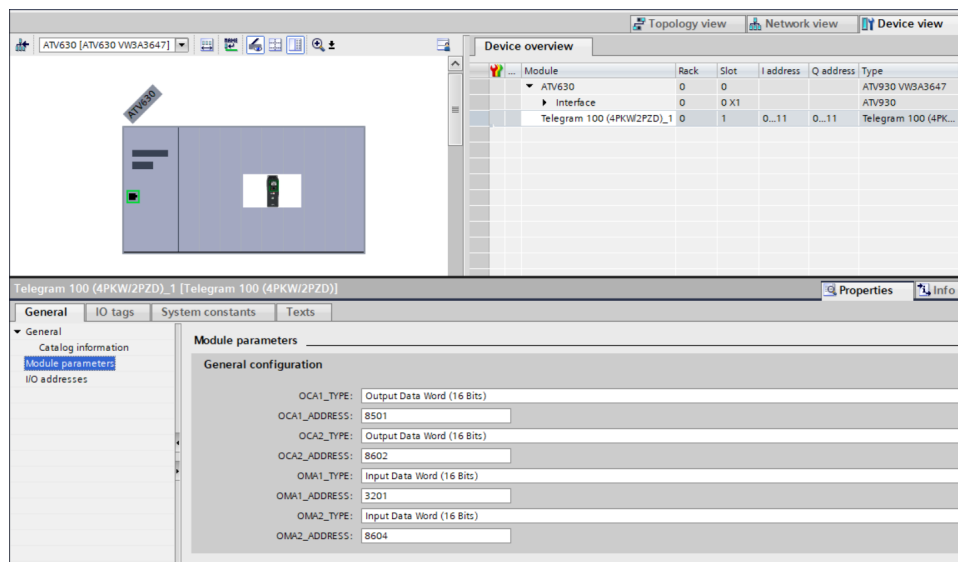
Options					
CPU operator panel					
Name	Address	Display format	Monitor value	Modify value	
1 "ETA"	%IWB	Hex	16#0250		
2 "RFRD"	%IWI0	Hex	16#0000		
3 "CMD"	%QWB	Hex	16#0000		
4 "LFRD"	%QWI0	Hex	16#0000		
5	<Add new>				

Configuring a drive with the Telegram 101, 102, 106, or 107

Configuring the drive Communication Scanner

The configuration of the fieldbus module is defined by the controller, by default the 2 first read and write are linked to the default parameters: **[Cmd Register]** *CMD*, **[Speed Setpoint]** *LFRD*, **[Status Register]** *ETA* and **[Output Velocity]** *RFRD*. The 4 next read or write parameters are not configured.

To add new parameters or modify the default configuration of the communication scanner, open the properties dialog box of the device and configure the OCA/OMA values in the parameter assignment tab.



New parameters are added or modified by entering the drive Modbus address.

For example: *ACC* is configured to read the value of **[Acceleration]** *ACC*, which Modbus address is 9001.

Parameters Management with the Telegram 100, 101, 102, 106, 107

Description

In native modes several accesses to the drive parameters are possible:

- The standard acyclic requests from drive profile, for more information see [Drive Parameters Channel](#), page 25.
- PKW mechanisms for 16-bit data and 32-bit data.

Parameter Management Through the PKW Area

With telegram 100, 101, 106, 107 you can read or write any drive parameter by using this PKW area. (This addressing format is identical to the PKW mechanism).

NOTE: The management of the parameters using PKW area is a mechanism implemented by Schneider Electric

NOTE: Drive parameters can be accessed through acyclic requests as defined in the drive profile standard.

The PKW area is made of four input words and four output words.

The table lists the controller-to-drive parameters in the input PKW area:

PKW Number	PKE Name	Description
PKW1	PKE	The Modbus address of the parameter is detailed here.
PKW2	R/W	Request code: 0: no request 1: read 2: write (16 bit) 3: write (32 bit)
PKW3	PWE	Parameter is used when PKW2 = 3
PKW4	PWE	Parameter value in case of write request

The table lists the drive-to-controller parameters in the output PKW area:

PKW Number	PKE Name	Description
PKW1	PKE	Copy of the input PKE
PKW2	R/W	Response code: 0: no request 1: read done (16 bit) 2: write done (16 bit) 3: request in progress 4: read done (32 bit) 5: write done (32 bit) 7: read or write error
PKW3	PWE	Parameter is used when PKW2 = 4 or 5
PKW4	PWE	If the request is successful, the parameter value is copied here.

Operations

Operating States

Configuring Communication Error Response

⚠ WARNING

LOSS OF CONTROL

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

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

Description

The response of the drive in the event of an Profinet communication interruption can be configured. Configuration can be performed using the display terminal from:

[Complete settings] CST- → **[Error/Warning handling]** CSWM- → **[Communication Module]** COMO- → **[Fieldbus Interrupt Resp]** CLL.

The values of the **[Fieldbus Interrupt Resp]** CLL parameter, which triggers a transition to the operating state fault are:

Value	Meaning
[Freewheel Stop] NST	Freewheel stop (factory setting)
[Ramp Stop] RMP	Stop on ramp
[Fast stop] FST	Fast stop
[DC injection] DCI	DC injection stop

The values of the **[Fieldbus Interrupt Resp]** CLL parameter, which does not trigger a transition to the operating state fault are:

Value	Meaning
[Ignore] NO	Detected error ignored
[Per STT] STT	Stop according to configuration of [Type of stop] STT
[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 maintained] 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

The fallback speed can be configured in:

[Complete settings] CST- → **[Error/Warning handling]** CSWM- → **[FallbackSpeed]** LFF parameter.

⚠ WARNING

LOSS OF CONTROL

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

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

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

Operating Modes

Configuring the Control Channel

Overview

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

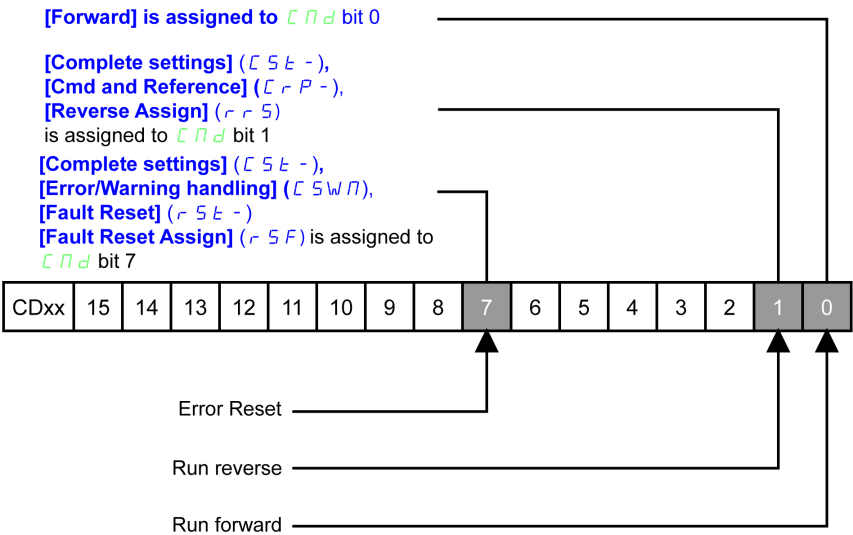
- I/O mode - a simple command word (based on forward, reverse, and reset binary commands).
- Combined mode (with native profile CiA 402) - Both reference value and command word come from the communication network.
- Separate (with native profile CiA 402) - reference value and command word come from separate 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

Description

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	[Com. Module] NET

The bits of the command word can now be configured.

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

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

In [Error/Warning handling] **CSWm** → [Fault reset] **RST-**, configure:

[Fault Reset Assign] RSF	[CD07] CD07
---------------------------------	--------------------

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

Description

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 ➔ **[Command and Reference]** **CRP**-submenu :

- Check if **[Ref Freq 1 Config]** **FR1** is set on according to the communication source (PROFINET: **[Com. Module]** **NET**).
- **[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.

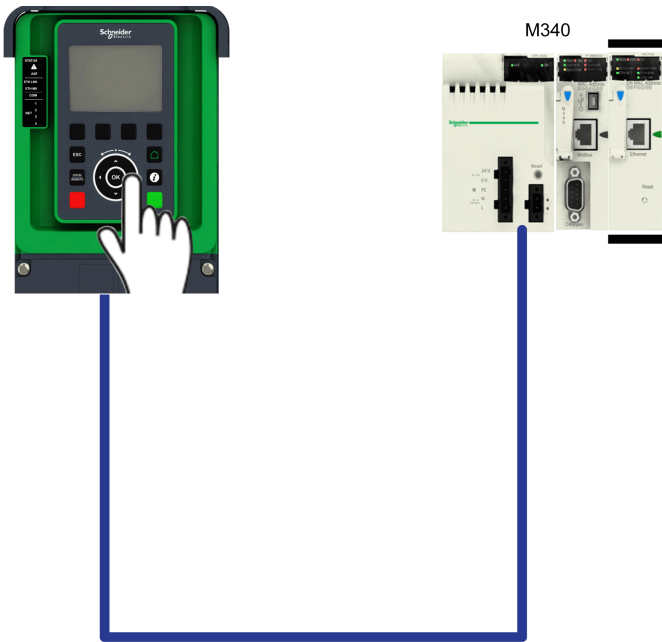
Profile	Ref1 Channel setting
CiA 402 combined mode	[Not separ.] SIM
CiA 402 separate mode	[Separate] SEP
I/O profile	[I/O profile] IO

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

Description

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:

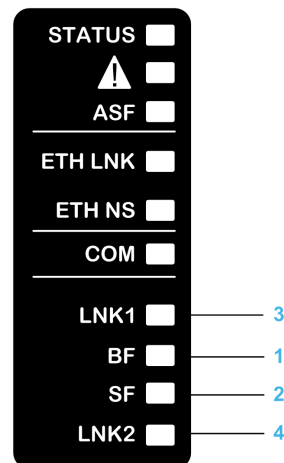
[Ref Freq 1 Config] FR1	[Ethernet] ETH
[Reverse Disable] RIN	Default
[Stop Key Enable] PST	Default
[Control Mode] CHCF	[Separate] SEP
[Command Switching] CCS	Default
[Cmd channel 1] CD1	[Com. Module] NET

Diagnostics and Troubleshooting

Fieldbus Status LEDs

LED Indicators

The following figure describes the LEDs status module:



LED Description

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

LNK1 and LNK2

These LEDs indicate the status of the Ethernet adapter ports:

Color & status	Description
OFF	No link
Blinking Green/ Yellow	Power on testing
Green ON	Link established at 100 Mbit/s
Yellow ON	Link established at 10 Mbit/s
Blinking Green	Fieldbus activity at 100 Mbit/s
Blinking Yellow	Fieldbus activity at 10 Mbit/s

Module Status

This LED indicates the module status:

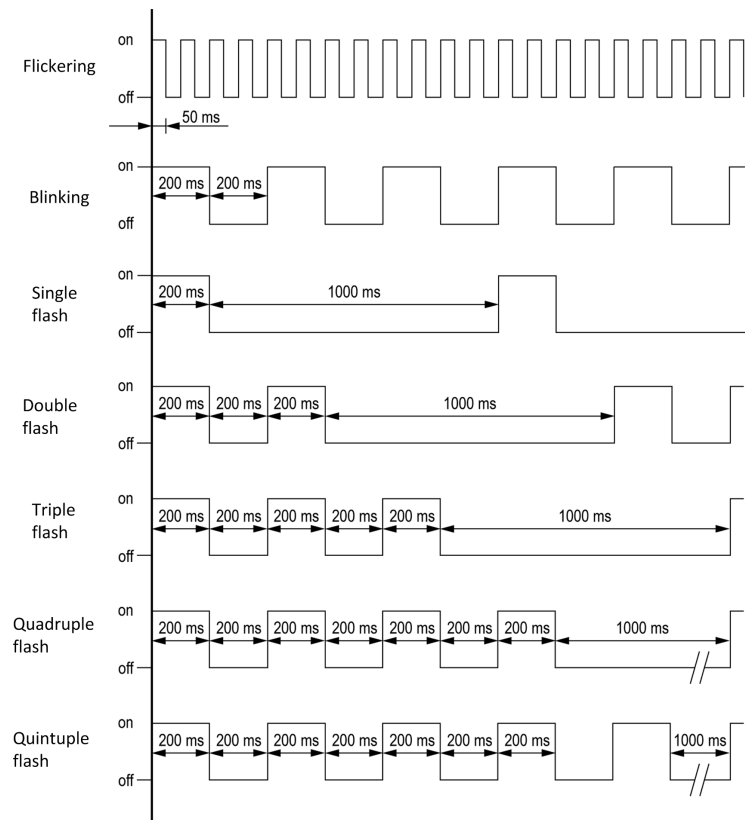
Color & Status	Description
OFF	The device is powered off
Red ON	The device has detected an ILF error
Green ON	The device is ready and operational
Red flickering	The device has detected a communication interruption / wrong configuration or a PROFINET controller at <code>Stop</code> state.
Green flickering	In combination with other LEDs: DCP manual identification phase / DCP flash mode
Green/Red blinking	Power up testing
Red single flash	No connection to the PROFINET controller

Network Error Status

Color & Status	Description
OFF	The device does not have an IP address or is powered off
RED ON	Error detected on the module
Green ON	At least a port is connected and has a valid IP address.
Green flickering	In combination with other LEDs: DCP manual identification phase / DCP flash mode or as long as the iPar-Client did not accomplish transfer (backup or restore) its parameters
Green/Red blinking	Power-up testing
Green flashing 3 times	All ports are unplugged, but the module has an IP address
Green flashing 4 times	Error detected: duplicate IP address
Green flashing 5 times	The module is performing a DHCP sequence

NOTE: If the fieldbus module operates as a Modbus TCP server only, LED 1 and 2 have another behavior.

LED Behavior



Connection problem with the fieldbus module

Description

If the product cannot be addressed via the fieldbus, first check the connections. The product manual contains the technical data of the device and information on fieldbus and device installation.

Verify the following:

- Power connections to the device.
- Fieldbus cable and fieldbus wiring.
- Fieldbus connection to the device.

Fieldbus Response Test

Description

If the connections are correct, check the settings for the fieldbus addresses. After correct configuration of the transmission data, test the fieldbus mode.

In addition to the controller that knows the device via the data in the GSDML file and its address, a bus monitor should be installed. As a passive device, it can display messages.

- Switch off or on the supply voltage of the drive system.
- Observe the network messages shortly after switching on the drive. A bus monitor can be used to record the elapsed time between telegrams and the relevant information in the telegram.

Possible Errors: Addressing, Parameterization, Configuration

If it is impossible to connect to a device, check the following:

- Addressing: The address of the network device must be a valid IP address. Each network device must have a unique address.
- Parameterization: The parameterized ident number and the user parameters must match the values stored in the GSDML file.

Communication Interruption

Description

The drive triggers an error **[Internal Link Error] ILF** when the following events occur:

- Hardware error is detected on the PROFINET module
- Communication interruption between the PROFINET module and the drive

The response of the drive in the event of an **[Internal Link Error] ILF** error cannot be configured, and the drive stops in freewheel. This detected error requires a power reset.

The diagnostic parameter can be used to obtain more detailed information about the origin of the **[Internal Link Error] ILF** (**[InternCom Error1] ILF1** if the detected error has occurred on fieldbus module in slot A).

The **[InternCom Error1] ILF1** parameter can be accessed on the graphic display terminal in **[Communication] COMO** → **[Communication map] CMM** → **[PROFINET DIAG] PRN**

Value	Description of the values of the [Internal Link Error] ILF parameter
0	No error detected
1	Internal communication interruption with the drive
2	Hardware error detected
3	Error found in the EEPROM checksum
4	EEPROM
5	Flash memory
6	RAM memory
7	NVRAM memory
101	Unknown module
102	Communication interruption on the drive internal bus
103	Time out on the drive internal bus (500 ms)

[Fieldbus Com Interrupt] \overline{L} \overline{n} \overline{F}



Probable Cause

Communication interruption on fieldbus module.

This error is triggered when the communication between the fieldbus module and the master (PLC) is interrupted.



Remedy

- Verify the environment (electromagnetic compatibility).
- Verify the wiring.
- Verify the timeout.
- Deactivate the "Autonegotiation" in TIA Portal.
- Replace the option module.
- Contact your local Schneider Electric representative.



Clearing the Error Code

This detected error can be cleared with the **[Auto Fault Reset]** or manually with the **[Fault Reset Assign]** parameter after its cause has been removed.

[Internal Error 6] *INF 6*



Probable Cause

- The option module installed in the drive is not recognized.
- The removable control terminal modules (if existing) are not present or not recognized.
- The embedded Ethernet adapter is not recognized.
- The drive firmware is not compatible with the option module.
- Option module corrupted due to multiple firmware updates.



Remedy

- Verify the catalog number and compatibility of the option module.
- Plug the removable control terminal modules after the drive has been switched off.
- Update the drive firmware.
- Contact your local Schneider Electric representative.



Clearing the Error Code

This detected error requires a power reset.

Diagnostic (PROFINET Service)

Diagnostic

PROFINET diagnostic is associated with specific data which can be helpful during maintenance:

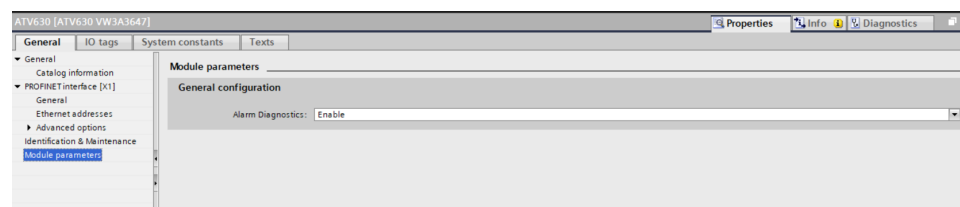
- The error code, if a detected error is present,
- The value of ETA operating state word,
- The value of the output frequency.

This data report and gives an indication on the drive status when the diagnostic event was triggered

Byte	Description	
1...28	Header information	Header information with interrupts from PROFINET IO in case of manufacturer-specific diagnostic.
29	Ext_Diag_Data	External diagnostic data length = 6
30		IF ETA.bit 3 = 1: ADL LFT LSB Otherwise: 0
31		ADL ETA LSB
32		ADL ETA MSB
33		LSB of the last value of the output speed
34		MSB of the last value of the output speed

Enabling Diagnostics

By default, alarm diagnostics function is enabled. It can be modified during the configuration phase as shown below:



Monitoring of Communication Channel

⚠ 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.

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 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, 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	CANopen	Fieldbus Module	Ethernet Embedded
Control word	CMD	CMD1	CMD2	CMD3	CMD5
Extended control word	CMI	CMI1	CMI2	CMI3	CMI5
Reference speed (rpm)	LFRD	LFRD1	LFRD2	LFRD3	LFRD5
Reference frequency (0.1 Hz)	LFR	LFR1	LFR2	LFR3	LFR5
Reference for torque control mode (0.1% of the normal torque) ⁽¹⁾	LTR	LTR1	LTR2	LTR3	LTR5
Reference value supplied by PI controller	PISP	PISP1	PISP2	PISP3	PISP5
Reference value supplied by analog multiplier function	MFR	MFR1	MFR2	MFR3	MFR5
⁽¹⁾ : If available					

Network Monitoring Criteria

The table provides the details of the detected errors

Protocol	Criteria	Error Code
PROFINET module	10: No valid IP	[Fieldbus Error]
	9: Duplicated IP address	
	12: iPar unconfigured	
	13: iPar unrecoverable error detected	
	0: No error detected	[Fieldbus Com Interrupt]
	1: Network timeout (configurable timeout) for received requests destined for the drive	
	EEPROM detected error	[Internal Link Error]

Control-Signal Diagnostics

Introduction

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

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

Control Word Display

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

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

The **[Command word image]** **CWI** submenu (**[COM. Module cmd.]** **CMD3**) parameter is used to display the hexadecimal value of the control word from the fieldbus.

Reference Frequency Display

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

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

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

Operating State Word Display

The **[Status Register]** **ETA** parameter gives the value of the operating state word (ETA).

The table provides the bit details of **[Status Register]** **ETA** parameter:

Bit	Description
DRIVECOM	Status word
Bit0 = 1	Ready to switch on
Bit1 = 1	Switched on
Bit2 = 1	Operation enabled
Bit3 = 1	Operating state fault
Bit4 = 1	Power stage is switched on
Bit5 = 0	Quick stop active
Bit6 = 1	Switch on disabled
Bit7 = 1	Warning
Bit8 = 1	Drivecom reserved
Bit9 = 0	Forced local mode in progress
Bit10 = 1	Reference value reached (steady state)
Bit11 = 1	Reference value exceeded (< LSP or > HSP)
Bit12	Reserved
Bit13	Reserved
Bit14 = 1	Stop imposed via STOP key
Bit15 = 0	Motor rotation in forward direction (or stopped)

Glossary

A

Abbreviations:

Req. = Required

Opt. = Optional

AC:

Alternating Current

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

C

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

D

DC:

Direct Current

dec.:

Decimal

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. Further information can be found in the pertinent standards such as IEC 61800-7, ODVA Common Industrial Protocol (CIP).

H

hex:

Hexadecimal

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.

PWM:

Pulse Width Modulation.

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.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

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

© 2023 Schneider Electric. All rights reserved.

BQT466190.01 — 12/2023