Altivar Soft Starter ATS480

Soft Starter for Asynchronous Motors

Embedded Modbus RTU Manual

NNZ85539.02
04/2022

www.se.com

Legal Information

Table of Contents

Safety Information

Important Information

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

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

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

⚠ DANGER

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

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

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

Please Note

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

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

Qualification of Personnel

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

Intended Use

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

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

Product related information

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

⚠⚠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 equipment.
- 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 equipment, block the motor shaft to prevent rotation.
- Insulate both ends of unused conductors of the motor cable.

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 equipment:

- Use all required personal protective equipment (PPE).
- 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 equipment.
- Lock all power switches in the open position.
- Verify the absence of voltage using a properly rated voltage sensing device.

Before applying voltage to the equipment:

- 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.

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- Never operate energized switch with door open.
- Turn off switch before removing or installing fuses or making load side connections.
- Do not use renewable link fuses in fused switches.

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

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

⚠⚠DANGER

ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION

Do not use damaged products or accessories.

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

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

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

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

The present document assumes that you are fully aware of all normative standards and requirements that apply to your application. Since the soft starter 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.
- 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.

The products 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

⚠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.

This product meets the EMC requirements according to the standard CEI 60947-4-1. This device has been designed for environment A. Use of this product in a domestic environment (B environment) may cause unwanted radio interference.

⚠⚠WARNING

RADIO INTERFERENCE

- In a domestic environment (B environment), this product may cause radio interference in which case supplementary mitigation measures may be required.
- The references from ATS480D17Y to ATS480C11Y can be adapted to a domestic environment (B environment) by adding an external bypass contactor. For other ATS480 references, you must consider other mitigation measures.

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

NOTICE

DESTRUCTION DUE TO INCORRECT MAINS VOLTAGE

Before switching on and configuring the product, verify that it is approved for the mains voltage.

Failure to follow these instructions can result in 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 onto the market.

This documentation is valid only for ATS480.

The characteristics that are presented in this manual should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the manual and online information, use the online information as your reference.

The technical characteristics of the devices described in the present document also appear online. To access the information online:

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. • 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.**

Document Scope

The purpose of this document is to:

- Show you how to connect the Modbus RTU fieldbus on your soft starter.
- Show you how to configure the soft starter to use the Modbus RTU embedded for monitoring and control.
- Provide examples of setup using Modbus RTU communication.

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

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:

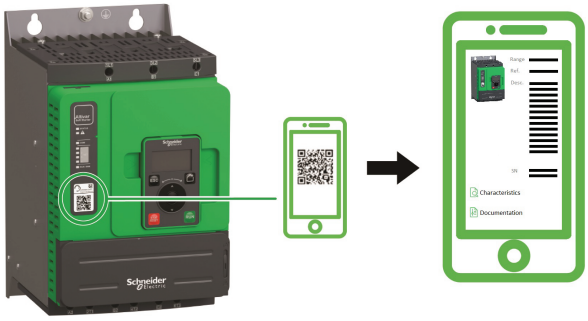
- The whole catalog for detailed characteristics and selection guides
- The CAD files to help design your installation, available in over 20 different file formats
- All software and firmware to maintain your installation up to date
- A large quantity of White Papers, Environment documents, Application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

Title of documentation	Catalog number
Catalog: Altivar Soft Starter ATS480	DIA2ED2210602EN (English), DIA2ED2210602FR (French), DIA2ED2210602CN (Chinese), DIA2ED2210602DE (German), DIA2ED2210602IT (Italian), DIA2ED2210602SP (Spanish), DIA2ED2210602PTBR (Brazilian Portuguese), DIA2ED2210602TR (Turkish)
ATS480 Getting Started Manual	NNZ85504 (English), NNZ85505 (French), NNZ85506 (Spanish), NNZ85507 (Italian), NNZ85508 (German), NNZ85509 (Chinese), NNZ85510 (Portuguese), NNZ85511 (Turkish)
ATS480 Getting Started Manual Annex for UL	NNZ86539 (English)
ATS480 User Manual	NNZ85515 (English), NNZ85516 (French), NNZ85517 (Spanish), NNZ85518 (Italian), NNZ85519 (German), NNZ85520 (Chinese), NNZ85521 (Portuguese), NNZ85522 (Turkish)
ATS48 to ATS480 Substitution Manual	NNZ85529 (English), NNZ85530 (French), NNZ85531 (Spanish), NNZ85532 (Italian), NNZ85533 (German), NNZ85534 (Chinese), NNZ85535 (Portuguese), NNZ85536 (Turkish)
ATS480 Embedded Modbus RTU Manual	NNZ85539 (English)
ATS480 EtherNet/IP – Modbus TCP Manual VW3A3720	NNZ85540 (English)
ATS480 PROFIBUS DP Manual VW3A3607	NNZ85542 (English)
ATS480 CANopen Manual VW3A3608, VW3A3618, VW3A3628	NNZ85543 (English)
ATS480 Communication Parameter Addresses	NNZ85544 (English)
ATS480 Cascade Function Application Note	NNZ85564 (English)
SoMove: FDT	SoMove FDT (English, French, German, Spanish, Italian, Chinese)
ATS480: DTM	ATS480 DTM Library EN (English – to be installed first), ATS480 DTM Lang FR (French), ATS480 DTM Lang SP (Spanish), ATS480 DTM Lang IT (Italian), ATS480 DTM Lang DE (German), ATS480 DTM Lang CN (Chinese)
EcoStruxure Automation Device Maintenance	EADM (English)
Recommended Cybersecurity Best Practices	CS-Best-Practices-2019–340 (English)

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

Electronic product data sheet

Scan the QR code in front of the soft starter to get the product data sheet.



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 soft starters 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:

European standards:

- IEC 60947–1 Low–Voltage Switchgear and Control Gear – General rules
- IEC 60947–4-2 Semiconductor Motor controllers, Starters and Soft Starters
- IEC 60529 Degrees of protection provided by enclosures (IP Code) Safety of machinery – Electrical equipment of machines – General requirements
- IEC 60664–1 Insulation coordination for equipment within low-voltage supply systems – Principles, requirements, and tests
- IEC 61000–4–2/-4–3/4–4/4–5/4–6/4–11/4–12 Electromagnetic Compatibility
- IEC 60721–3 Classification of environmental conditions
- IEC 61131–2: Programmable controllers – Part 2: Equipment requirements and tests
- IEC 60068: Environmental testing
- IEC 61158 series: Industrial communication networks – Fieldbus specifications
- IEC 61784 series: Industrial communication networks – Profiles
- IEC 62443: Security for industrial automation and control systems

European Community directives:

- 86/188/EEC Protection of Workers for the Risks Related to Exposure to Noise at Work
- 2014/35/EU Low Voltage Directive
- 2014/30/EU EMC Directive
- 2006/42/EC Machine Directive

North American standards:

- UL 60947–4–2: Low–Voltage Switchgear and Control gear – Part 4-2: Contactors and Motor–Starters – AC Semiconductor Motor Controllers and Starters

Other standards:

- ISO 12100:2010: Safety of machinery – General principles for design – Risk assessment and risk reduction
- GB/T 14078.6-2016: Low—Voltage Switchgear and Control Gear - - Part 4-2: Contactors and motor starters - - AC Semiconductor Motor Controllers and Starters (including Soft Starters)
- IEC 61800-9-2: Adjustable speed electrical power drive systems – Part 9-2: Ecodesign for power drive systems, motor starters, power electronics and their driver applications – Energy efficiency indicators for power drive systems and motor starters

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

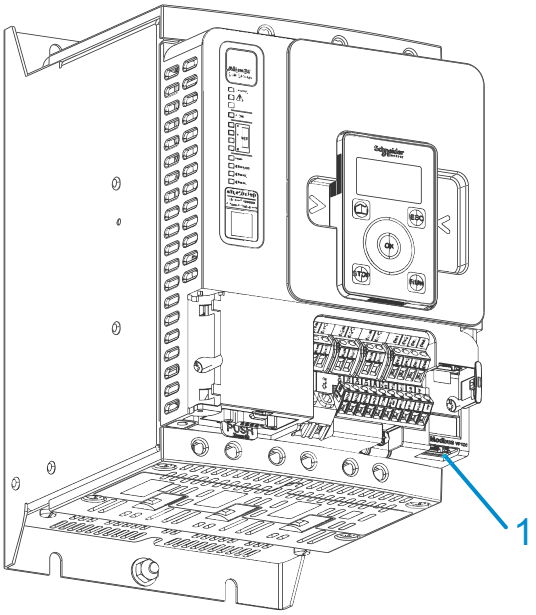
92500 Rueil-Malmaison

France

Presentation

Hardware Overview

General



1 Modbus RTU communication port

Software Overview

Supported Modbus Functions

The device supports the following Modbus functions:

Function Name	Code		Description	Remarks
	Dec.	Hex		
Read Holding Registers	03	03 hex	Read N output words	Maximum PDU length: 125 words
Write One Output Word	06	06 hex	Write 1 output word	–
Diagnostics	08	08 hex	Diagnostics	–
Write Multiple Registers	16	10 hex	Write N output word	Maximum PDU length: 123 words
Read/write Multiple Registers	23	17 hex	Read/write multiple registers	Maximum PDU length: 125 words (R), 121 words (W)
(Subfunction) *Read Device Identification*	43/14	2B hex/ 0E hex	Encapsulated interface transport/ Read device identification	–

Communication Parameter Addresses

For more information about the Communication Parameter Addresses, please refers to the ATS480 Communication Parameter Addresses NNZ85544, page 12.

Cybersecurity

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 odification 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 ATS480 upgrades are implemented consistently to the current version of firmware available on se.com.
- 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

NOTICE
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 equipment damage.**

Cybersecurity helps to provide:

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

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

From the norm definition, Altivar Soft Starter ATS480 is considered as Embedded Device of the ICS network, and has been designed following the norm IEC62443-4-1 and the technical security requirements are defined in compliance with norm IEC 62443-4-2.

Altivar Soft Starter ATS480 security features prevent the unauthorized disclosure of information via eavesdropping or casual exposure.

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 ATS480 are in complement of the points above.

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

NOTICE
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 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 ATS480 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

Altivar Soft Starter ATS480 offers the following security features:

Threats	Desired security property on Embedded Device	ATS480 security features
Information disclosure	Confidentiality	Password encrypted in a non-reversible way
		User access control
Tampering	Device integrity	Cryptographic signature of firmware package
		Secure root of trust
Denial of Service	Availability	Device backup/restore
		Security export/import
		Achilles Level 2
Spoofing/Elevation of privilege	User Authenticity / Authorization	Strong password policy
		Access control commissioning tools Modbus Serial
		Access control local Keypad
		Access control commissioning tools Modbus TCP
		Access control commissioning tools WebServer
Repudiation	Non-repudiability	Secure event logging

Confidentiality

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

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

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 ATS480 and facilitates protected file transfer: digitally signed firmware is used to help protect the authenticity of the firmware running on the ATS480 and only allows firmware generated and signed by Schneider Electric.

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

Availability

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

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

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

Communication robustness, the ATS480 Ethernet fieldbus 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 ATS480, 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 ATS480 controls the access through:

- SoMove DTM (Serial and Ethernet connection)
- The webserver (Ethernet option required)
- EcoStruxure Control Expert
- EADM (EcoStruxure Automation Device Maintenance)

Non Repudiation by Security Event Logging

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

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

- Machine and human-readable reporting options for current device security settings
- Audit event logs to identify:
  - The ATS480 configuration modification
  - The device users' activity (login, logout, etc...)
  - The device firmware updates
  - Audit storage capacity of 500 event logs by default
  - Timestamps, including date and time, match ATS480 clock

ATS480 Security Policy

To facilitate cybersecurity first configurations, the ATS480 offers 2 security profiles with preset ATS480 security features. This operation applies default values adapted to the security level targeted by the system of which the device is part.

Selection of these 2 security policies can be done upon first power up of the device, both with the display terminal, SoMove, DTM or EcoStruxure Control Expert.

Security Policy "Minimum"

This profile offers a minimum of cybersecurity features. The user access control (login & password check at connection) are disabled on SoMove, EADM, WebServer and EcoStruxure Control Expert.

Those connections remain unsecured and open for potential elevation of privilege. This profile is to be used for installation where authentication & authorization constraints are covered by access control mitigation external to the device.

When Minimum policy is selected, each user accessing the device is considered to have ADMIN role and privileges.

Security Policy "Advanced"

This profile presets the device security by enabling security features. The user access control is enabled for the web server, SoMove EADM and EcoStruxure Control Expert.

When activating the "Advanced" security policy, the user is identified as Admin and is requested to create a login and a password unique to the device.

A default password is displayed on the display terminal. It can be kept as it is or modified.

Refer to the following cybersecurity features summary per security profile:

ATS480 security feature	Open for configuration (activation or settings)	Preset security policy	
		Minimum	Advanced
Password encrypted in a non-reversible way	-	-	✓
User access control	-	-	✓
Cryptographic signature of firmware package	-	✓	✓
Secure root of trust	-	✓	✓
Device backup/restore	ADMIN only	✓	✓
Security export/import	ADMIN only	✓	✓
Achilles	-	✓	✓
User management	ADMIN only	-	✓
Strong password policy	ADMIN only	-	✓
Access control commissioning tools Modbus Serial	ADMIN only	-	✓
Access control commissioning tools Modbus TCP	ADMIN only	-	✓
Access control commissioning tools WebServer	ADMIN only	-	✓
Secure event logging	-	✓	✓

Import / Export Security Policy

The device security settings can be exported from a device to be archived and/or applied in the same or another device. The result of a security policy export consists in the creation of a security policy file. This file is identified with the extension .secp.

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

Security settings	Included in import / export operation
User access control settings	✓
Password policy	✓
User database, including username and password	✓
Password history, last 5 for each users	✓
Device default password	– For security reasons, the default password is unique to each device and cannot be exported
Security events	– The security events base is private property of a device and cannot be applied to another device

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.

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.

Initial Setup

Before using the device, it is mandatory to select a security policy, refer to the Chapter **Initial Setup** in the User Manual NNZ85515..

Password

Changing Password

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

Reset Password

The Altivar Soft Starter ATS480 stores password in a secure non-reversible format. It is impossible to retrieve a password that has been lost by his user.

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

To reset the ADMIN password:

Step	Action
1	Navigate to the menu **[Device Management]** DMT ➡ **[Cybersecurity]** CYBS
2	Scroll to the parameter **[Reset Password]** SRPW and press **OK**
3	The default password is visible on the graphic display terminal until the ADMIN modifies it.

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

Password Policy

By default, the password policy of the Altivar Soft Starter ATS480 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 (@ % + ‘ ! # “ $ ^ ? : , ( ) [ ] ~ _ . ; = & / \ – [SPACE])

In addition, for password changes, the password history is saved and prevents 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.

NOTE: Changing the User authentication security policy (elevation or reduction of privilege) will be taken into account:

- Upon next connection to the soft starter, if the Initial Setup connection is still open
- Immediately in other scenarios

Security Event Logging

The following time-stamped events are logged in a dedicated security log file:

- User authentications, authentication and logout attempts
- Security parameter changes
- Access to the security events
- Device reboot, startup
- Device hardware modifications and software updates
- Device Configuration Integrity changes (restore, download or factory settings)

The Altivar Soft Starter ATS480 can store up to 500 events, a warning is raised when the log base is reaching 90% of capacity. This warning can be acknowledged with SoMove. When the maximum capacity is reached, the oldest events are erased.

If access control is disabled, any security event is identified as ADMIN action.

Embedded Device provides the capability to determine whether a given human took a particular action. The link is established between the user identifier, the action realized and the timestamping of the action (date and time) to provide an efficient source of security logging.

Irrelevant date & time can result in false interpretation of the security event logging and lead to either false positive or undetectable security threat detection.

NOTICE
WRONG TIMESTAMPING RESULT IN NON-REPUDIATION ISSUE • Verify and regularly realign the synchronization of the device data & time. **Failure to follow these instructions can result in equipment damage.**

The security events can be read from SoMove, DTM and EcoStruxure Control Expert. For security reasons, security logs are stored in a database to which read-only access is provided. There is no possibility to edit or erase this log database.

The format system log record follows the syntax defined by Syslog RFC–5424 2009 and the semantic normalized by Schneider Electric.

Below is an example of this format:

<86>1 2022-01-24T09:59:53.06Z MyDevice ATS480 Credential USERACCOUNT_CHANGE [cred@3833 name="ADMIN"] Password changed

Elements from the example, from left to right	Syslog word	Description
<86>	PRI	Event priority (81 for alert events, 85 for notice events, 86 for informational events)
1	VERSION	Syslog protocol version
2022-01-24T09:59:53.06Z	TIMESTAMP	Date and time in UTC
MyDevice	HOSTNAME	Device name, or serial number if **[Device Name]** PAN is not defined
ATS480	APP–NAME	Product commercial reference
Credential	PROCID	Identify the process and the network protocol service that originated the message
USERACCOUNT_CHANGE	MSGID	Identify the type of event
[cred@3833 name="ADMIN"]	STRUCTURED–DATA • [authn@3833]	Event information depending on the event category: • Structured-data used for authentication events
	• [authz@3833]	• Structured-data used for authorization events
	• [config@3833]	• Structured-data used for configuration events
	• [cred@3833]	• Structured-data used for credential management events
	• [system@3833]	• Structured-data for events in the system that are not captured by other event types like operating mode state change or hardware failure
	• [backup@3833]	• Structured data used for backup
Password changed	MSG	Message containing event specific information, if any

Upgrades Management

When the Altivar Soft Starter ATS480 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 standards.

Clear Device / Secure Decommissioning

The device security policy can be totally erased. This operation is part of the device secure disposal use case executed during clear device operation.

Upon execution, security settings are totally erased form the device, including any internal backup, usernames, passwords and history.

For security reasons, it is strongly recommended to perform this operation while removing the device from its intended environment.

To erase the device security policy go to one of those menu:

- **[Device Management]** DMT ➡ **[Backup/Restore]** BRDV and scroll to **[Clear device]** CLR
- **[Device Management]** DMT ➡ **[Factory settings]** FCS and scroll to **[Clear device]** CLR

This parameter is visible in expert mode only. To active the expert mode go to the menu **[My preferences]** MYP ➡ **[Parameter access]** PAC and set **[Access Level]** LAC to **[Expert]** EPR.

Basics

Profile

Definition of a Profile

Types of Profiles

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
- ...

Application Profile

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

Interchangeability

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

Functional Profiles Supported by the Altivar Soft Starter

NOTE: The following document is valid if **[Control Mode]** CHCF is set to **[Standard Profile]** STD.

ATS48 Compatibility Profile

This profile allows to manage the compatibility with an Altistart ATS48.

To continue to use**[Control Mode]** CHCF set to **[SE8 Profile]** SE8, please refer to the ATS48 Modbus Manual.

About compatibility, some of Altistart ATS48 address parameters have particularities, so please refer to the ATS480 substitution manual (NNZ85529).

NOTE: [Control Mode] CHCF is set to **[SE8 Profile]** SE8 **(factory setting)**.

Standard Profile

To be in Standard Profile, **[Control Mode]** CHCF is set to **[Standard Profile]** STD.

The Standard Profile supported by the Altivar Soft Starter is based on the CiA402, which has been adapted to the characteristics of the Altivar Soft Starter and therefore to all communication ports.

The control word is compliant according to CiA402.

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

NOTE:

- Altivar Soft Starter starts up following a command sequence
- After switching on and when an operating mode is started, Altivar Soft Starter goes through several operating states

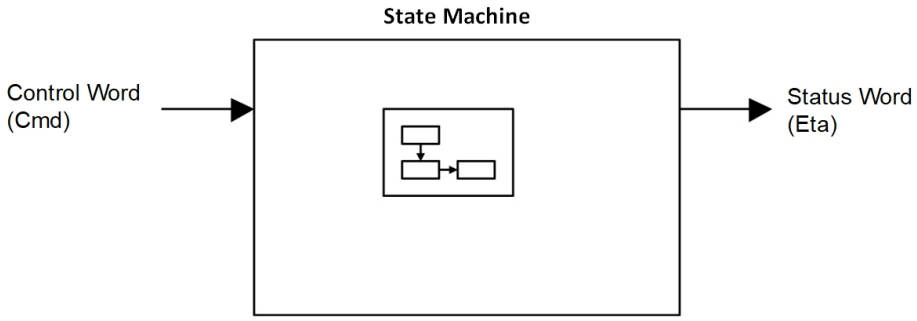
Functional Description

Introduction

Soft starter operation involves one main function, which is illustrated in the diagrams below.

Altivar Soft Starter

The following figure shows the control diagram for soft starter operation:



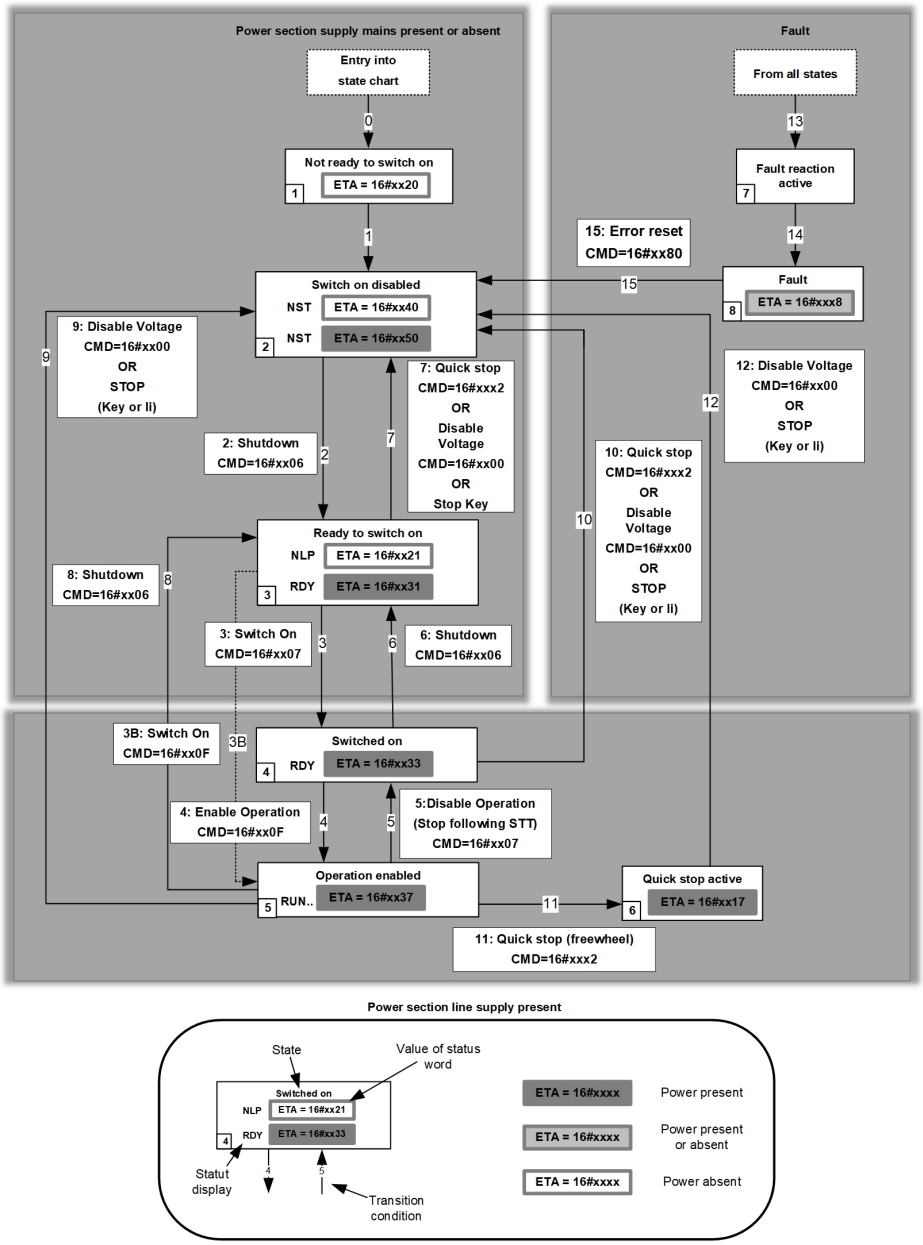
Standard Mode Operating State Diagram

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 Standard Mode state diagram:



Description of Operating States

Soft starter Operating State

Each state represents an internal reaction by the soft starter.

The operating state of the soft starter changes depending on whether the control word is sent to CMD or an event occurs (an error detection, for example).

The soft starter operating state can be identified by the value of the status word 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	The power stage is not ready to switch on. The soft starter is locked, no power is supplied to the motor. The configuration and adjustment parameters can be modified.
3 - Ready to switch on	The power stage is ready to switch on and awaiting power stage supply mains. The soft starter is locked, no power is supplied to the motor. The configuration and adjustment parameters can be modified. **NOTE:** If mains contactor is wired on a relay (**[R1 Assignment]** R1 is set to **[Isolating Relay]** ISOL or **[R3 Assignment]** R3 is set to **[Mains Contactor]** LLC), mains contactor is not closed and we stay in this state until a run command is given.
4 - Switched on	Power stage is switched on. The power stage of the soft starter is ready to operate, but voltage has not yet been applied to the output. The adjustment parameters can be modified. **NOTE:** By default, Relay R1 **[R1 Assignment]** R1 is set to **[Operating State Fault]** FLT then the mains contactor is closed. The soft starter is locked, no power is supplied to the motor. **NOTE:** If mains contactor is wired on a relay (**[R1 Assignment]** R1 is set to **[Isolating Relay]** ISOL or **[R3 Assignment]** R3 is set to **[Mains Contactor]** LLC), we reach temporarily this state once Run command is applied and mains contactor is closed allowing presence of power stage before switching to *5 - Operation enabled*.
5 - Operation enabled	Power stage is enabled. The soft starter is in running state For a separate control stage with mains contactor, the contactor is closed. The soft starter is unlocked, power is supplied to the motor. The soft starter functions are activated and voltage is applied to the motor terminals. If the Halt command is applied, no power is supplied to the motor. The adjustment parameters can be modified. The configuration parameters cannot be modified. The reaction of the soft starter to a Disable operation command is to stop following to the **[Type of stop]** STT.
6 - Quick stop active	The soft starter performs a freewheel stop and remains locked in the operating state *6-Quick stop active*. Before restarting the motor, it is required to go to the operating state *2-switch on disabled*. The soft starter stops according to freewheel stop and then remains in state *6 - Quick stop active* until: • The **STOP** key is pressed or • A freewheel stop command via the digital input of the terminal.
7 - Fault reaction active	Transient state during which the soft starter performs a stop due to a detected error. If behavior of the detected error is configurable, then the reaction will depend on setting of it's **error response**.
8 - Fault	End of the stop caused by change to the previous state *7 - Fault reaction active*. Power stage is disabled. The soft starter is locked, no power is supplied to the motor if an error detection has been triggered. Else the soft starter change to the step *2- switch on disable*. The soft starter function is disabled

Summary

Device Status Summary

Operating State	Power Supply to Power Stage	Power Supplied to Motor	Modification of Configuration Parameters
1 - Not ready to switch on	Not required	No	Yes
2 - Switch on disabled	Not required	No	Yes
3 - Ready to switch on	Not required	No	Yes
4 - Switched on	Required	No	Yes
5 - Operation enabled	Required	Yes	No
6 - Quick stop active	Required	No	No
7 - Fault reaction active	Depends on error response configuration	Depends on error response configuration	No
8 - Fault	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.
- A Setting parameter can be accessed in all operating state of the soft starter.

Command Register CMD

Bit Mapping of the Control Word

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
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	***Decelerated stop order*** *(factory setting)*. The Bit can be set to an other function. **NOTE:** If no function is assigned, the Bit will return to his factory setting.	***Dynamic braking stop*** *(factory setting)*. The Bit can be set to an other function. **NOTE:** If no function is assigned, the Bit will return to his factory setting.	Manufacturer specific assignable	Manufacturer specific assignable	Reserved (=0)	Reserved (=0)	Halt 0 = run asked 1 = stop asked

Command	State Transition	Final Operating State	Bit 7	Bit 3	Bit 2	Bit 1	Bit 0	Example Value
			Fault Reset	Enable Operation	Quick Stop	Enable Voltage	Switch On	
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
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 (**[Freewheel]** F, **[Deceleration]** D, or **[Braking]** B) the soft starter remains in the *5 - Operation enabled* state.

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

Bit	Modbus Serial
Bit 11	C111
Bit 12	C112
Bit 13 is set to ***Dynamic braking stop*** *(factory setting)*. This Bit can be set to an other function. **NOTE:** If no function is assigned, the Bit will return to his factory setting.	C113
Bit 14 is set to ***Decelerated stop order*** *(factory setting)*. This Bit can be set to an other function. **NOTE:** If no function is assigned, the Bit will return to his factory setting.	C114
Bit 15	C115

For example, to assign the preheating to bit15 of Modbus serial, simply configure the **[Preheating Assign]** PRHA parameter with the **[C115]** C115 value.

Status Word ETA

Bit Mapping of the Status Word

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

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8
Reserved (=0)	Manufacturer-specific Stop via STOP key	Reserved (=0)	Reserved (=0)	Reserved (=0)	Reserved (=0)	Remote (local mode control) Command via fieldbus	Reserved (=0)

Operating State	Bit 6 Switch On Disabled	Bit 5 Quick Stop	Bit 4 Voltage Enabled	Bit 3 Fault	Bit 2 Operation Enabled	Bit 1 Switched On	Bit 0 Ready to Switch On	ETA Masked by 006F H (1)
1 -Not ready to switch on	0	X	0	0	0	0	0	0020 hex
2 -Switch on disabled	1	X	X	0	0	0	0	0040 hex 0050 hex
3 -Ready to switch on	0	1	X	0	0	0	1	0021 hex 0031 hex
4 -Switched on	0	1	1	0	0	1	1	0033 hex
5 -Operation enabled	0	1	1	0	1	1	1	0037 hex
6 -Quick stop active	0	0	1	0	1	1	1	0017 hex
7 -Fault reaction active	X	X	X	0	1	1	1	–
8 -Fault	X	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.

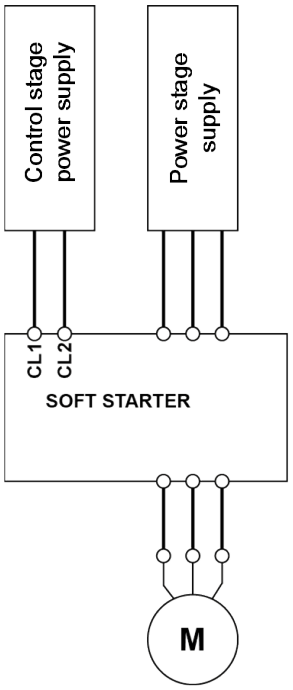
Starting Sequence

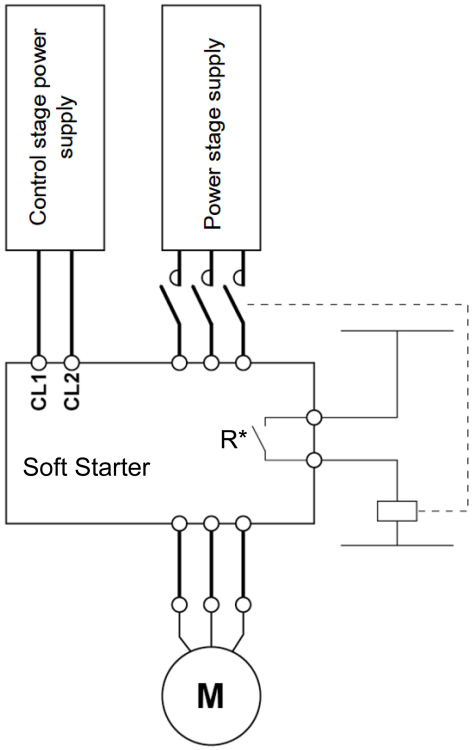
Description

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

There are 2 possible scenarios:

Power stage supply	Mains contactor controlled by another device	Mains contactor controlled by the soft starter (1)





(1) R*: R1 or R3:

- **[R1 Assignment]** R1 is set to **[Isolating Relay]** ISOL

  NOTE: If R1 is set to **[Isolating Relay]** ISOL, R3 can't be set to **[Mains Contactor]** LLC.

- **[R3 Assignment]** R3 is set to **[Mains Contactor]** LLC

  NOTE: If R3 is set to **[Mains Contactor]** LLC, R1 can't be set to **[Isolating Relay]** ISOL.

Sequence for a Soft starter

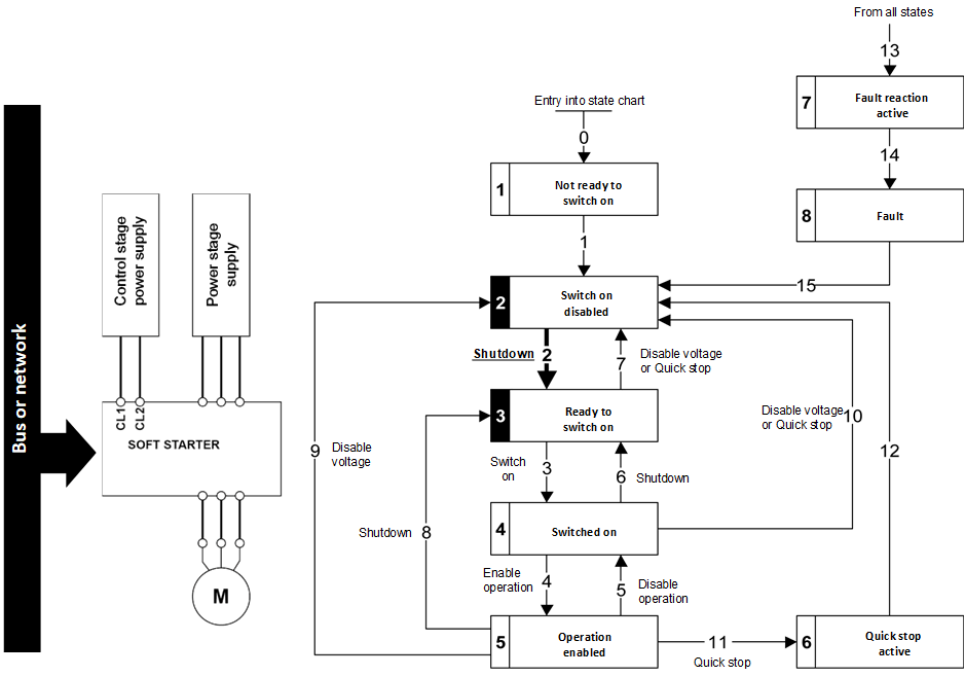
Description

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.

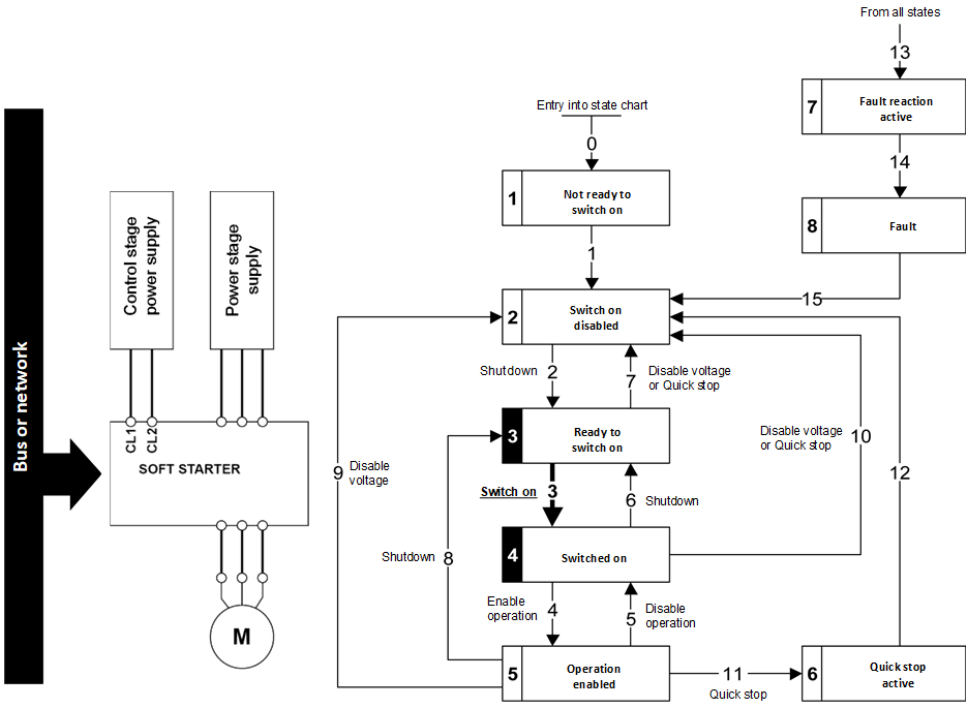


Step 2

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

Power Stage Supply	Terminal Display	Status Word
Absent	NLP	21 hex
Present	RDY	31 hex

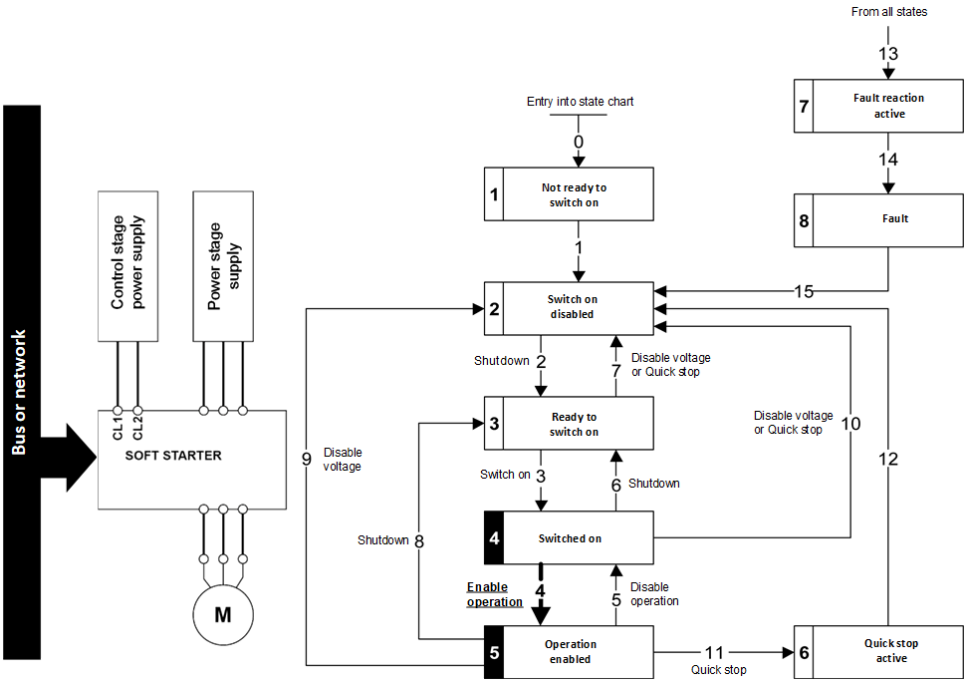
- Apply the *3 - Switch on* command



Step 3

- If power supply is present; check that the soft starter is in the operating state *4 - Switched on*.

  NOTE: If power supply is not present, we stay in *3 - Ready to switch on*.
- Then apply the *4- Enable operation* command.
- The motor can be started.



Sequence for a Soft starter with Mains Contactor Control

Description

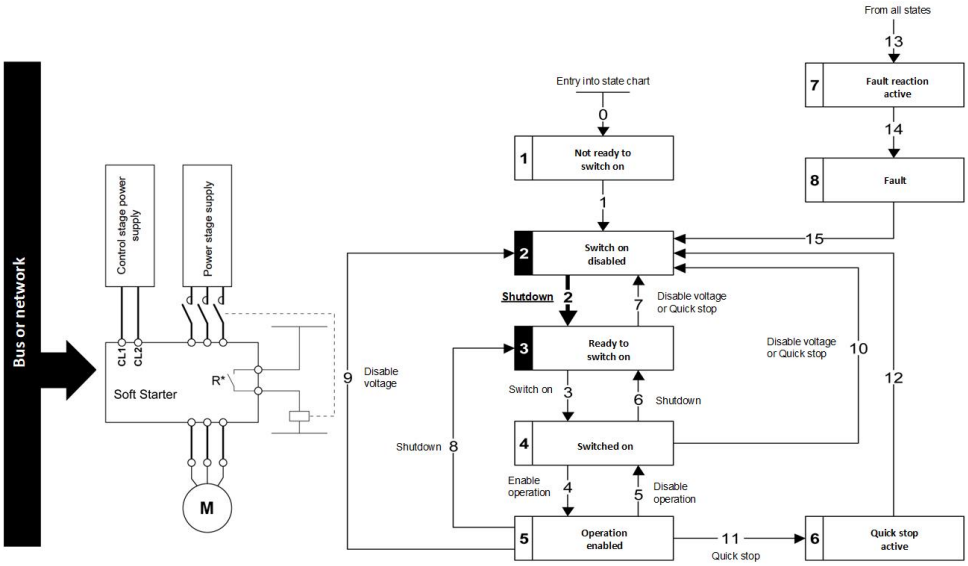
Power is supplied separately to the power and control stages.

If power is supplied to the control stage, it does not have to be supplied to the power stage as well. The soft starter 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 - Shut down* command.



NOTE:

R*: R1 or R3:

- **[R1 Assignment]** R1 is set to **[Isolating Relay]** ISOL

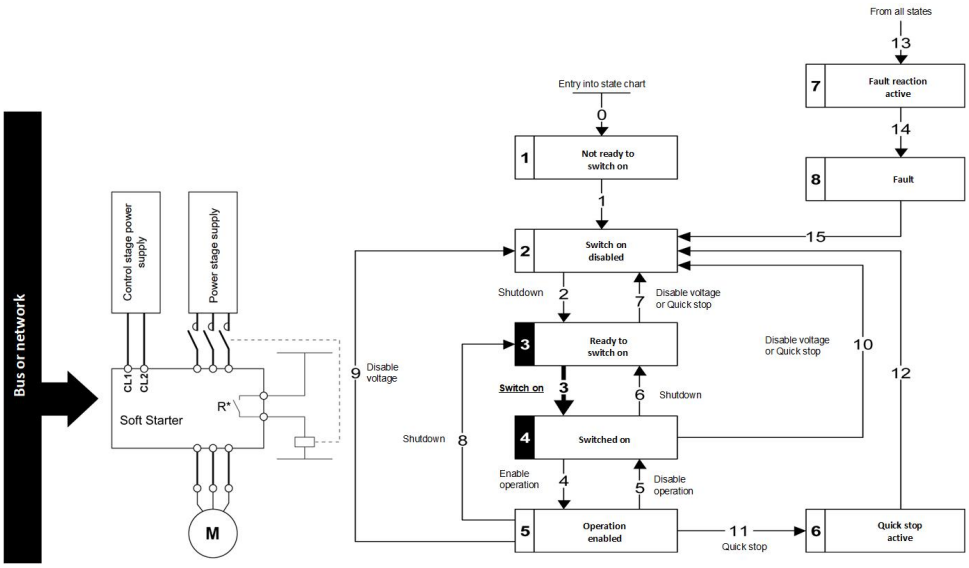
  NOTE: If R1 is set to **[Isolating Relay]** ISOL, R3 can't be set to **[Mains Contactor]** LLC.

- **[R3 Assignment]** R3 is set to **[Mains Contactor]** LLC

  NOTE: If R3 is set to **[Mains Contactor]** LLC, R1 can't be set to **[Isolating Relay]** ISOL.

Step 2

- Check that the soft starter 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 by giving RUN command.
- 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 soft starter triggers an error **[Input Contactor]** LCF.



NOTE:

R*: R1 or R3:

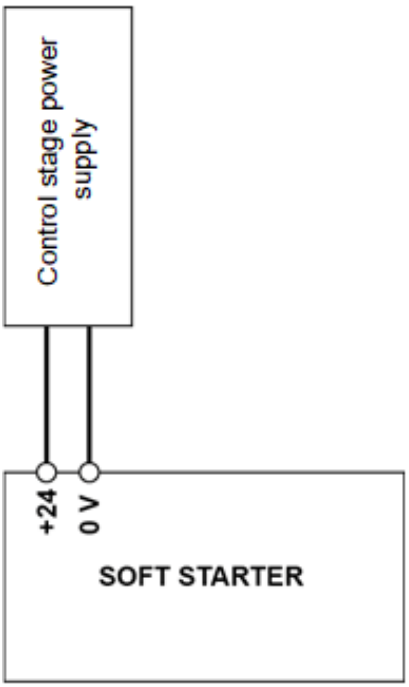
- **[R1 Assignment]** R1 is set to **[Isolating Relay]** ISOL

  NOTE: If R1 is set to **[Isolating Relay]** ISOL, R3 can't be set to **[Mains Contactor]** LLC.

- **[R3 Assignment]** R3 is set to **[Mains Contactor]** LLC

  NOTE: If R3 is set to **[Mains Contactor]** LLC, R1 can't be set to **[Isolating Relay]** ISOL.

Automation Commissioning Only

Control stage supplied via +24 V of the control board	Use case
	In case of no electrical accreditation to work on the product with the presence of the supply mains, it is possible to connect a separate 24V supply to commission the soft starter with no supply mains applied to the product.

Modbus Functions

Modbus Protocol

Introduction

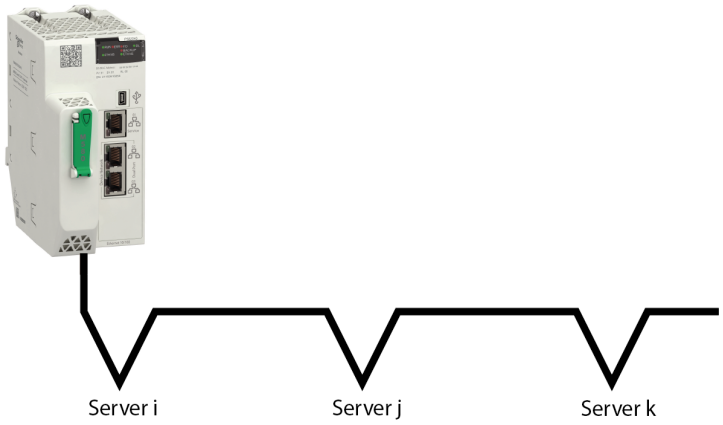
The transmission mode used is RTU. The frame does not contain message header and end of message bytes.

Server address	Request code	Data	CRC16

The data is transmitted in binary code.

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

Principle



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

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

It interrogates each of the servers in succession

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

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

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

Direct server-to-server communications are not possible.

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

The 2 types of dialogue are possible between client and servers:

- The client sends a request to a server and waits for its response
- The client sends a request to all servers without waiting for a response (broadcasting principle)

Addresses

Address specification:

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

Supported Modbus Functions

Introduction

The soft starter supports the following Modbus functions:

Function Name	Code		Description	Remarks
	Dec.	Hex		
Read Holding Registers	03	03 hex	Read N output words	Maximum PDU length: 125 words
Write One Output Word	06	06 hex	Write 1 output word	–
Write Multiple Registers	16	10 hex	Write N output word	Maximum PDU length: 123 words
Read/write Multiple Registers	23	17 hex	Read/write multiple registers	Maximum PDU length: 125 words (R), 121 words (W)
(Subfunction) *Read Device Identification*	43/14	2B hex/ 0E hex	Encapsulated interface transport/ Read device identification	–
Diagnostics	08	08 hex	Diagnostics	–

Read Holding Registers (03 hex)

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

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

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

Request

Function code	1 byte	03 hex
Starting address	2 bytes	0000 hex...FFFF hex
Quantity of registers	2 bytes	1 to 125 (0x7D)

Response

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

Detected error

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

Then, here an example of a request to read registers @9860 to @9863:

Code	Name	Logic Address
IN	Nominal motor current (A)	2684 hex= 9860
LSC	Stator loss compensation (%)	2685 hex= 9861
BST	Voltage boost level (%)	2686 hex= 9862
TBS	Time before starting (s)	2687 hex= 9863

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

Request

server no.	Function Code	Number of first word	Number of words	CRC16
02	03	2684	004	0C45

Response

server no.	Function Code	Number of bytes read	First word value	Second word value	Third word value	Last word value	CRC16
02	03	08	000A	0032	0000	0002	8896
	Value of:	–	@9860	@9861	@9862	@9863	–
	Parameters:	–	IN	LCS	BST	TBS	–

Analyzed:

Code	Read		Result
	hex	dec.	
IN	000A hex	10	10 x Ie starter current rating (A)
LSC	0032 hex	50	50%
BST	0000 hex	0	0%
TBS	0002 hex	2	2 s

Write 1 Output Word (06 hex)

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

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

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

Request

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

Response

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

Detected error

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

Then, here an example of a request to write register @9060:

Write on:

Code	Name	Logic Address
ACC	Acceleration ramp time (s)	2364 hex= 9060

Write value 000D hex in server address 02 hex:

Code	Write	
	hex	dec.
ACC	000D hex	13

Request:

server no.	Function Code	Word number	Value of word	CRC16
02	06	2364	000D	0267

Response:

server no.	Function Code	Word number	Value of word	CRC16
02	06	2364	000D	0267

Analyzed:

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

Write Multiple Register (10 hex)

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

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

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

Request

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

Response

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

Detected error

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

Then, here an example of a request to write registers @9060 and @9061:

Write on:

Code	Name	Logic Address
ACC	Acceleration ramp time (s)	2364 hex= 9060
DEC	Deceleration ramp time (s)	2365 hex= 9061

Write values on server address 02 hex:

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

Request

server no.	Request code	No. of first word	Number of words	Number of bytes	Value of first word	Value of Second word	CRC16
02 hex	10 hex	2364 hex	0002 hex	04 hex	0014 hex	001E hex	B60D hex

Response

server no.	Response code	No. of first word	No. of words	CRC16
02 hex	10 hex	2364 hex	0002 hex	0BA0 hex

Analyzed:

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

Read/Write Multiple Registers (17 hex)

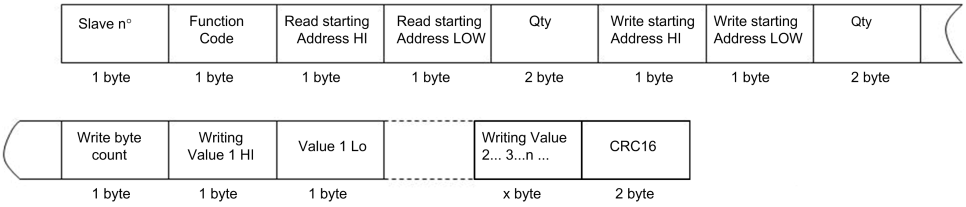
This function code performs a combination of one read operation and one write operation in a single MODBUS transaction. The write operation is performed before the read. Holding registers are addressed starting at zero. Therefore holding registers 1-16 are addressed in the PDU as 0-15.

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

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

For example

Description	Length in Byte	Value	Comment
Function code	1	17 hex	–
Read starting address	2	XXXX hex	Modbus address
Quantity	2	03 hex	Contain number of holding registers to be read
Write starting address	2	XXXX hex	Modbus address
Quantity	2	03 hex	Contain number of holding registers to be written
Write byte count	1	06 hex	The byte count specifies the number of bytes to follow in the field write register value
Write registers value	6	XXXXXX XXXXXX hex	Address to be written respectively in NCA1 to NCA4. For example: CMD, ERRD, CMI



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

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

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

The interface consists of 3 categories of objects :

- Basic Device Identification:

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

- Regular Device Identification:

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

- Extended Device Identification:

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

The table provides the device identification details:

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

Request

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

Response

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

Example

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

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

Id of object number 2	Length of object number 2	Value of object number 2
01	0B	**ATS480xxxxxx**
1 byte	1 byte	11 bytes

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

CRC16	
Lo	Hi
1 byte	1 byte

The total response size equals 49 bytes

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

- Object number 1: Manufacturer name (always **Schneider Electric**, that is. 18 bytes).
- Object number 2: Device reference (ASCII string; for example, **ATS480xxxxxx**, that is. 11 bytes).
- Object number 3: Device version, in **MMmm** format where **MM** represents the determinant and **mm** the subdeterminant (4-bytes ASCII string; for example,: **0201** for version 2.1).

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

Diagnostics (08 hex)

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

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

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

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

Subcode 00 hex: Echo

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

Subcode 0A hex: Counter reset

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

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

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

Request and response (the frame format is identical)

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

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

Example

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

Request and response (the frame format is identical)

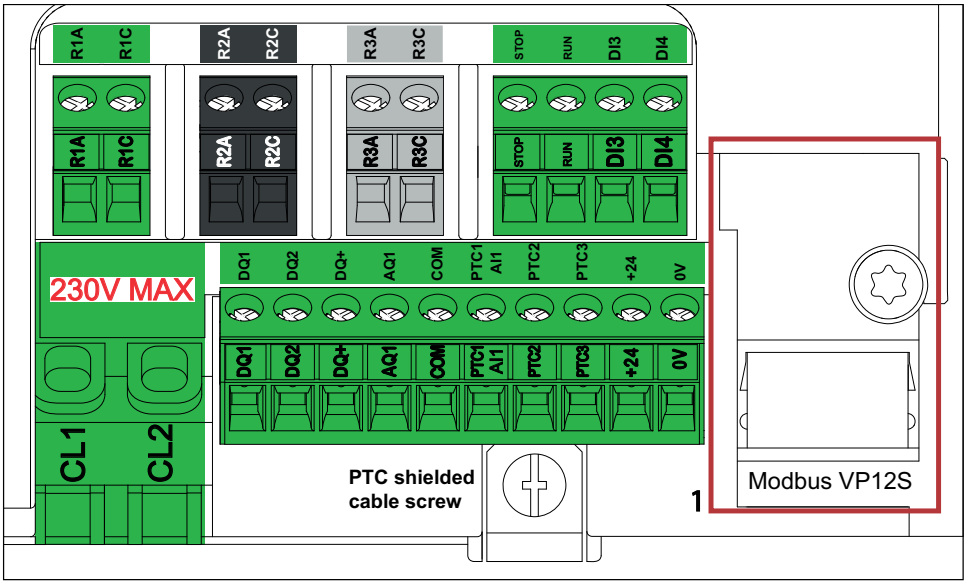
server no.	Request code or response code	Subcode		Value of first byte	Value of second byte	CRC16	
		Hi	Lo			Lo	Hi
02 hex	08 hex	00 hex	00 hex	31 hex	32 hex	74 hex	1B hex

Hardware Setup

Hardware Presentation

Modbus Serial Communication Port

The following figure shows the terminal view of the soft starter:



1 Modbus RTU communication port

Firmware Version

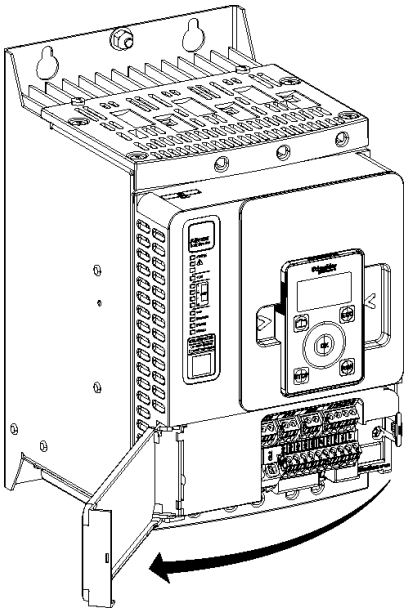
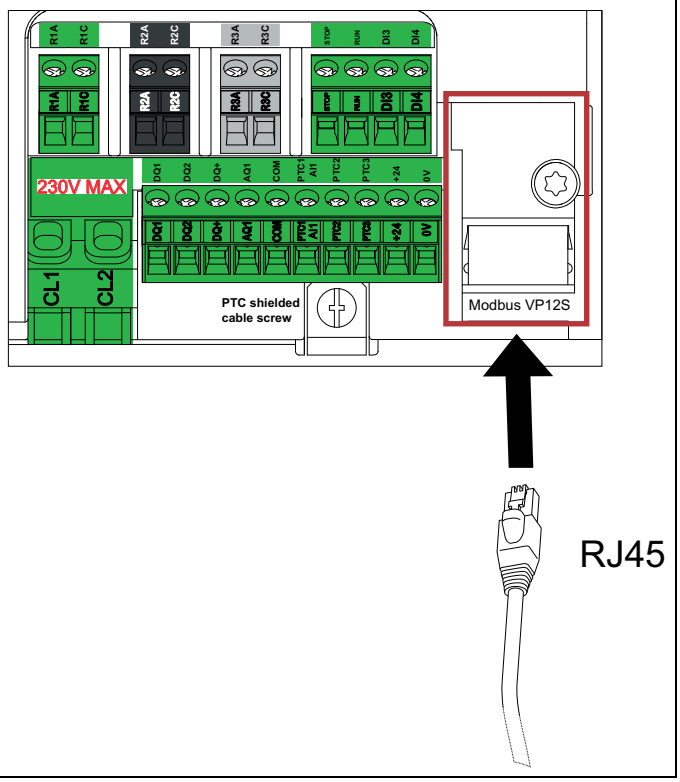
Compatibility

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

Connection to the Adapter

Procedure to access to the Modbus VP12S port of the Soft starter

Apply the following instructions to remove the front cover of the soft starter:

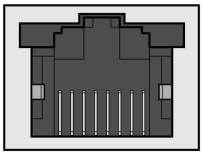
Step	Action	
1	Open the terminal cover	
2	Plug the RJ45 cable to the RJ45 socket identified with “Modbus VP12S”	

Electrical Installation

Connection to Soft starter

Connect the RJ45 cable connector to the device connector.

The following figure shows the pin layout for RJ45 connector:



8 7 6 5 4 3 2 1

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

Pin	Signal
1	Reserved
2	
3	
4	D1(1)
5	D0(1)
6	–
7	12 Vdc(2)
8	Common
(1) Modbus signals (2) Supply for RS232 / RS485 converter or a remote terminal	

RS485 Bus Schematic

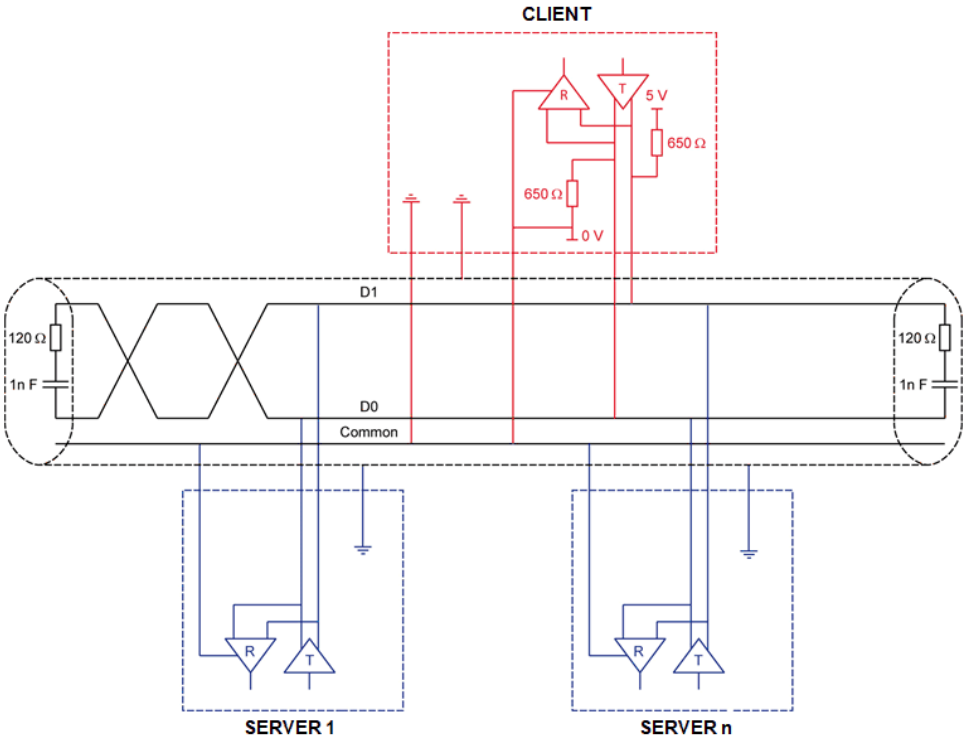
The RS485 standard allows variants of different characteristics:

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

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

Schematic Diagram

The following is the RS485 bus schematic diagram:



Characteristic	Definition
Type of trunk cable	Shielded cable with 1 twisted pair and at least a third conductor
Maximum length of bus	1000 m at 19200 bps with the Schneider Electric TSX CSA••• cable
Maximum number of stations (without repeater)	32 stations that are 31 servers
Maximum length of tap links	• 20 m for 1 tape link • 40 m divided by the number of tape links on a multiple junction box
Bus polarization	• One 450...650 Ω pull-down resistor at 5 V (650 Ω recommended) • One 450...650 Ω pull-down resistor at the common (650 Ω recommended) This polarization is recommended for the client.
Line terminator	One 120 Ω 0.25 W resistor in series with 1 nF 10 V capacitor
Common polarity	Yes (Common), connected to the protective earth ground at one or more points of the bus

Cable Routing Practices

Immunity Against Interference

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

Accessories Presentation

Information

Connection accessories should be ordered separately (See the catalog).

Flashing Cordset Cable

It is possible to connect to SoMove or EADM using the Flashing Cordset (VW3A8127) or (TCSMCNAM3M002P) cable.

Software Setup

Basic Settings

Structure of the Parameter Table

General Legend

Pictogram	Description
	This parameter can be set during operation or when stopped. **NOTE:** It is advisable to stop the motor before modifying any of the settings
	The motor must be stopped to set this parameter.
	Power cycle must be performed after setting this parameter.
	Read only parameter, mainly used for monitoring.
	Expert mode required to access this parameter.

Menu Presentation

Below an example of a menu presentation:

[Short Label] CODE

Access path: **[Menu]** ➡ **[Sub-menu]**

About this menu
Description of the menu.

Parameter Presentation

Below an example of a parameter presentation:

HMI label	Setting or Display	Factory setting
[Short Label] CODE (pictogram)	XXX...XXX **[unit]** **[additional informations]**	**Factory setting**: **[Short Label]** CODE
[Long label] Access path: **[Menu]** ➡ **[Sub-menu]** Reference exclusivity and required optional modules. Example: Fieldbus Module VW3A3607 is required. Description of the parameter. Parameter incompatibilities and / or required configuration. Example: This parameter can be accessed it **[Short Label]** CODE is set to **[Short Label]** CODE. This parameter is not compatible with **[Short Label]** CODE. Impact on other parameters. Example: If this parameter is modified, the parameter **[Short Label]** CODE is set to factory settings.		

Finding a Parameter in This Document

Display on HMI Tools

A parameter is identified by:

- Its short label displayed on the Plain Text Display Terminal, and on the Graphic Display Terminal
- Its long label displayed on SoMove DTM Parameter list tab, on the Graphic Display Terminal by pressing  , and on the Webserver
- Its code displayed on SoMove DTM Parameter list tab, on the Graphic Display Terminal by pressing  , and on the Webserver

Example: **[Acceleration]** is a short label, its code is ACC and its long label is ***Acceleration ramp time***.

With the Manual

It is possible to use either the parameter name or the parameter code to search in the manual the page giving details of the selected parameter.

[Modbus Fieldbus] MD1

Access path: **[Communication]** COM ➡ **[Modbus Fieldbus]** MD1

About this Menu

This menu provides the parameters to set the embedded Modbus fieldbus.

HMI label	Setting	
[Modbus Address] ADD	Logic address: 1771 hex = 6001 Range: 0...247 Factory setting: 0	Type: UINT (Unsigned16) Read/write: R/WS Unit: -
Device modbus address This parameter sets the embedded Modbus device address. Address 0 is reserved for point to point connection.		
[Modbus Baud Rate] TBR	Logic address: 1773 hex = 6003 Factory setting:**[19200 bps]** 19200	Type: WORD (Enumeration) Read/write: R/WS Unit: bps
Modbus baud rate This parameter sets the embedded Modbus baud rate. • **[Automatic]** AUTO: Automatic detection • **[4800 bps]** 4800: 4,800 bauds • **[9600 bps]** 9600: 9,600 bauds • **[19200 bps]** 19200: 19,200 bauds • **[38.4 Kbps]** 38400: 38,400 bauds		
[Term word order] TWO	Logic address: 1776 hex = 6006 Factory setting: **[ON]** HIGH	Type: WORD (Enumeration) Read/write: R/WS
Terminal Modbus: Word order This parameter sets the embedded Modbus terminal word order. • **[OFF]** LOW: Low word first • **[ON]** HIGH: High word first		
[Modbus Format] TFO	Logic address: 1774 hex = 6004 Factory setting: **[8-E-1]** 8E1	Type: WORD (Enumeration) Read/write: R/WS
Modbus format This parameter sets the embedded Modbus frame format. **NOTE:** Connection to SoMove is done using the format **[8-E-1]** 8E1. • **[8-O-1]** 8O1: 8 bits odd parity 1 stop bit • **[8-E-1]** 8E1: 8 bits even parity 1 stop bit • **[8-N-1]** 8N1: 8 bits no parity 1 stop bit • **[8-N-2]** 8N2: 8 bits no parity 2 stop bits		

HMI label	Setting	
[ModbusTimeout] TTO	Logic address: 1775 hex = 6005 Range: 0.1...30 s Factory setting: 5 s	Type: UINT (Unsigned16) Read/write: R/WS Unit: 0.1 s

Modbus timeout

This parameter sets the embedded Modbus communication timeout.

[Modbus Error Resp] SLL	Logic address: 1B62 hex = 7010 Factory setting: **[Freewheel Stop]** YES	Type: WORD (Enumeration) Read/write: R/WS

Response to Modbus interruption

This parameter sets the type of stop applied to the motor when a loss of communication is detected on the embedded Modbus channel.

- **[Ignore]** NO: Detected error ignored, triggers warning **[Modbus Com Warn]** SLLA
- **[Freewheel Stop]** YES: Error is triggered and motor stops in freewheel
- **[Per STT]** STT: Motor stops according to the value sets in **[Type of stop]** STT and no error is triggered
- **[Deceleration]** DEC: Stop in deceleration following the values set to **[Deceleration]** DEC and **[End Of Deceleration]** EDC, error is triggered at the end of deceleration
- **[Braking]** BRK: Stop in braking following the values set to **[Braking Level]** BRC and **[DC Braking To Stop]** EBA, error is trigger at the end of braking

⚠WARNING

LOSS OF CONTROL

If this parameter is set to **[Ignore]** NO, Modbus communication monitoring is disabled.

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

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

[Product restart] RP	Logic address: 1BD8 hex = 7128 Factory setting: **[Not Assigned]** NO	Type: WORD (Enumeration) Read/write: R/WS

Product restart

Manually restart the device via the HMI. Press and hold the **OK** button on the display terminal for 2 seconds to restart the device.

This parameter is automatically set to **[Not Assigned]** NO after restart.

- **[Not Assigned]** NO: No restart
- **[Yes]** YES: Restart the soft starter

The Restart function performs a Fault Reset and then restarts the device. During this Restart procedure, the device goes through the same steps as if it had been switched off and on again. Depending on the wiring and the configuration of the device, this may result in immediate and unanticipated operation.

⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

The Restart function performs a Fault Reset and restarts the device.

- Verify that activating this function does not result in unsafe conditions.

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

Local Configuration of the Communication Scanner

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

The communication scanner (**[Com. scanner input]** ICS and **[Com. scanner output]** OCS) are accessible via the following menus: **[Communication]** COM ➡ **[Modbus SL]** MSL ➡ **[Modbus Fieldbus]** MD1

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

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

Sub Menu	Parameter description	Default assignment	Modbus address xxxxx (dec.) xxxx hex
[Com. scanner input] ICS	**[Scan. IN1 address]** NMA1 Source address of the 1st input word	**[Status Register]** ETA (@3201)	12701 319D hex
	[Scan. IN2 address] NMA2 Source address of the 2nd input word	**[Motor Current]** LCR (@3204)	12702 319E hex
	[Scan. IN3 address] NMA3 Source address of the 3rd input word	**[Motor Therm State]** THR (@9630)	12703 319F hex
	[Scan. IN4 address] NMA4 Source address of the 4th input word	**[CiA402 Error Code]** ERRD (@8606)	12704 31A0 hex
	[Scan. IN5 address] NMA5 Source address of the 5th input word	0	12705 31A1 hex
	[Scan. IN6 address] NMA6 Source address of the 6th input word	0	12706 31A2 hex
	[Scan. IN7 address] NMA7 Source address of the 7th input word	0	12707 31A3 hex
	[Scan. IN8 address] NMA8 Source address of the 8th input word	0	12708 31A4 hex

Sub Menu	Parameter description	Default assignment	Modbus address xxxxx (dec.) xxxx hex
[Com. scanner output] OCS	**[Scan.Out1 address]** NCA1 Destination address of the 1st output word	**[Cmd Register]** CMD (@8501)	12721 31B1 hex
	[Scan.Out2 address] NCA2 Destination address of the 2nd output word	0	12722 31B2 hex
	[Scan.Out3 address] NCA3 Destination address of the 3rd output word	0	12723 31B3 hex
	[Scan.Out4 address] NCA4 Destination address of the 4th output word	0	12724 31B4 hex
	[Scan.Out5 address] NCA5 Destination address of the 5th output word	0	12725 31B5 hex
	[Scan.Out6 address] NCA6 Destination address of the 6th output word	0	12726 31B6 hex
	[Scan.Out7 address] NCA7 Destination address of the 7th output word	0	12727 31B7 hex
	[Scan.Out8 address] NCA8 Destination address of the 8th output word	0	12728 31B8 hex

Monitoring the Communication Scanner

It is also possible to monitor the value of the parameters which has been configured in the communication scanner. This monitored values (**[Com. scanner input map]** ISA and **[Com scan output map]** OSA) are accessible via the following menus: **[Communication]** COM ➡ **[Communication map]** CMM ➡ **[Modbus network diag]** MND.

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

Sub Menu	Parameter description	Default assignment	Modbus address xxxxx (dec.) xxxx hex
[Com. scanner input map] ISA	**[Com Scan In1 val.]** NM1 Source value of the 1st input word	**[Status Register]** ETA (@3201)	12741 31C5 hex
	[Com Scan In2 val.] NM2 Source value of the 2nd input word	**[Motor Current]** LCR (@3204)	12742 31C6 hex
	[Com Scan In3 val.] NM3 Source value of the 3rd input word	**[Motor Therm State]** THR (@9630)	12743 31C7 hex
	[Com Scan In4 val.] NM4 Source value of the 4th input word	**[CiA402 Error Code]** ERRD (@8606)	12744 31C8 hex
	[Com Scan In5 val.] NM5 Source value of the 5th input word	0	12745 31C9 hex
	[Com Scan In6 val.] NM6 Source value of the 6th input word	0	12746 31CA hex
	[Com Scan In7 val.] NM7 Source value of the 7th input word	0	12747 31CB hex
	[Com Scan In8 val.] NM8 Source value of the 8th input word	0	12748 31CC hex
[Com scan output map] OSA	**[Com Scan Out1 val.]** NC1 Destination address of the 1st output word	**[Cmd Register]** CMD (@8501)	12761 31D9 hex
	[Com Scan Out2 val.] NC2 Destination address of the 2nd output word	0	12762 31DA hex
	[Com Scan Out3 val.] NC3 Destination address of the 3rd output word	0	12763 31DB hex
	[Com Scan Out4 val.] NC4 Destination address of the 4th output word	0	12764 31DC hex
	[Com Scan Out5 val.] NC5 Destination address of the 5th output word	0	12765 31DD hex
	[Com Scan Out6 val.] NC6 Destination address of the 6th output word	0	12766 31DE hex
	[Com Scan Out7 val.] NC7 Destination address of the 7th output word	0	12767 31DF hex
	[Com Scan Out8 val.] NC8 Destination address of the 8th output word	0	12768 31E0 hex

[Product restart] RP

HMI label	Setting	
[Product restart] RP	Logic address: 1BD8 hex = 7128 Factory setting: **[Not Assigned]** NO	Type: WORD (Enumeration) Read/write: R/WS

Product restart

Manually restarts the device via the HMI. Press and hold the **OK** button on the display terminal for 2 seconds to restart the device.

This parameter is automatically set to **[Not Assigned]** NO after restart.

- **[Not Assigned]** NO: No restart
- **[Yes]** YES: Restart the device

The Restart function performs a Fault Reset and then restarts the device. During this Restart procedure, the device goes through the same steps as if it had been switched off and on again. Depending on the wiring and the configuration of the device, this may result in immediate and unanticipated operation.

⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

The Restart function performs a Fault Reset and restarts the device.

- Verify that activating this function does not result in unsafe conditions.

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

[Modbus HMI] MD2

Access path: **[Communication]** COM ➡ **[Modbus HMI]** MD2

About this Menu

This menu provides the parameters to manage the communication with the display terminal.

The communication timeout with the display terminal is 2 seconds.

HMI label	Setting	
[Modbus 2 baud rate] TBR2	Logic address: 1787 hex = 6023 Factory setting: **[19200 bps]** 19200	Type: WORD (BitString16) Read/write: R/WS

Modbus 2 baud rate

This parameter sets the HMI Modbus baud rate.

- **[4800 bps]** 4800: 4,800 bauds
- **[9600 bps]** 9600: 9,600 bauds
- **[19200 bps]** 19200: 19,200 bauds
- **[38.4 Kbps]** 38400: 38,400 bauds

[Term 2 word order] TWO2	Logic address: 178A hex = 6026 Factory setting: Factory setting: **[ON]** HIGH	Type: WORD (BitString16) Read/write: R/WS

HMI label	Setting	
Terminal Modbus 2: Word order This parameter sets the HMI Modbus terminal word order. • **[OFF]** LOW: Low word first • **[ON]** HIGH: High word first		
[Modbus 2 format] TFO2	Logic address: 1788 hex = 6024 Factory setting: **[8-E-1]** 8E1	Type: WORD (BitString16) Read/write: R/WS
Modbus format This parameter sets the HMI Modbus frame format. • **[8-O-1]** 8O1: 8 bits odd parity 1 stop bit • **[8-E-1]** 8E1: 8 bits even parity 1 stop bit • **[8-N-1]** 8N1: 8 bits no parity 1 stop bit • **[8-N-2]** 8N2: 8 bits no parity 2 stop bits		
[Product restart] RP	Logic address: 1BD8 hex = 7128 Factory setting: **[Not Assigned]** NO	Type: WORD (Enumeration) Read/write: R/WS
Product restart Manually restart the device via the HMI. Press and hold the **OK** button on the display terminal for 2 seconds to restart the device. This parameter is automatically set to **[Not Assigned]** NO after restart. • **[Not Assigned]** NO: No restart • **[Yes]** YES: Restart the soft starter The Restart function performs a Fault Reset and then restarts the device. During this Restart procedure, the device goes through the same steps as if it had been switched off and on again. Depending on the wiring and the configuration of the device, this may result in immediate and unanticipated operation.		

⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

The Restart function performs a Fault Reset and restarts the device.

- Verify that activating this function does not result in unsafe conditions.

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

Communication parameters

About this Section

This section shows the I/O parameters and their communications addressees.

For more information about the Communication Parameter Addresses, please refers to the ATS480 Communication Parameter NNZ85544.

Comportment when an communication error occurs

If an error appears, the device return to his initial state.

For example, if:

- a pump is connect to R3.
- the pump is assign to OL1R.
- the pump is in run state.

If an communication error occurs, the pump is set to stop mode.

Logic I/O

Code	Settings	
[Logic Inputs States] IL1R	Logic address: 1452 hex = 5202	Type: WORD (BitString16) Read/write: R Unit: -
Logic inputs states • Bit0 : "DI1" Digital inputs real image • Bit1 : "DI2" Digital inputs real image • Bit2 : "DI3" Digital inputs real image • Bit3 : "DI4" Digital inputs real image		
[Logic Outputs States] OL1R	Logic address: 145C hex = 5212	Type: WORD (BitString16) Read/write: R/W Unit: -
Logic outputs states • Bit0 : "R1" relay real image • Bit1 : "R2" relay real image • Bit2 : "R3" relay real image • Bit8 : "DQ1" digital outputs real image • Bit9 : "DQ2" digital outputs real image The relay or logic outputs can be controlled via the network. Simply write this parameter. The outputs to be controlled must not be assigned to a soft starter function, otherwise the write operation has no effect.		

Analog inputs

Code	Settings	
[AI1] AI1C	Logic address: 147A hex = 5242	Type: INT (Signed16) Read/write: R Unit: -
Physical value AI1 AI1 customer image (1mV, 0.001mA) • (AI1T == "PTC") : 0.01 kOhm • (AI1T == "1PT2") : 0.1 Ohm • (AI1T == "1PT23") : 0.1 Ohm • else : 0.001 V		

Code	Settings	
[Analog Input 1 Standardized Value] AI1R	Logic address: 1470 hex= 5232	Type: INT (Signed16) Read/write: R Unit: -
Analog input 1 standardized value AI1 real application image		

Analog outputs

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

Code	Settings	
[AQ1] AO1C	Logic address: 1497 hex = 5271	Type: INT (Signed16) Read/write: R/W Unit: -
AQ1 physical value AQ1 customer image (1mV, 0.001mA)		
[Analog Output 1 Standardized Value] AO1R	Logic address: 148D hex = 5261	Type: INT (Signed16) Read/write: R/W Unit: -
Analog output 1 standardized value AQ1 real application image		

Base Monitoring

Code	Settings	
[Status Register] ETA	Logic address: 0C81 hex = 3201	Type: WORD (BitString16) Read/write: R Unit: -
Status Register • Bit0 = 1 : Ready to switch on • Bit1 = 1 : Switched on • Bit2 = 1 : Operation enabled • Bit3 = 1 : Detected error • Bit4 = 1 : Voltage enabled • Bit5 = 0 : Quick stop active • Bit6 = 1 : Switch on disabled • Bit7 = 1 : Alarm present • Bit8 : Reserved • Bit9 = 0 : Local mode control • Bit10 to Bit13: Reserved • Bit14 = 1 : Stop imposed by STOP key • Bit15 : Reserved		
[Motor Current] LCR	Logic address: 0C84 hex = 3204	Type: UINT (Unsigned16)

Code	Settings	
		Read/write: R Unit: 0.1 A
Motor current RMS Motor current. Average of the three line currents based on the measurement of the fundamental of the motor line currents.		
[Motor Therm State] THR	Logic address: 259E hex = 9630	Type: UINT (Unsigned16) Read/write: R Unit: 1 %
Motor thermal state This parameter monitors the motor thermal state. 100% corresponds to the nominal thermal state at the nominal motor current set to **[Motor Nom Current]** IN. Refers to the ATS480 User Manual NNZ85515 for more information.		
[Motor Run Time] RTH	Logic address: 0CAC hex = 3244	Type: UINT (Unsigned32) Read/write: R Unit: 1 s
Motor run time This parameter monitors how long the motor has been energized.		
[Elc Energy Cons] OCK	Logic address: 299C hex = 10652	Type: UINT (Unsigned32) Read/write: R/WS Unit: kWh
Electrical energy consumed by the motor (kWh)		
[Active Command Channel] CCC	Logic address: 20FA = 8442	Type: WORD (BitString16) Read/write: R Unit: -
Active command channel Active command channels status • Bit0 = 1 : Terminal board • Bit2 = 1 : Deported keypad • Bit3 = 1 : Modbus • Bit6 = 1 : CANopen • Bit9 = 1 : COM option board • Bit14 = 1 : Indus • Bit15 = 1 : SoMove		

Command Register

Code	Settings	
[Cmd Register] CMD	Logic address: 2135 hex = 8501	Type: WORD (BitString16) Read/write: R/W Unit: -

- Bit0 = 1 : ***Switch on*** Mains contactor control
- Bit1 = 1 : ***Enable voltage*** Authorization to supply power
- Bit2 = 0 : ***Quick Stop*** active
- Bit3 = 1 : ***Enable Operation*** Run command active
- Bit4 to Bit6: ***Reserved***
- Bit7 : ***Error reset request*** : active on rising edge
- Bit8 to Bit10: ***Reserved***
- Bit11 : ***Specific function assignment***
- Bit12 : ***Specific function assignment***
- Bit13 : ***Dynamic braking stop*** *(factory setting)*.
  The Bit can be set to an other function.
  NOTE: If no function is assigned, the Bit will return to his factory setting.
- Bit14 :***Decelerated stop order*** *(factory setting)*.
  The Bit can be set to an other function.
  NOTE: If no function is assigned, the Bit will return to his factory setting.
- Bit15 : ***Specific function assignment***

Extended Control Word

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

- Bit0 – ***Restore factory settings request***: Active on rising edge when motor is powered off. Once request is considered, this bit is automatically reset
- Bit1 – ***Store customer parameters request***: Active on rising edge when motor is powered off. Once request is considered, this bit is automatically reset
- Bit2 – ***Restore saved customer parameters***: Active on rising edge when motor is powered off. Once request is considered, this bit is automatically reset
- Bit3 = 1 : ***External error***: Active on rising edge
- Bit4 to Bit12: ***Reserved***
- Bit13 = 1 : ***Lock device when motor stopped***
- Bit14 = 1 : ***Disable line monitoring***
- Bit15 : ***Disable parameter consistency check***
  - Bit15 = 1 : no check of parameter consistency and device is locked when stopped
  - Bit15 = 0 : all parameters are validated

Fieldbus Integration Using Control Expert (M340)

Introduction

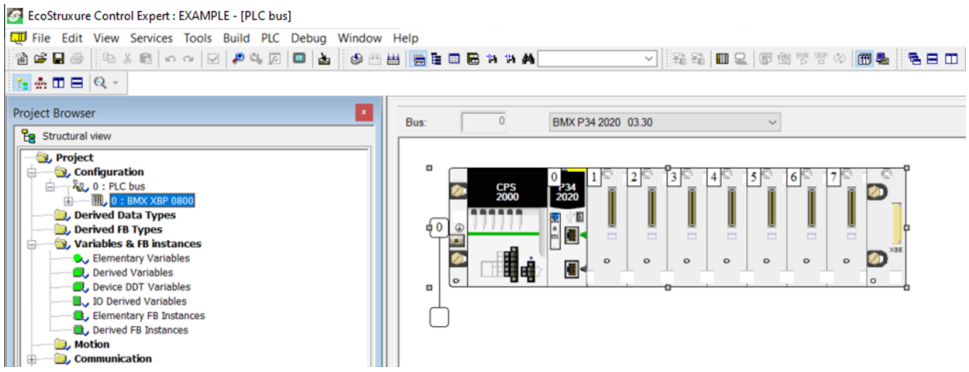
Overview

The following figure shows the basic configuration to control the soft starter with a M340 PLC.

Modbus RTU Configuration

Modbus RTU Port Configuration

From the project browser, open the Modbus RTU port configuration by double-clicking the Modbus RTU port.

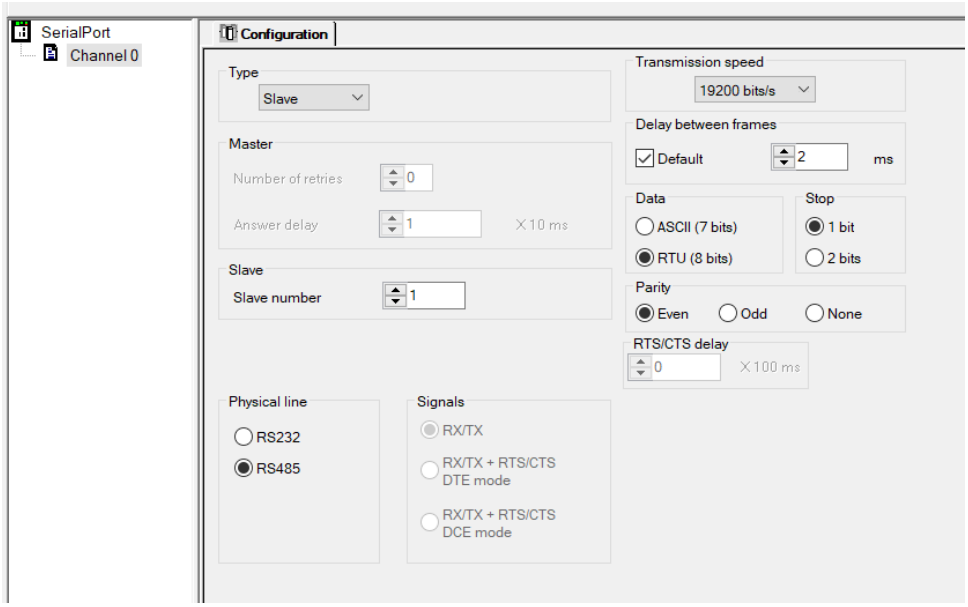


Configuration of the Client

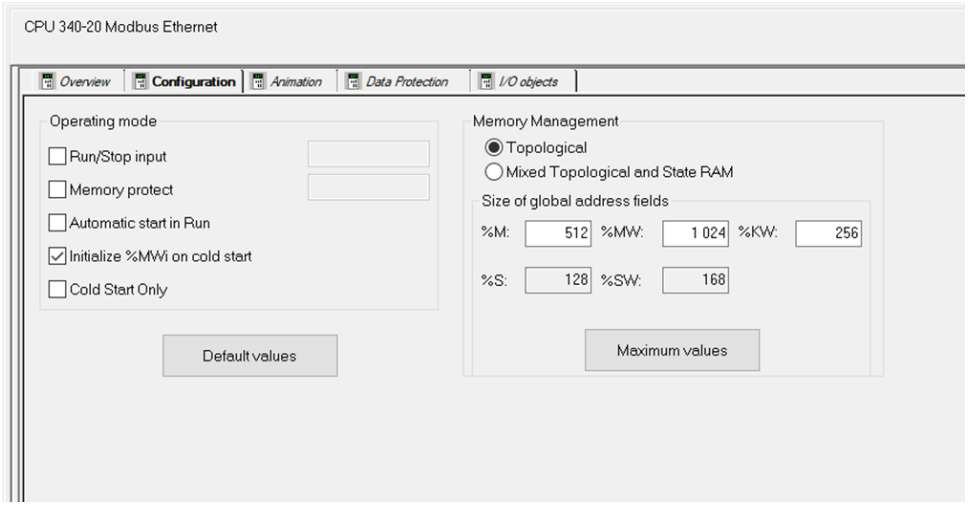
PLC Configuration

Click on the active port:

The configuration can be managed in the **Configuration** tab.



The configuration of the memory area of the PLC is set by default and can be modified.



Soft Starter Configuration with SoMove

Overview

In the following example, the soft starter configuration must be done as follows in-order to establish communication between the soft starter and the M340.

The soft starter configuration is done using the SoMove software.

Factory Settings

Before configuring the soft starter, make sure that you reset the soft starter to factory settings.

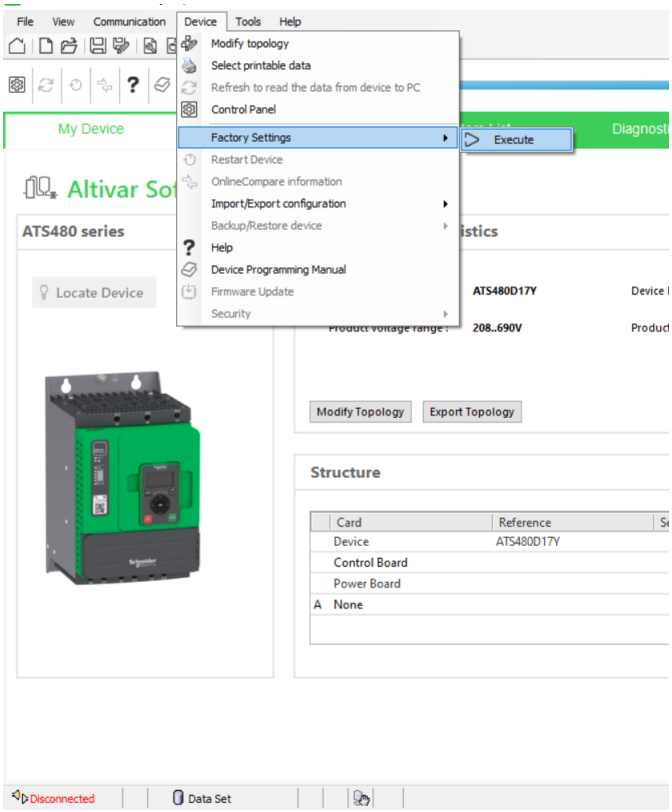
⚠WARNING

UNANTICIPATED EQUIPMENT OPERATION

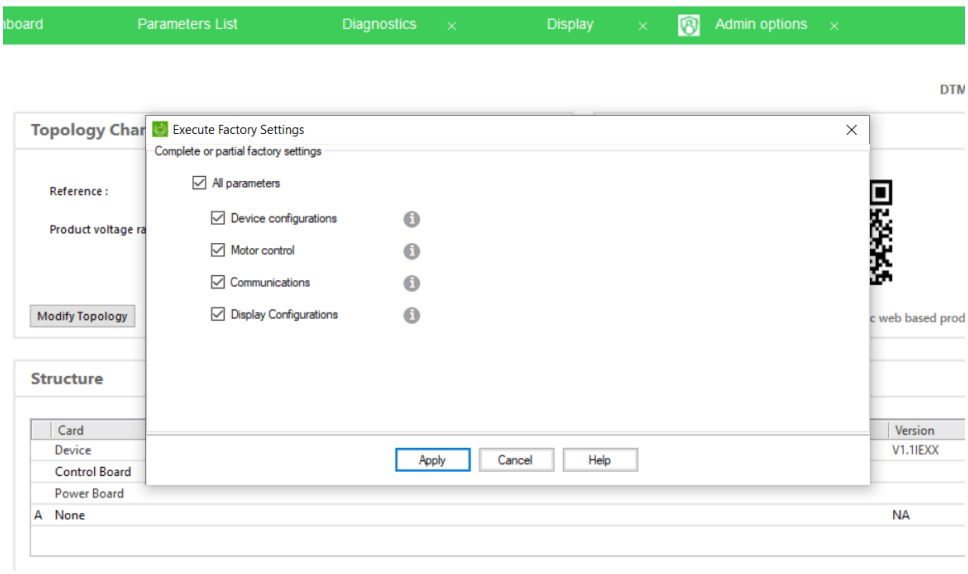
- Verify that restoring the factory settings or modifying the configuration is compatible with the type of wiring used.
- If you are recalling a stored configuration, perform a comprehensive commissioning test to verify correct operation.

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

- Right click on the device, select **Device menu > Factory Settings > Execute**:



Result: Following window is displayed:



- Select **All parameters**, then click on **Apply**

Result: The factory setting is applied to the soft starter configuration

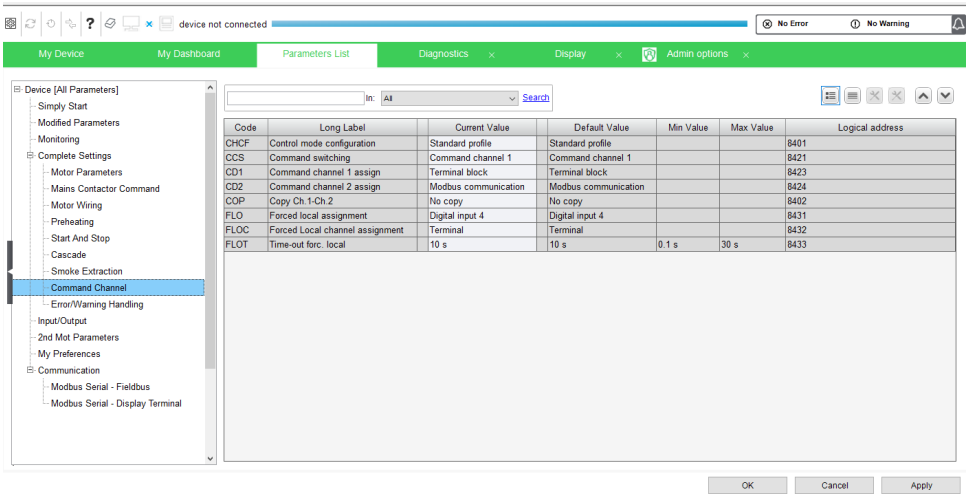
Command Configuration

To control the soft starter with the Modbus Embedded, select **Modbus Communication** as active command.

Go to:

- **Parameters List** tab
- Click on **Command channel** part

Result: Following window is displayed:

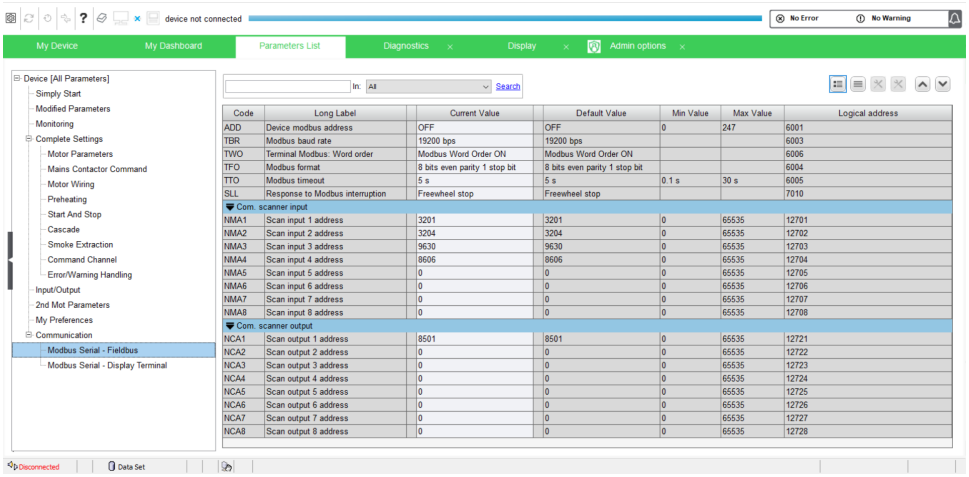


Modbus RTU Configuration

To perform the configuration of the Modbus Communication parameters of the soft starter, go to:

- **Communication, Modbus Serial – Fieldbus.**

Result: Following window is displayed:



Operations

Operating States

⚠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.**

Configuring Communication Error Response

The response of the soft starter in the event of a communication interruption can be configured.

Configuration can be performed using the display terminal from:

[Communication] COMO ➡ **[Communication Module]** COMO

Via the **[Modbus Error Resp]** SLL parameter.

The values of the **[Modbus Error Resp]** SLL parameter, which triggers a soft starter detected error **[Modbus Com Interruption]** SLF1 are:

Value	Meaning
[Freewheel Stop] YES	Motor triggers in error and is stopped in freewheel. **Factory setting**
[Deceleration] DEC	Motor is stopped in deceleration and triggers in error at the end of stop. The values are set to **[Deceleration]** DEC and **[End Of Deceleration]** EDC.
[Braking] BRK	Motor is stopped in dynamic braking and triggers in error at the end of stop. The values are set to **[Braking Level]** BRC and **[DC Braking To Stop]** EBA.

The values of the **[Modbus Error Resp]** SLL parameter which does not trigger a detected error are:

Value	Meaning
[Ignore] NO	Detected error ignored (in this case, the warning **[Modbus Com Warn]** SLLA is activated).
[Per STT] STT	Motor is stopped according to **[Type of stop]** STT parameter.

⚠WARNING

LOSS OF CONTROL

If this parameter is set to **[Ignore]** NO, Modbus communication monitoring is disabled.

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

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

Operating Modes

Configuration of the Soft starter for Operation with STD Profile

This section describes how to configure the settings of the soft starter if it is controlled in STD mode.

In the **[Complete settings]** CST- menu, **[Command channel]** CCP- submenu:

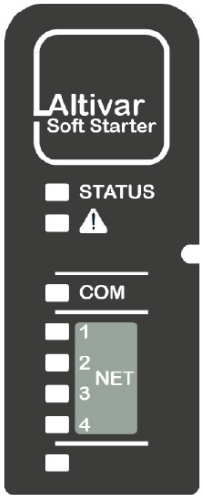
- **[Control Mode]** CHCF is set to **[Standard Profile]** STD.
- Check if **[Cmd channel 1]** CD1 (or **[Cmd channel 2]** CD2) is set on according to the communication source (**[Modbus]** MDB).

Diagnostics and Troubleshooting

Fieldbus Status LEDs

LED Indicators

The following figure describes the LEDs status for fieldbus monitoring:



LED Description

LED	Description
COM	Indicates the Modbus serial link connection status

LED COM : Link Activity

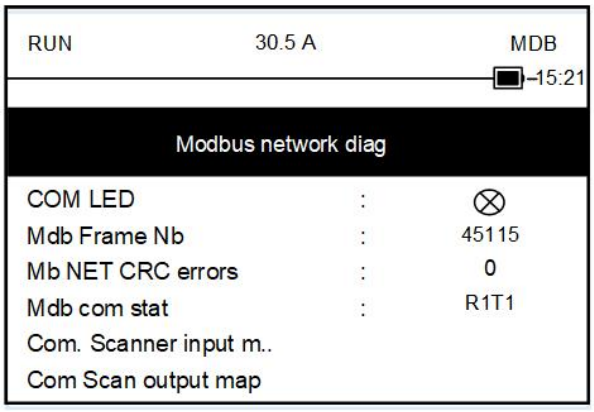
The table provides the LED status for Modbus serial connection

Color & Status	Description
OFF	No link
flashing	Fieldbus active

Communication Diagnostics

These parameters are visible only with the graphic display terminal.

On the terminal, in: **[Communication]** COM ➡ **[Communication map]** CMM ➡ **[Modbus network diag]** MND:



Modbus Counters

- **[Mdb Frame Nb]** M1CT indicate the number of Modbus frames received. The counter counts both correct and incorrect frames.
- **[Mb NET CRC errors]** M1EC indicate the number of Modbus frames containing checksum errors.

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

[Mdb Frame Nb] M1CT is modulo 65 536 counters, this means that, the value is reset to zero once the value of 65 535 is reached.

By contrast, the **[Mb NET CRC errors]** M1EC remain at 65 535 once this value is reached.

Each Modbus counter corresponds to a device parameter:

Menu	Parameter Name	Code	Logical Address
[Modbus network diag] MND	**[Mdb Frame Nb]**	M1CT	6011
	[Mb NET CRC errors]	M1EC	6010

Modbus Communication State

This can be accessed from the menu:

[Communication] COM ➡ **[Modbus network diag]** MND ➡ **[Mdb com stat]** COM1 :

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

[R0T1] R0T1: Modbus no reception, transmission

[R1T0] R1T0: Modbus reception, no transmission

[R1T1] R1T1: Modbus reception and transmission

Checking Connections

Description

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

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

Monitoring of Communication Channel

Command Channels

All the soft starter command parameters are managed on a channel-by-channel basis.

Parameter Name	Parameter Code			
	Taken Into Account by the Soft Starter	**Modbus Serial**	**CANopen**	**Fieldbus Module (PROFIBUS & Ethernet IP/MODBUS TCP)**
Control word	**[Cmd Register]** CMD	**[Modbus Cmd]** CMD1	**[CANopen Cmd]** CMD2	**[COM. Module cmd.]** CMD3
Extended Control word	**[Extended Control Word]** CMI	**[Extended Control Word]** CMI	**[Extended Control Word]** CMI	**[Extended Control Word]** CMI

Monitoring of Communication Channels

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

- The control word **[Cmd Register]** CMD from the active command channel
- The control word containing the command switch bit configured on **[Command Switching]** CCS

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 soft starter triggers a communication interruption.

The soft starter 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 soft starter 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 soft starter is only able to start if the channel involved in command value is enabled.

Example:

A soft starter in STD profile is connected to an active communication channel.

It is mandatory to write at least one time 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 soft starter copies the `run` commands value to the active channel (maintained).
- Monitoring of the active channels for the command resumes following a time delay **[Time-out forc. local]** FLOT.
- Soft starter control only takes effect once the soft starter has received the command from the active channels.

Communication Interruption Message

Description

If the device does not receive any Modbus request sent to its address for a predefined time **[ModbusTimeout]** `TTO`, a **[Modbus Com Interruption]** `SLF1` is triggered.

Glossary

A

Abbreviations:

Req. = Required

Opt. = Optional

AC:

Alternating Current

C

Client:

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

CRC16:

Cyclical Redundancy Check.

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:

Factory settings when the product is shipped

Fault Reset:

A function used to restore the soft starter 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

M

MEI:

Modbus Encapsulated Interface

Monitoring function:

Monitoring functions acquire a value continuously or cyclically (for example, by measuring) in order to check whether it is within permissible limits. Monitoring functions are used for error detection.

P

Parameter:

Device data and values that can be read and set (to a certain extent) by the user.

Q

Quick Stop:

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

R

R/WS:

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

S

Server:

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

W

Warning:

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

Z

Zone of operation:

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

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

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

NNZ85539.02 – 04/2022