# Altivar Soft Starter ATS480

## Soft Starter for Asynchronous Motor

## EtherNet/IP – Modbus TCP Manual - VW3A3720

NNZ85540.02
04/2022




www.se.com

# Legal Information

# Table of Contents


Safety Information ..... 7
- Qualification of Personnel ..... 8
- Intended Use ..... 8
- Product related information ..... 8

About the Book ..... 13
- At a Glance ..... 13
  - Validity note ..... 13
  - Document Scope ..... 13
  - Related Documents ..... 14
  - Electronic product data sheet ..... 15
  - Terminology ..... 15
  - Contact us ..... 16

Presentation ..... 17
- Hardware Overview ..... 17
- Software Overview ..... 18

Cybersecurity ..... 19
- Overview ..... 19
  - Security Policy ..... 22
  - Product Defense-in-Depth ..... 23
  - ATS480 Security Policy ..... 25
  - Potential Risks and Compensating Controls ..... 27
  - Data Flow Restriction ..... 28
- Initial Setup ..... 28
- Password ..... 28
- Security Event Logging ..... 29
- Upgrades Management ..... 30
- Clear Device / Secure Decommissioning ..... 31

Basics ..... 32
- Introduction ..... 32
- Profile ..... 33
  - Definition of a Profile ..... 33
  - Functional Profiles Supported by the Altivar Soft Starter ..... 34
  - Functional Description ..... 35
  - Standard Mode Operating State Diagram ..... 36
  - Description of Operating States ..... 37
  - Summary ..... 38
  - Command Register CMD ..... 39
  - Stop Commands ..... 40
  - Assigning Control Word Bits ..... 40
  - Status Word ETA ..... 41
  - Starting Sequence ..... 42
  - Sequence for a Soft starter ..... 43
  - Sequence for a Soft starter with Mains Contactor Control ..... 46
  - Automation Commissioning Only ..... 48
- Network Layer Supported Functions/Protocols ..... 49
- TCP and UDP Protocol ..... 51
- Modbus TCP Features ..... 53

Modbus TCP Frames ..... 53
Modbus TCP Servers ..... 54
Supported Modbus TCP Functions ..... 54
EtherNet/IP Features ..... 55
EtherNet/IP ..... 55
Cyclical Exchanges (Implicit Exchanges) ..... 56
Messaging (Explicit Exchanges) ..... 56
CIP Object ..... 57
Supported Object Classes ..... 57
Identity Object (01 hex) ..... 57
Message Router Object (02 hex) ..... 60
Assembly Object (04 hex) ..... 61
Connection Manager Object (06 hex) ..... 62
Modbus Object (44 hex) ..... 64
Application Object (70 hex to C7 hex) / Explicit Messaging ..... 65
Port Object (F4 hex) ..... 66
TCP/IP Interface Object (F5 hex) ..... 66
Ethernet Link Object (F6 hex) ..... 69
Hardware Setup ..... 72
Hardware Presentation ..... 72
Firmware Version ..... 72
Installation of the Module ..... 73
Electrical Installation ..... 74
Cable Routing Practice ..... 75
Accessories Presentation ..... 77
Software Setup ..... 78
Basic Settings ..... 78
Structure of the Parameter Table ..... 78
Finding a Parameter in This Document ..... 79
IP Parameter Settings ..... 80
**[Eth Module Config]** ETO ..... 81
**[Ethernet Module Diag]** MTE ..... 85
Communication parameters ..... 87
Additional Settings ..... 92
**[EnableOptWeb]** EWE ..... 92
User Authentication Settings ..... 92
FDR Settings ..... 95
RSTP Settings ..... 96
Bridge Settings & Ports Configuration ..... 96
Configuring I/O Scanning ..... 98
DNS Settings ..... 98
SNTP Settings ..... 99
SNMP Settings ..... 100
Fast Device Replacement ..... 102
Presentation ..... 102
Startup Detailed Behavior ..... 103
FDR Operation Behavior ..... 104
Local Configuration ..... 105
Downloaded Configuration ..... 106
Embedded Webserver ..... 109
Overview ..... 109

Connection to the Webserver ..... 109
My Dashboard ..... 112
Display - Device ..... 113
Setup - My Preference ..... 113
Fieldbus Integration Using Control Expert (M580) ..... 115
Introduction ..... 115
EtherNet/IP Configuration ..... 115
Configuration of the Client ..... 116
Soft Starter Configuration with Control Expert ..... 117
DTM Library ..... 120
DTM Browser ..... 120
Software Setup with Allen-Bradley PLC ..... 122
Introduction ..... 122
Soft Starter Configuration with SoMove ..... 122
PLC Configuration ..... 124
Operations ..... 130
Operating States ..... 130
Operating Modes ..... 133
Diagnostics and Troubleshooting ..... 134
Fieldbus Status LEDs ..... 134
Connection problem with the fieldbus module ..... 137
Monitoring of Communication Channel ..... 137
Control-Signal Diagnostics ..... 139
Glossary ..... 141

# 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.<br>• Do not include blank spaces in the reference or product range.<br>• 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.<br>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 install the Ethernet fieldbus on your drive.
- Show you how to configure the drive to use the Ethernet module for monitoring and control.
- Provide examples of setup using Ethernet communication.

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

## Related Documents

Use your tablet or your PC to quickly access detailed and comprehensive information on all our products on www.se.com The Internet site provides the information you need for products and solutions:

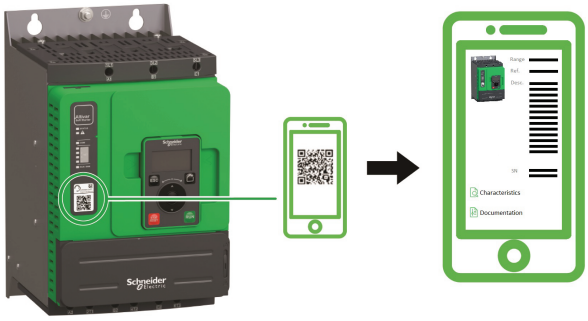
- The whole catalog for detailed characteristics and selection guides
- The CAD files to help design your installation, available in over 20 different file formats
- All software and firmware to maintain your installation up to date
- A large quantity of White Papers, Environment documents, Application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

The VW3A3720 is a dual port Ethernet modules that can be used in the following two industrial communication protocols :

- Modbus TCP
- EtherNet/IP

In addition, of the communication services provided by each protocol, the Ethernet module provides a set of services at the Ethernet and TCP/IP level.

The adapter offers an embedded Web server (in six languages) which offers comfortable displaying and commissioning functions directly from a standard web browser.

The following figure shows the hardware presentation of this module:

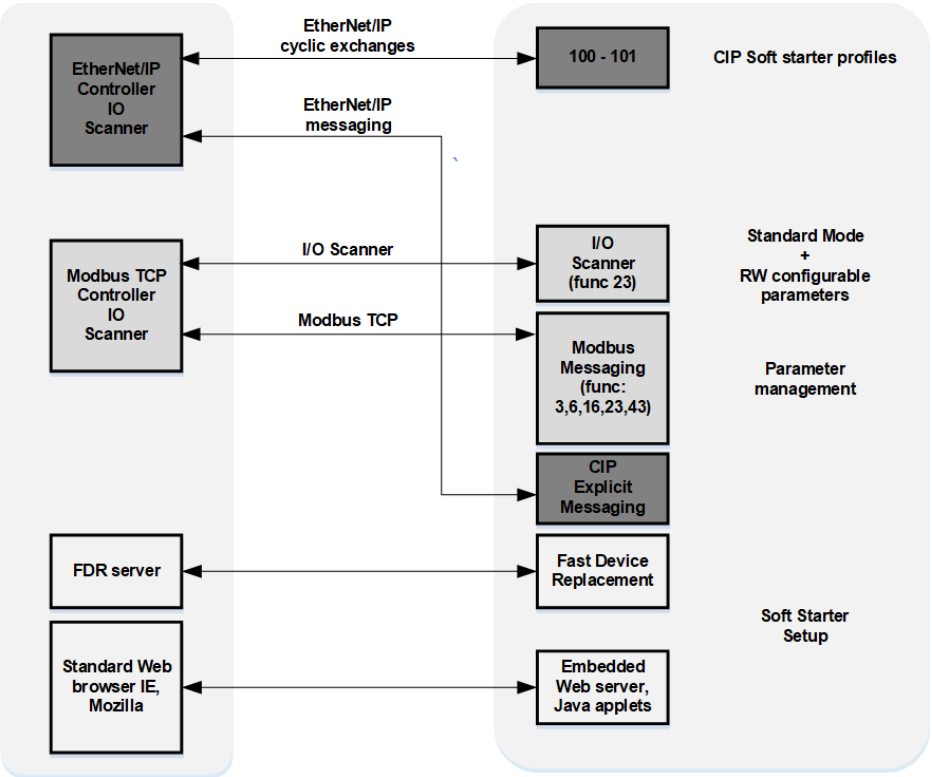
# Software Overview

## Simplified TCP/IP Model

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

| | |
|---|---|
| **Application** | Modbus TCP-EtherNet/IP |
| **Transport** | TCP / UDP |
| **Network** | IP |
| **Link** | Ethernet |

## Modbus TCP-EtherNet/IP Features Overview




**NOTE:** When using ModbusTCP, it is advisable to use function codes 16 or 23 to control the soft starter.

## Communication Parameter Addresses

For more information about the Communication Parameter Addresses, please refers to the ATS480 Communication Parameter Addresses NNZ85544, page 14.

# 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**<br>• Setup a security policy to your device and backup the device image with security administrator user account.<br>• Define and regularly review the password policy.<br>• Periodic change of the passwords, Schneider Electric recommends a modification of the password each 90 days.<br>**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**<br>• 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.<br>• For transmitting data over an external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.<br>**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.<br><br>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.<br><br>For transmitting data over external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.<br><br>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**<br>• Verify and regularly realign the synchronization of the device data & time.<br>**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 | Event information depending on the event category: |
| | • [ authn@3833 ] | • 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

## Introduction

### Modbus TCP

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

### EtherNet/IP

EtherNet/IP is a fieldbus based on TCP and UDP. EtherNet/IP extends Ethernet by an advanced industrial protocol (CIP, Common Industrial Protocol) as an application layer for automation applications in this way, Ethernet suites for industrial control. Products from different manufacturers can be networked without the need for special interface adaptation.

### TCP/IP and Ethernet Features

The product supports the following functions via:

- Manual IP address assignment
- Automatic IP address assignment via BOOTP or DHCP
- Automatic configuration data via FDR
- Commissioning via DTM-based commissioning software
- Diagnostics and configuration via integrated Web server
- Support of LLDP (Link Layer Discovery Protocol)
- Support of RSTP (Rapid Spanning Tree Protocol)
- Support of SNTP (Simple Network Time Protocol)
- Support of DNS (Domain Name System)
- Support of IPV6 for DPWS (Devices Profile for Web Services)
- Handling of QoS (Quality of Service)

### Web Server

The standard webserver (in six languages) provides access to pages such as:

- My dashboard
- Display
- Diagnostics
- Device
- Setup

# 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.

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

**NOTE:**

Fieldbus modules are incompatibles with **[Control Mode]** CHCF set to **[SE8 Profile]** SE8.

Using the **[SE8 Profile]** SE8 with an option module (CANopen, Ethernet, PROFIBUS DP) triggers an error **[Config Change]** CFF2.

To remedy:

- Press the **OK** key to validate the message displayed on the display terminal. This action will change **[Control Mode]** CHCF from **[SE8 Profile]** SE8 to **[Standard Profile]** STD
- Or turn Off the soft starter, remove the fieldbus module and turn On the soft starter.

### 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

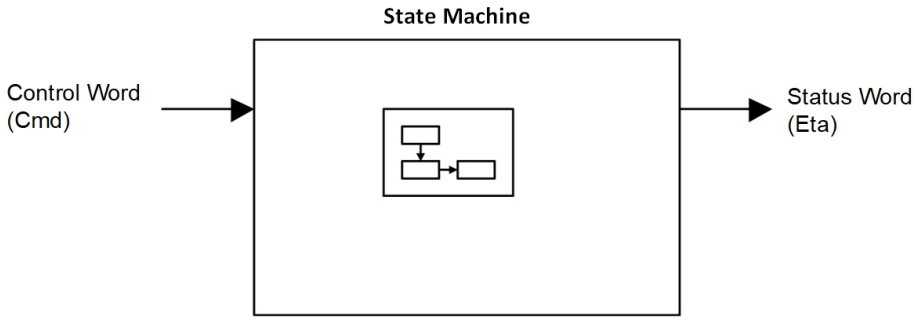
# Functional Description

## 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:



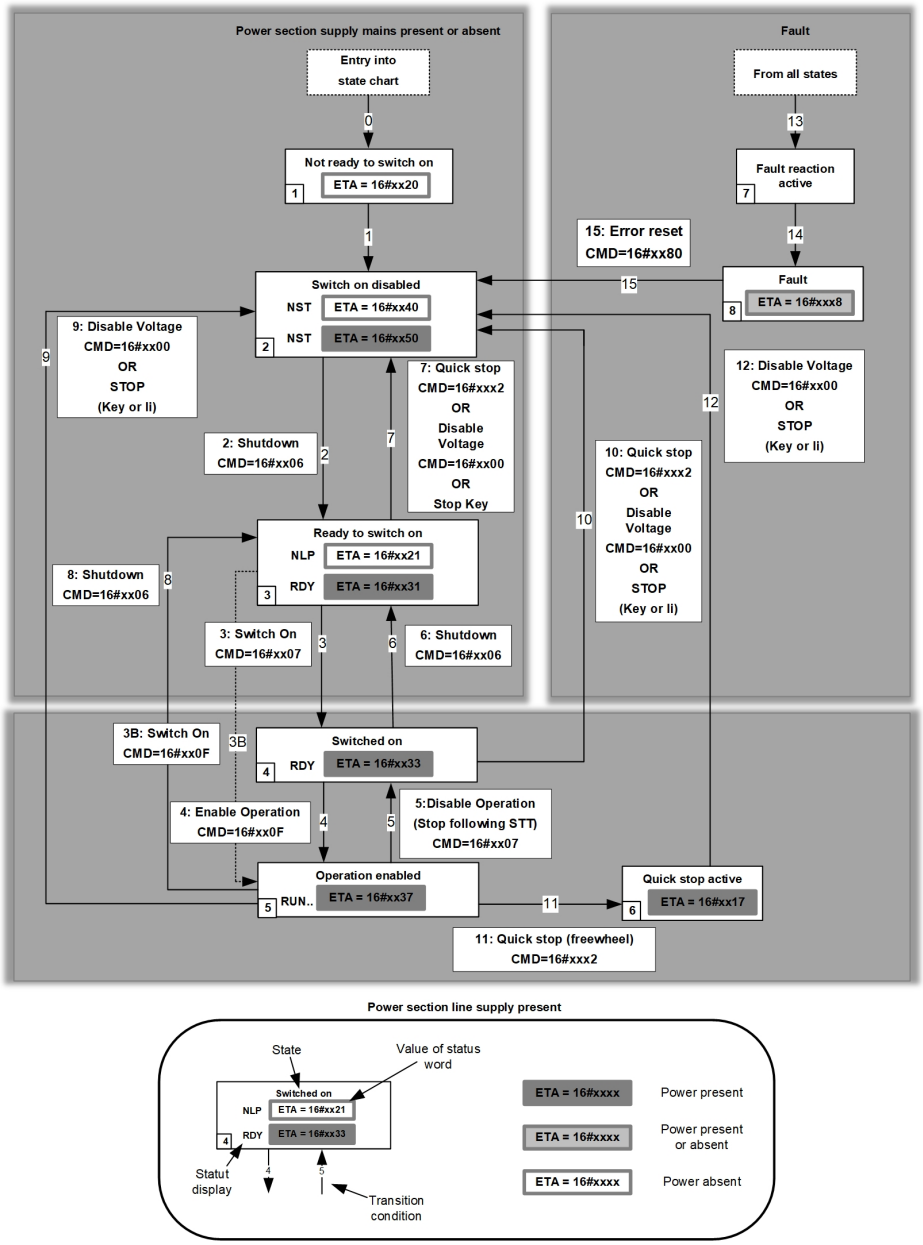
# Standard Mode Operating State Diagram

## 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.<br>The soft starter is locked, no power is supplied to the motor.<br>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.<br>The soft starter is locked, no power is supplied to the motor.<br>The configuration and adjustment parameters can be modified.<br>**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.<br>The power stage of the soft starter is ready to operate, but voltage has not yet been applied to the output.<br>The adjustment parameters can be modified.<br>**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.<br>**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<br>For a separate control stage with mains contactor, the contactor is closed.<br>The soft starter is unlocked, power is supplied to the motor.<br>The soft starter functions are activated and voltage is applied to the motor terminals.<br>If the Halt command is applied, no power is supplied to the motor.<br>The adjustment parameters can be modified.<br>The configuration parameters cannot be modified.<br>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*.<br>The soft starter stops according to freewheel stop and then remains in state *6 - Quick stop active* until:<br>• The **STOP** key is pressed or<br>• 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.<br>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*.<br>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*.<br>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)*.<br>The Bit can be set to an other function.<br>**NOTE:** If no function is assigned, the Bit will return to his factory setting. | ***Dynamic braking stop*** *(factory setting)*.<br>The Bit can be set to an other function.<br>**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<br>0 = run asked<br>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 | Fieldbus Module |
|---|---|
| Bit 11 | C311 |
| Bit 12 | C312 |
| Bit 13 is set to ***Dynamic braking stop*** *(factory setting)*.<br>This Bit can be set to an other function.<br>**NOTE:** If no function is assigned, the Bit will return to his factory setting. | C313 |
| Bit 14 is set to ***Decelerated stop order*** *(factory setting)*.<br>This Bit can be set to an other function.<br>**NOTE:** If no function is assigned, the Bit will return to his factory setting. | C314 |
| Bit 15 | C315 |

For example, to assign the preheating to bit15 of fieldbus module, simply configure the **[Preheating Assign]** PRHA parameter with the **[C315]** C315 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)<br>Command via fieldbus | Reserved (=0) |

| Operating State | Bit 6<br>Switch On Disabled | Bit 5<br>Quick Stop | Bit 4<br>Voltage Enabled | Bit 3<br>Fault | Bit 2<br>Operation Enabled | Bit 1<br>Switched On | Bit 0<br>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<br>0050 hex |
| *3 -Ready to switch on* | 0 | 1 | X | 0 | 0 | 0 | 1 | 0021 hex<br>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)...<br>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*.

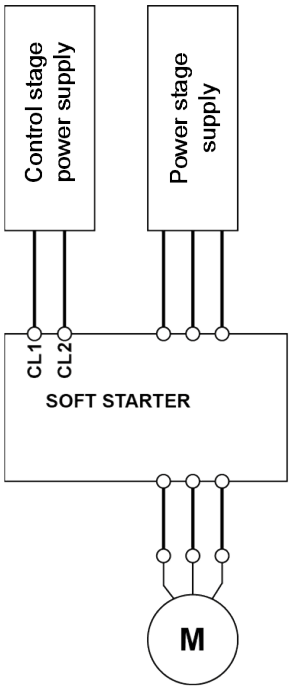
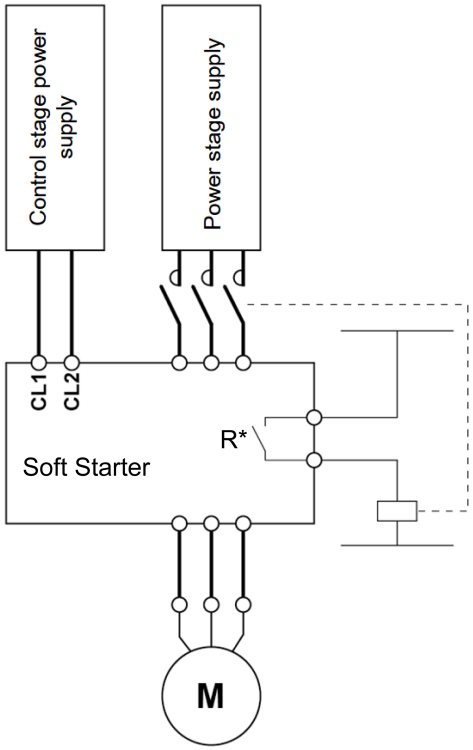
X: In this state, the value of the bit can be 0 or 1.

# 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<br>  | Mains contactor controlled by the soft starter (1)<br>  |

(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

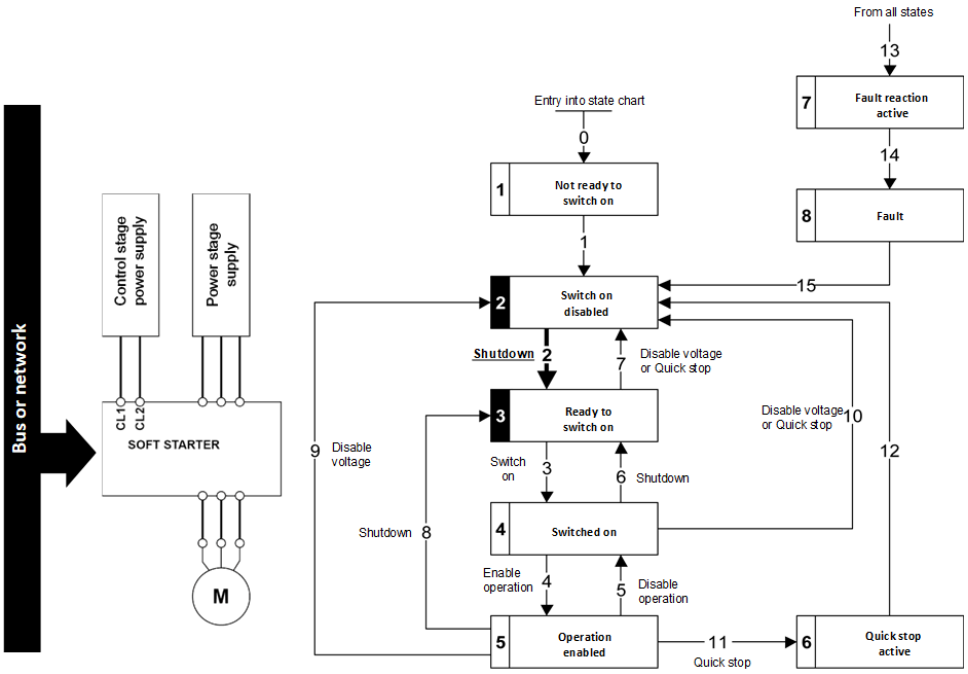
## Description

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.

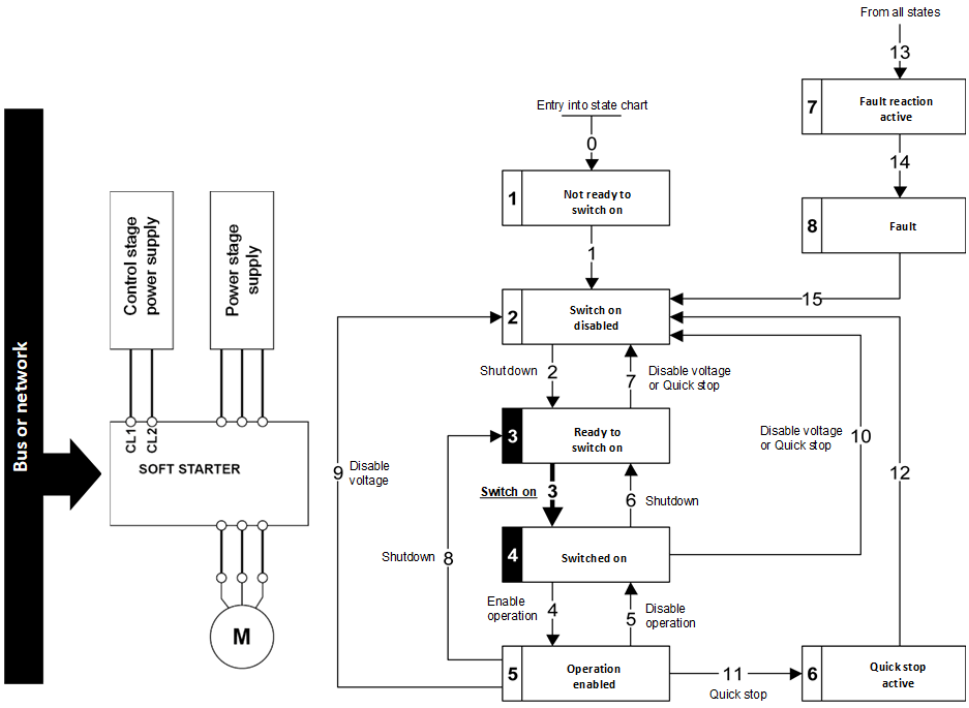


## Step 2

- 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 |

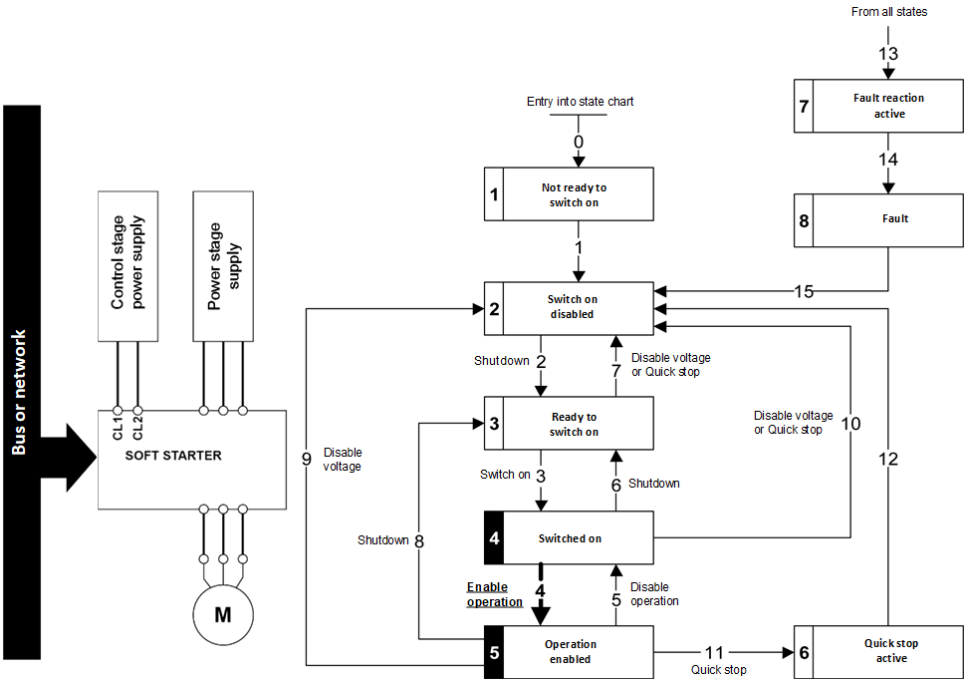
- Apply the *3 - Switch on* command



## 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

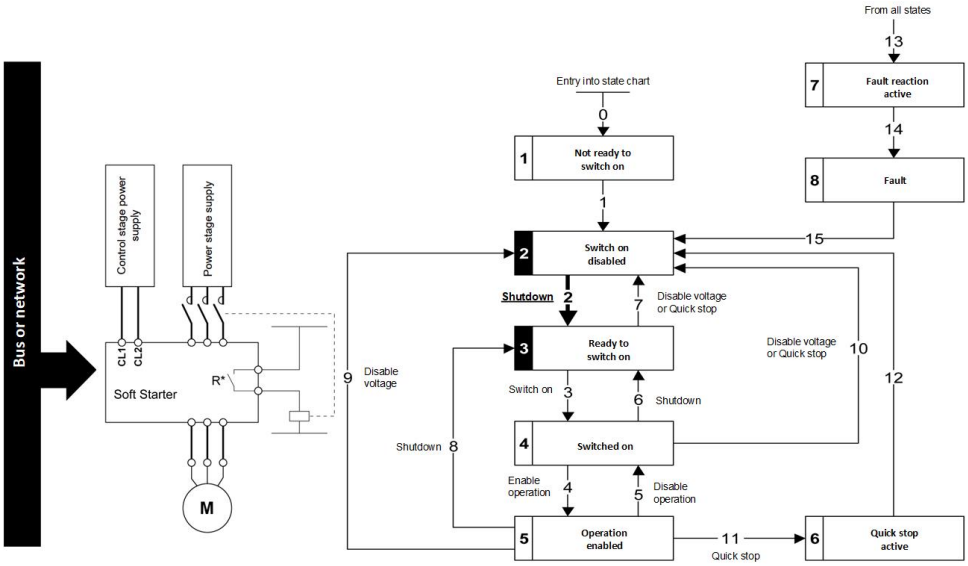
Power is supplied separately to the power and control stages.

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`

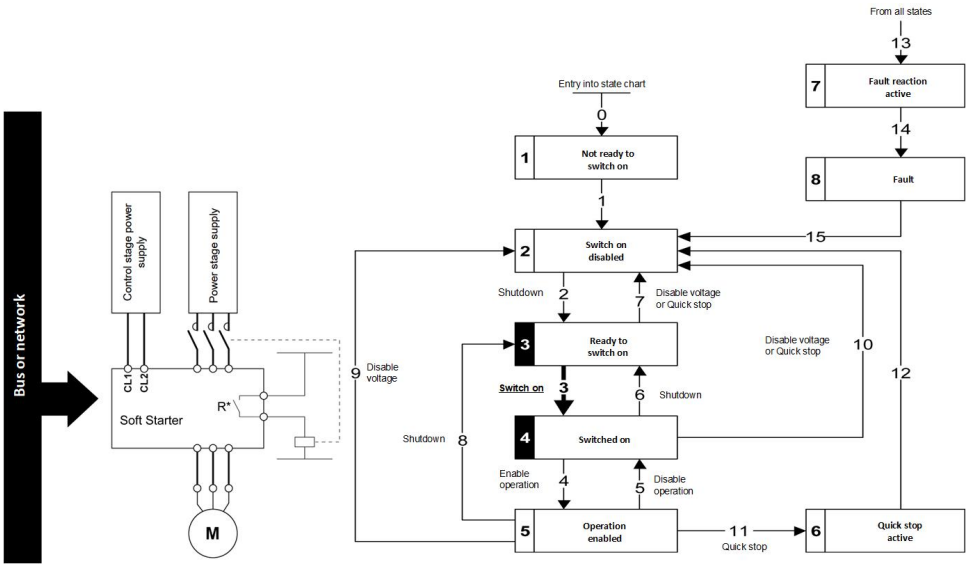
  **NOTE:** If `R1` is set to **[Isolating Relay]** `ISOL`, `R3` can't be set to **[Mains Contactor]** `LLC`.

- **[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:

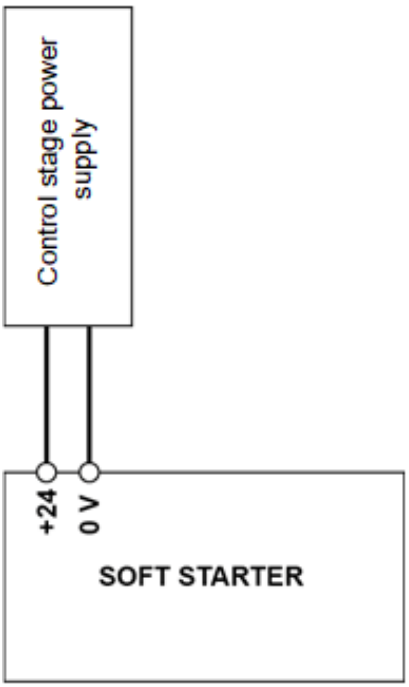
- **[R1 Assignment]** R1 is set to **[Isolating Relay]** ISOL

  **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. |

# Network Layer Supported Functions/Protocols

## ARP Protocol

The ARP (Address resolution protocol) is a protocol used to map network addresses (IP) to hardware addresses (MAC).

The protocol operates below the network layer as a part of the OSI link layer, and is used when IP is used over Ethernet. A host, wishing to obtain a physical address, broadcasts an ARP request onto the TCP/IP network. A unique IP address is assigned to the host, and is sent to its hardware address.

## ICMP Protocol

The VW3A3720 Ethernet modules manage the ICMP protocol.

- ICMP client: not supported
- ICMP server: the managed requests are the following:

| Type | Description |
|---|---|
| 0 | Echo reply (ping) |
| 3 | Destination unreachable |
| 4 | Sources quench |
| 5 | Redirect |
| 6 | Alternate host address |
| 8 | Echo request (ping) |
| 9 | Router advertisement |
| 10 | Router solicitation |
| 11 | Time exceeded |
| 12 | Parameter problem |
| 13 | Time stamp request |
| 14 | Time stamp reply |
| 15 | Information request |
| 16 | Information reply |
| 17 | Address mask request |
| 18 | Address mask reply |

## IP Protocol

The Ethernet adapter implements the IPV4 and IPV6 (for DPWS) protocols.

## SNMP Services

The Ethernet adapter accepts the community name “private” for writing and the community name “public” for Reading.

## MIB

| Objects | Description | Access | Default Value |
|---|---|---|---|
| `SysDescr` | Text description of the product | Read only | Schneider Electric Altivar Ethernet TCP/IP |
| `SysObjectID` | Points in the private MIB on the product part number | Read only | 1.3.6.1.4.1.3833.1.100.4.2 |

| Objects | Description | Access | Default Value |
|---|---|---|---|
| SysObjec-tRef | Soft starter reference | Read only | ATS4XX |
| SysUpTime | Time elapsed since the last power-up | Read only | Managed by the option |
| SysContact | Information allowing to contact the node manager | Read/write | " " |
| SysName | Node administrative name | Read/write | Device name |
| SysLocation | Physical location of the product | Read/write | " " |
| SysService | Indicates the service type offered by the product. | Read only | 72 |

# TCP and UDP Protocol

## Connections

## BOOTP and DHCP Protocol

The following table describes the DHCP frame format:

| | | | |
|---|---|---|---|
| OP (1 byte) | HTYPE (1 byte) | HLEN (1 byte) | HOPS (1 byte) |
| XID (4 bytes) | | | |
| SECS (2 bytes) | | FLAGS (2 bytes) | |
| CIADDR (4 bytes) | | | |
| YIADDR (4 bytes) | | | |
| SIADDR (4 bytes) | | | |
| GIADDR (4 bytes) | | | |
| CHADDR (16 bytes) | | | |
| SNAME (64 bytes) | | | |
| FILE (128 bytes) | | | |
| OPTIONS (312 bytes) | | | |

DHCP frame fields are described as follows:

| Field | Description |
|---|---|
| op | Message type DHCP request / DHCP reply |
| htype | Address hardware type |
| hlen | Hardware address length |
| hops | Used by relay agent |
| xid | Transaction identifier, random number chosen by the client allowing to associate the request and the response |
| secs | Time in seconds since the beginning of the transaction |
| flags | First bit used for the broadcast reply flag |
| ciaddr | Client IP address, only used if the client can respond to ARP request |
| yiaddr | Client IP address, “your” IP address proposed by the server |
| siaddr | IP address of the server |
| giaddr | Gateway IP address, used when a relay agent needs to be crossed |
| sname | Server name |
| file | Location of boot file |
| options | Optional parameters with DHCP extensions |

## DHCP Message

The DHCP protocol uses 8 different types of message during the IP assigning process.

The following table describes the 8 messages:

| Message | Description |
|---|---|
| DISCOVER | The client tries to discover the DHCP server using a broadcast |
| OFFER | The server proposes a configuration |
| REQUEST | The client chooses a DHCP server and declines other offers |

| Message | Description |
|---|---|
| ACK | The chosen server assigns the IP configuration |
| NAK | The server rejects the client request |
| DECLINE | The client declines the assigned IP configuration |
| RELEASE | The client releases Its IP address before the end of the lease |
| INFORM | The client asks for network information (it already has an IP address) |

## Operating Modes

The choice between DHCP, BOOTP, and fixed configuration is made through one parameter:

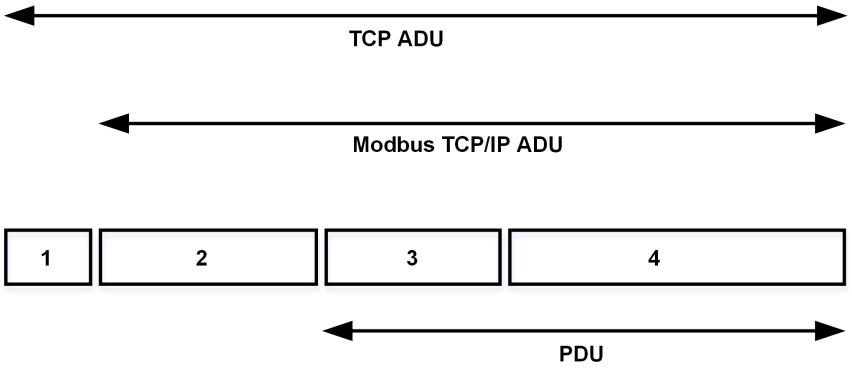
- Fixed: the Ethernet adapter uses the address stored in parameter.
- BOOTP: the Ethernet adapter receives the addresses from BOOTP server.
- DHCP: if the device name [XXX] is valid, the Ethernet adapter receives the addresses from the DHCP server.

# Modbus TCP Features

## Modbus TCP Frames

### TCP Telegrams

Modbus TCP telegrams are not only Modbus standard requests and responses encapsulated in TCP frames.




**1** TCP header

**2** MBPA: Modbus application protocol header

**3** ADU: Application data unit

**4** PDU: Protocol data unit (The Modbus message itself)

### MBAP Header Structure

| Fields | Length | Description | Client | Server |
|---|---|---|---|---|
| Transaction identifier | 2 bytes | Identification of a Modbus request / response transaction | Initialized by the client | Recopied by the server from the received request |
| Protocol identifier | 2 bytes | 0= Modbus protocol | Initialized by the client | Recopied by the server from the received request |
| Length | 2 bytes | Number of following bytes | Initialized by the client (request) | Initialized by the server (response) |
| Unit identifier | 1 byte | Identification of a remote adapter connected on a serial line or on other buses | Initialized by the client | Recopied by the server from the received request |

# Modbus TCP Servers

## Overview

| Unit ID | Modbus TCP server | Accessible parameters |
|---|---|---|
| 0/248 | Soft starter | See the file related to soft starter communication parameters. |
| 255 | Soft starter I/O scanner | See I/O scanner setting, page 55 |

# Supported Modbus TCP Functions

## Modbus TCP Services

The Modbus TCP option supports the following services:

| Function Name | Code | | Description | Remarks |
|---|---|---|---|---|
| | Dec | Hex | | |
| Read holding registers | 03 | 03 hex | Read N output words | Max PDU length: 125 words |
| Write 1 output word (Unit ID 0-248 only) | 06 | 06 hex | Write 1 output word | – |
| Write multiple registers | 16 | 10 hex | Write N output word | Max PDU length: 123 words |
| Read/write multiple registers (Uint ID 0-248 and 255) | 23 | 17 hex | Read/write multiple registers | Max PDU length: 121 words (W), 125 words (R) |
| (Subfunction)<br>Read device identification | 43/14 | 2B hex<br>0E hex | Encapsulated interface transport / read device identification | See the table below |

## Identification

| Id | Value | Comment |
|---|---|---|
| 00 hex | `Schneider Electric` | Device manufacturer |
| 01 hex | ATSXXX | Soft starter commercial part number |
| 02 hex | `0101` | Soft starter version |
| 04 hex | – | – |
| 05 hex | – | – |
| 06 hex | `Customized Name` | Device name |

## I/O Scanning Service

The I/O scanning service is used to exchange periodic I/O data between:

- A controller or PLC (I/O scanner).
- Devices (I/O scanning servers).

This exchange is performed by implicit requests, thus avoiding the need to program the controller (PLC).

The I/O scanner periodically generates the read/write multiple registers (23 = 17 hex) request. The I/O scanning service operates if it has been enabled in the PLC and in the soft starter. The soft starter parameters assigned to I/O scanning have been selected by default. This assignment can be modified by configuration.

When the I/O scanning service has been enabled in the soft starter:

- A TCP connection is assigned to it.
- The parameters assigned in the periodic variables are exchanged cyclically between the Ethernet adapter and the soft starter.
- The parameters assigned to the periodic output variables are reserved for I/O scanning. They cannot be written by other Modbus services, even if the I/O scanner is not sending its periodic output variables.

### I/O Scanner Setting

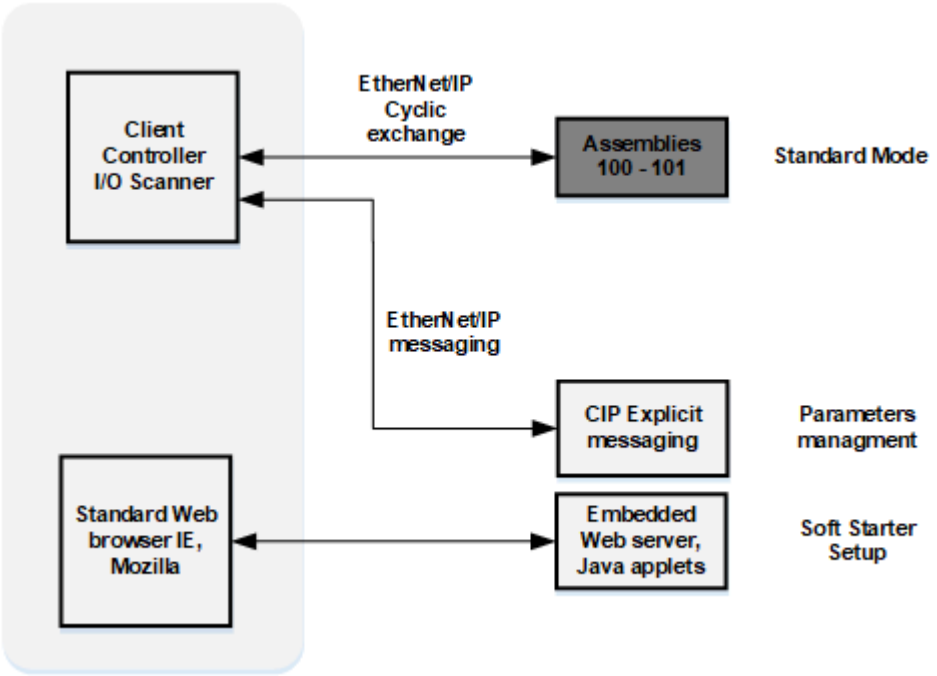
The communication scanner is managed through the DTM-based PC software.

| Channel | Factory Setting |
|---|---|
| Output 1 | CMD (8501) |
| Output 2 | OL1R (5212) |
| Output 3 | AO1C (5271) |
| Up to output 32 | 0 |
| Input 1 | ETA (3201) |
| Input 2 | LCR (3204) |
| Input 3 | THR (9630) |
| Input 4 | ERRD (8606) |
| Input 5 | IL1R (5202) |
| Input 6 | RTH (3244) |
| Input 7 | OCK (10562) |
| Input 8 | CCC (8442) |
| Up to Input 32 | 0 |

# EtherNet/IP Features

## EtherNet/IP

### EtherNet/IP Fieldbus Module Features Overview



The Ethernet adapter supports the following profiles:

- Soft starter standard profile for assembly 100 and 101.

In addition to these cyclic exchanges, the adapter also supports explicit messaging.

## Cyclical Exchanges (Implicit Exchanges)

### Overview

This part gives a description of the assembly sets and how to configure them.

### Principle of Control Configuration

By the configuration of the control, it is possible to decide from which channel the soft starter receives its commands either permanently or depending on a switching command. Numerous configurations are possible. For more information, refer to the user manual. The following configurations are some of the available possibilities.

The selection of the assembly set is made with the Ethernet Module.

### Control with Communication Scanner

If the assemblies selected are 100 and 101, the soft starter is controlled according to Standard profile.

By configuring the communication scanner, it is possible to assign any relevant parameter of the soft starter to the 32 input and 32 output variables of the assemblies. This is available through the DTM interface.

## Messaging (Explicit Exchanges)

### Introduction

Parameters of the soft starter can be accessed by R/W as CIP objects.

### Altivar Parameters Path

The soft starter parameters are grouped in classes:

- Each application class has only one instance.
- Each instance groups 200 parameters.
- Each attribute in an instance relates to a parameter.

The first parameter registered in the first application class (class code: 70 hex = 112) has the logical address 3000.

**Example**

The following table describes the examples of logical addresses:

| Logical Address | Hexadecimal | Decimal |
|---|---|---|
| 3000 | 70 hex / 01 hex / 01 hex | 112/1/1 |
| 3100 | 70 hex / 01 hex / 65 hex | 112/1/101 |
| 3200 | 71 hex / 01 hex / 01 hex | 113/1/1 |
| 64318 | A2 hex / 01 hex / 77 hex | 418/1/119 |

# CIP Object

## Supported Object Classes

### Introduction

Two categories of object classes can be defined:

- CIP device on EtherNet/IP
- Communications Adapter Device (0x0C) Profile

These objects are detailed in the following table:

| Object class | Class ID | Cat. | No. of instances | Effect on behavior interface |
|---|---|---|---|---|
| Identity | 01 hex | 1 | 1 | This object provides identification of and general information about the device |
| Message router | 02 hex | 1 | 1 | The Message Router Object provides a messaging connection point through which a Client may address a service to any object class or instance residing in the physical device |
| Assembly | 04 hex | 2 | 12 | The Assembly Object binds attributes of multiple objects, which allows data to or from each object to be sent or received over a single connection. |
| Connection manager | 06 hex | 1 | 1 | Use this object for connection and connectionless communications, including establishing connections across multiple subnets. |
| Modbus Object | 44 hex | 1 | 1 | ODVA describes how to encapsulate a Modbus frame using a CIP object.<br><br>Modbus Class Object presents the ethernet IP interface with the Modbus encapsulation service defined in the ODVA. |
| Application | 70 hex to C7 hex | 3 | 1 | Vendor-specific object - soft starter parameters. |
| Port Object | F4 hex | 1 | 1 | The port object represents the underlying interface of CIP which is EtherNet/IP. |
| TCP/IP interface | F5 hex | 1 | 1 | TCP/IP configuration. |
| Ethernet link | F6 hex | 1 | 1 | Counter and status information. |

## Identity Object (01 hex)

### Overview

This object provides identification of and general information about the device.

### Class Code

| Hexadecimal | Decimal |
|---|---|
| 01 hex | 1 |

## Class Attributes

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 1 | Get | Revision | UINT | X | Revision index of the class |
| 2 | Get | Max instances | UINT | 1 | 1 defined instance |
| 3 | Get | Number of instances | UINT | 1 | – |
| | | | | | |
| 6 | Get | Max ID of class attributes | UINT | 7 | – |
| 7 | Get | Max ID of instance attribute | UINT | 7 | – |

## Instance Attributes

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 1 | Get | Vendor ID | UINT | 0x00-F3 | – |
| 2 | Get | Device type | UINT | 0x00-0C | The value retrieved using the service GetDeviceType. |
| 3 | Get | Product code | UINT | 0x18-0B. | The value retrieved using the service GetDeviceType. |
| 4 | Get | Revision | Struct of: USINT<br>USINT | x | GetSoft starterVersion |
| 5 | Get | Status | WORD | – | See definition in the following table |
| 6 | Get | Serial number | UDINT | – | First byte: 18 hex<br>Second…Fourth byte: last 3 bytes of MAC-ID |
| 7 | Get | Product name | Struct of: USINT<br>STRING | – | ATSXXX |

## Attribute 5–Status

| Bit | Definition | How |
|---|---|---|
| 0 | Owned by scanner (predefined scanner/adapter connection) | No interface |
| 2 | Configured | If any of the product (option + soft starter) NVS attributes has changed from their default (out of box values).<br>**NOTE:** Network communications attributes are not included here. |
| 4 - 7 | Extended device status: See below | – |
| 8 | Minor recoverable Fault | No minor recoverable fault. |
| 9 | Minor unrecoverable Fault | No minor unrecoverable fault. |
| 10 | Major recoverable Fault | **[Fieldbus Com Interrupt]**CNF detected error or CIP connection timeout or Ethernet network overload. |

| Bit | Definition | How |
|---|---|---|
| 11 | Major unrecoverable Fault | **[Internal Link Error]**`ILF` detected error, EEPROM failed, OB hardware detected error. |
| Others | Reserved 0 | – |

## Bit 4-7 Definition

| Bit 4-7 | Definition | How |
|---|---|---|
| 0 0 0 0 | Self-testing or unknown | Not used |
| 0 0 0 1 | Firmware update in progress | Not used |
| 0 0 1 0 | At least on faulted I/O connection | – |
| 0 0 1 1 | No I/O connections established | – |
| 0 1 0 0 | Non-volatile configuration bad | Non-volatile memory detected error in OB |
| 0 1 0 1 | Major fault - either bit 10 or 11 is true | Bit 10 or 11 is true |
| 0 1 1 0 | At least one I/O connection in run mode | – |
| 0 1 1 1 | At least one I/O connection established, all in idle mode | – |
| 1 0 0 0<br>1 0 0 1 | Reserved, shall be 0 | – |
| 1 0 1 0 to<br>1 1 1 1 | Vendor specific | – |

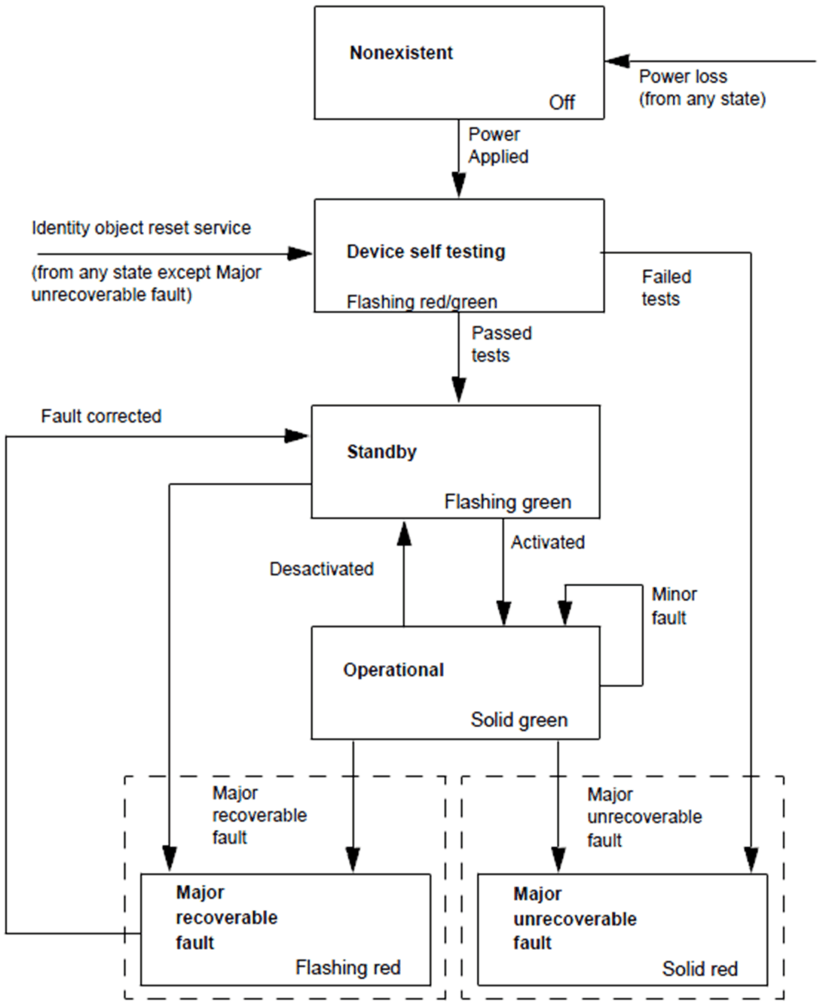
## Supported Class Services

| Service code | Service name | Description |
|---|---|---|
| 01 hex | `Get_Attribute_All` | Read all attributes |
| 0E hex | `Get_Attribute_Single` | Read one attribute |

## Supported Instance Services

| Service code | Service name | Description |
|---|---|---|
| 01 hex | `Get_Attribute_All` | Read all attributes |
| 0E hex | `Get_Attribute_Single` | Read one attribute |
| 10 hex | `Set_Attribute_Single` | Write one attribute |

### State Diagram for the Identity Object




## Message Router Object (02 hex)

### Overview

The Message Router Object provides a messaging connection point through which a Client may address a service to any object class or instance residing in the physical device

This is the element through which all the `Explicit messages` objects pass in order to be directed towards the truly destined objects.

### Class Code

| Hexadecimal | Decimal |
|---|---|
| 02 hex | 2 |

### Class Attributes

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 1 | Get | `Revision` | UINT | X | Revision index of the class |
| 2 | Get | `Max instances` | UINT | 1 | 1 defined instance |
| 3 | Get | `Number of instances` | UINT | 1 | – |

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 4 | Get | Optional attribute list | UINT | One of 1, 2, 3, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119 | – |
| 5 | Get | Optional service list | UINT | 10 | – |
| 6 | Get | Max ID of class attributes | UINT | 7 | – |
| 7 | Get | Max ID of instance attribute | UINT | 119 | – |

## Assembly Object (04 hex)

### Overview

The Assembly Object binds attributes of multiple objects, which allows data to or from each object to be sent or received over a single connection.

### Supported Class Attributes

| Attribute ID | Access | Name | Data type | Value | Detail |
|---|---|---|---|---|---|
| 1 | Get | Revision | UINT | X | Revision index of the class |
| 2 | Get | Max instances | UINT | 101 | One defined instance |
| 3 | Get | Number of instances | UINT | 2 | – |
| 4 | Get | Number of attributes | UINT | 1 | – |
| 6 | Get | Max ID of class attributes | UINT | 7 | – |
| 7 | Get | Max ID of instance attribute | UINT | 4 | – |

### Supported Instances

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 3 | Get/Set | Data | ARRAY OF BYTE | | |
| 4 | Get | Size | UINT | | |

### Supported Instances for Altivar Process

| Instance | Type | Name |
|---|---|---|
| 100 | AC Soft Starter output | `Native Soft Starter Output` |
| 101 | AC Soft Starter input | `Native Soft Starter Input` |

### Supported Class Services

| Service code | Service Name | Description |
|---|---|---|
| 0E hex | `Get_Attribute_Single` | Read one attribute |

### Supported Instance Services

| Service Code | Service Name | Description |
|---|---|---|
| 0E hex | `Get_Attribute_Single` | Read one attribute |
| 10 hex | `Set_Attribute_Single` | Write one attribute |

### Output Instance Data Description

| Instance | Byte | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|---|---|---|---|---|---|---|---|---|---|
| 100 | 0-1 | I/O Scanning word 1 | | | | | | | |
| | 2-3 | I/O Scanning word 2 | | | | | | | |
| | 4-5 | I/O Scanning word 3 | | | | | | | |
| | 6-7 | I/O Scanning word 4 | | | | | | | |
| | 8-9 | I/O Scanning word 5 | | | | | | | |
| | 10-11 | I/O Scanning word 6 | | | | | | | |
| 101 | 0-1 | Scanner Read word 1 | | | | | | | |
| | 2-3 | Scanner Read word 2 | | | | | | | |
| | 4-5 | Scanner Read word 3 | | | | | | | |
| | 6-7 | Scanner Read word 4 | | | | | | | |
| | 8-9 | Scanner Read word 5 | | | | | | | |
| | 10-11 | Scanner Read word 6 | | | | | | | |

## Connection Manager Object (06 hex)

### Overview

Use this object for connection and connectionless communications, including establishing connections across multiple subnets.

### Class Code

| Hexadecimal | Decimal |
|---|---|
| 06 hex | 6 |

## Class Attributes

| Attribute ID | Access | Name | Need | Data type | Value | Details |
|---|---|---|---|---|---|---|
| 1 | Get | Revision | Opt. | UINT | X | Revision index of the class |
| 2 | Get | Max instances | Opt. | UINT | 4 | 3 defined instance |

## Attributes of Instance 1 - Explicit Message Instance

| Attribute | Access | Name | Need | Data type | Value | Details |
|---|---|---|---|---|---|---|
| 1 | Get | State | Req. | USINT | – | 0: Non-existent<br>3: Established<br>5: Deferred Delete |
| 2 | Get | Instance_type | Req. | USINT | 0 | Explicit Message |
| 3 | Get | TransportClass_trigger | Req. | BYTE | 83 hex | Class 3 server |
| 4 | Get | Produced_connection_id | Req. | UINT | 10xxxxxx011 | xxxxxx = Node address |
| 5 | Get | Consumed_connection_id | Req. | UINT | 10xxxxxx100 | xxxxxx = Node address |
| 6 | Get | Initial_comm_ characteristics | Req. | BYTE | 21 hex | Explicit messaging via Group 2 |
| 7 | Get | Produced_connection_size | Req. | UINT | 36 | Produced data maximum size (in bytes) |
| 8 | Get | Consumed_connection_size | Req. | UINT | 36 | Consumed data maximum size (in bytes) |
| 9 | Get/Set | Expected_packet_rate | Req. | UINT | 2500 | 2.5 sec. (TimeOut) |
| 12 | Get/Set | Watchdog_timeout_action | Req. | USINT | 1 or 3 | 1: Auto-Delete<br>3: Deferred Delete (Default) |
| 13 | Get | Produced connection path length | Req. | UINT | 0 | Length of attribute 14 data |
| 14 | Get | Produced connection path | Req. | Array of UINT | Null | Not used |
| 15 | Get | Consumed connection path length | Req. | UINT | 0 | Length of attribute 16 data |
| 16 | Get | Consumed connection path | Req. | Array of UINT | Null | Not used |
| For details, refer to Ethernet/ specification for more information. | | | | | | |

## Supported Class Attributes

| Attribute ID | Ac-cess | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 1 | Get | Revision | UINT | X | Revision index of the class |
| 2 | Get | Max Instances | UINT | 1 | 1 defined instance |
| 3 | Get | Number of Instances | UINT | 1 | – |
| 4 | Get | Optional attribute list | STRUCT of | – | List of optional attribute numbers |
| 6 | Get | Max ID of class attributes | UINT | 7 | – |
| 7 | Get | Max ID of instance attributes | UINT | 8 | Attribute ID number of last class attribute |

### Supported Instance1 (Explicit) Attributes

| Attribute ID | Access | Name | Data type | Details |
|---|---|---|---|---|
| 1 | Get | Open Requests | UINT | Number of forward open service requests received. |
| 2 | Get | Open Format Rejects | UINT | Number of forward open service requests which were rejected due to bad format. |
| 3 | Get | Open Resources Rejects | UINT | Number of forward open service requests which were rejected due to lack of resources. |
| 4 | Get | Open Other Rejects | UINT | Number of forward open service requests which were rejected for reasons other than bad format or lack of resources. |
| 5 | Get | Close Requests | UINT | Number of forward close service requests received. |
| 6 | Get | Close Format Requests | UINT | Number of forward close service requests which were rejected due to bad format. |
| 7 | Get | Close Other Requests | UINT | Number of forward close service requests which were rejected for reasons other than bad format. |
| 8 | Get | Connection Timeouts | UINT | Total number of connection timeouts that have occurred in connections controlled by this connection manager. |

### Supported Class Services

| Service code | Service name | Description |
|---|---|---|
| 01 hex | Get_Attribute_All | Read all attributes |
| 0E hex | Get_Attribute_Single | Read one attribute |

### Supported Instance Services

| Service code | Service name | Description |
|---|---|---|
| 0E hex | Get_Attribute_Single | Read one attribute |
| 10 hex | Set_Attribute_Single | Write one attribute |
| 4E hex | Forward_Close | Closes a connection |
| 54 hex | Forward_Open | Opens a connection, maximum data size is 511 bytes |

## Modbus Object (44 hex)

### Overview

ODVA describes how to encapsulate a Modbus frame using a CIP object.

Modbus Class Object presents the ethernet IP interface with the Modbus encapsulation service defined in the ODVA.

### Class Code

| Hexadecimal | Decimal |
|---|---|
| 44 hex | 44 |

# Application Object (70 hex to C7 hex) / Explicit Messaging

## Overview

The whole parameter mapping of the soft starter be accessible through the Application objects.

## Application Object Behavior

Class = ((AdL - 3000) / 200) + 70 hex

Instance = 1

Attribute = (AdL % 200) + 1

AdL = (class - 70h) * 200 + attribute - 1 + 3000

This rule allows the access to address under 20599. The other addresses are not accessible.

The soft starter parameters are grouped into classes.

- Each application class has only one instance.
- Each instance groups 200 parameters.
- Each attribute in an instance relates to a parameter.

## Supported Class Attributes

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 1 | Get | Revision | UINT | X | Revision index of the class |
| 2 | Get | Max Instances | UINT | 1 | One defined instance |
| 3 | Get | Number of Instances | UINT | 1 | – |
| 6 | Get | Max ID of class attributes | UINT | 6 | – |
| 7 | Get | Max ID of instance attribute | UINT | X | – |

## Supported Instance Attributes

| Attribute ID | Access | Name | Data type | Details |
|---|---|---|---|---|
| 1 | Get/ Set | 1st parameter of the block | UINT | Value returned by the soft starter at address xx |
| – | – | – | – | Value returned by the soft starter at address xx |
| X | Get/ Set | Last parameter of the block | UINT | Value returned by the soft starter at address xx |

## Supported Class Services

| Service code | Service name | Description |
|---|---|---|
| 0E hex | Get_Attribute_Single | Read one attribute |

### Supported Instance Services

| Service code | Service name | Description |
|---|---|---|
| 0E hex | Get_Attribute_Single | Read one attribute |
| 10 hex | Set_Attribute_Single | Write one attribute |

## Port Object (F4 hex)

### Overview

The port object represents the underlying interface of CIP which is EtherNet/IP.

### Class Code

| Hexadecimal | Decimal |
|---|---|
| F4 hex | 244 |

### Class Attributes

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 1 | Get | Revision | UINT | X | Revision index of the class |
| 2 | Get | Max instances | UINT | 2 | 2 defined instance |
| 3 | Get | Number of instances | UINT | 2 | – |
| 6 | Get | Max ID of class | UINT | 9 | – |
| 7 | Get | Max ID of instance | UINT | 11 | – |
| 8 | Get | Entry port | UINT | 2 | – |
| 9 | Get | Port Instance Info | UINT | 0x000-2 0004 0001 0001 0000 0000 | – |

## TCP/IP Interface Object (F5 hex)

### Overview

The TCP/IP Interface Object provides the mechanism to configure a device's TCP/IP network interface. Examples of configurable items include the device's IP Address, Network Mask, and Gateway Address.

### Supported Class Attributes

| Attribute ID | Ac-cess | Name | Data type | Value | Detail |
|---|---|---|---|---|---|
| 1 | Get | Revision | UINT | X | Revision index of the class |
| 2 | Get | Max instances | UINT | 1 | 1 defined instance |
| 3 | Get | Number of instances | UINT | 1 | – |
| 4 | Get | Optional attribute list | UINT | 0x00-11 0010 0009 | – |

| Attribute ID | Access | Name | Data type | Value | Detail |
|---|---|---|---|---|---|
| | | | | 0008 0004 | |
| 6 | Get | Max ID of class attributes | UINT | 7 | – |
| 7 | Get | Max ID of instance attribute | UINT | 17 | – |

## Supported Instance Attributes

| Attribute ID | Access | Name | Data type | Detail |
|---|---|---|---|---|
| 1 | Get | Status | DWORD | 0 = The interface configuration attribute has not been configured<br>1 = The interface configuration attribute contains valid configuration |
| 2 | Get | Configuration capability | DWORD | Bit 0 = 1 (TRUE) shall indicate that the device is capable of obtaining its network configuration via BOOTP<br>Bit 1 = 1 (TRUE) shall indicate that the device is capable of resolving host names by querying a DNS server<br>Bit 2 = 1 (TRUE) shall indicate that the device is capable of obtaining its network configuration via DHCP<br>Bit 3 = 1 (TRUE) shall indicate that the device is capable of sending its host name in the DHCP request<br>Bit 4 = 1 (TRUE) shall indicate that the Interface Configuration attribute is settable.<br>Bit 5-31: reserved |
| 3 | Get/Set | Configuration control | DWORD | Bits 0-3 start-up configuration<br>0 = The device shall use the interface configuration values previously stored<br>1 = The device shall obtain its interface configuration values via BOOTP<br>2 = The device shall obtain its interface configuration values via DHCP upon start-up (1)<br>3-15 = Reserved for future use<br>Bit 4 = 1 (TRUE), the device shall resolve host names by querying a DNS server<br>Bit 5-31: reserved |
| 4 | Get | Physical link object | STRUCT of<br>UINT<br>EPATH | Path size<br>Path: Logical segments identifying the physical link object<br>Example [20][F6][24][01]: [20] = 8-bit class segment type;<br>[F6] = Ethernet link object class; [24] = 8-bit instance segment type; [01] = instance 1 |
| 5 | Get/Set | Interface configuration | STRUCT of<br>UDINT<br>UDINT<br>UDINT<br>UDINT<br>UDINT<br>String | IP address (0: no address configured)<br>Network mask (0: no network mask configured)<br>Gateway address (0: no address configured)<br>Name server address (0: no address configured)<br>Name server address 2 (0: no address configured) |

| Attribute ID | Access | Name | Data type | Detail |
|---|---|---|---|---|
| | | | | Domain name |
| 6 | Get/Set | Host name | String | Read/write name of the soft starter |
| 8 | Get/Set | TTL value | USINT | TTL value for EtherNet/IP multicast packets |
| 9 | Get/Set | Mcast config | Struct Of. | IP multicast address configuration |
| | | Alloc control | USINT | 0 - Use default allocation algorithm to generate multicast addresses<br>1 - Multicast addresses shall be allocated according to the values in Num Mcast and Mcast Start Addr |
| | | Reserved | USINT | Shall be 0 |
| | | Num Mcast | UINT | Number of multicast addresses to allocate for EtherNet/IP |
| | | Mcast Start Addr | UDINT | Starting multicast address from which to begin allocation |

(1) If set option board parameter OBP:FDRU=0 is also set to implicitly disable the FDR mechanism on the DHCP protocol. This to be compatible with CIP tools that has configured the device to operate in a non-FDR specific environment. You have to manually enable the feature if you wish to use it.

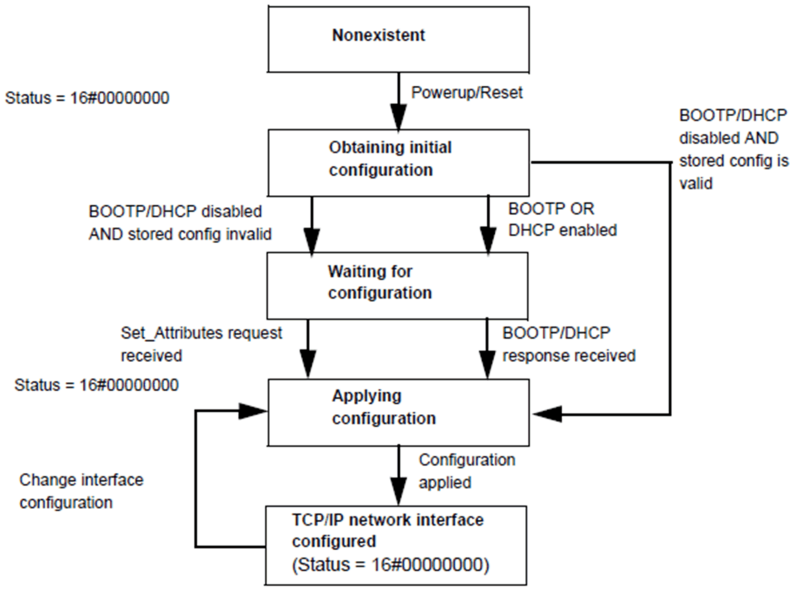
## Supported Class Services

| Service code | Service name | Description |
|---|---|---|
| 01 hex | Get_Attribute_All | Read all attributes |
| 0E hex | Get_Attribute_Single | Read one attribute |
| 10 hex | Set_Attribute_Single | Write one attribute |

## Supported Instance Services

| Service code | Service name | Description |
|---|---|---|
| 0E hex | Get_Attribute_Single | Read one attribute |
| 10 hex | Set_Attribute_Single | Write one attribute |
| 01 hex | Get_Attribute_All | – |

### TCP/IP Interface Behavior




## Ethernet Link Object (F6 hex)

### Overview

The Ethernet Link Object maintains link-specific counters and status information for an IEEE 802.3 communications interface. Each device shall support exactly one instance of the Ethernet Link Object for each IEEE 802.3 communications interface on the module.

### Class Attributes

| Attribute ID | Access | Name | Data type | Value | Details |
|---|---|---|---|---|---|
| 1 | Get | `Revision` | UINT | X | Revision index of the class |
| 2 | Get | `Max instances` | UINT | 2 | 2 defined instance |
| 3 | Get | `Number of instances` | UINT | 2 | – |
| 4 | Get | `Optional attribute list` | UINT | One of 4, 7, 8, 9, 10 | – |
| 6 | Get | `Max ID of class attributes` | UINT | 7 | – |
| 7 | Get | `Max ID of instance attribute` | UINT | 11 | – |

### Supported Instance Attributes

| Attribute ID | Access | Name | Data type | Detail |
|---|---|---|---|---|
| 1 | Get | `Interface speed` | UDINT | Interface speed currently in use |
| 2 | Get | `Interface flags` | DWORD | Bit 0: Link status indicates whether the Ethernet 802.3 communications interface is connected to an active network. 0 indicates an inactive link; 1 indicates an active link<br><br>Bit 1: Half/Full duplex indicates the duplex mode currently in use. 0 indicates that the interface is running half duplex; 1 indicates full duplex |

| Attribute ID | Access | Name | Data type | Detail |
|---|---|---|---|---|
| | | | | Bit 2-4: Negotiation status<br>• 0: Auto-negotiation in progress<br>• 1: Auto-negotiation and speed detection not successful<br>• 2: Auto negotiation not successful but detected speedduplex was defaulted<br>• 3: Successfully negotiated speed and duplex<br>• 4: Auto-negotiation not attempted. Forced speedand duplex<br>Bit 5: Manual setting require reset<br>• 0: Indicates that the interface can activate changes to link parameters (autonegotiate, duplex mode, interface speed) automatically<br>• 1: Indicates that the device requires a reset service be issued to its identity object in order for the changes to take effect.<br>Bit 6: Local hardware error<br>• 0: Indicates that the interface detects no local hardware error<br>• 1: Indicates that a local hardware error is detected. The meaning of this is product-specific<br>Bit 7-31: Reserved shall be set to zero |
| 3 | Get | Physical address | USINT [6] | MAC layer address |
| 4 | Get | Interface counters | – | – |
| 5 | Get | Media counters | – | – |
| 6 | Get/Set | Interface control | – | Force auto negotiate, half full and speed |
| 7 | Get | Interface type | USINT | 2 |
| 10 | Get | Interface label | SHORT_STRING | Service code |

## Supported Class Services

| Service code | Service name | Description |
|---|---|---|
| 0E hex | Get_Attribute_Single | Read one attribute |
| 01 hex | Get_Attribute_All | – |

## Supported Instance Services

| Service code | Service name | Description |
|---|---|---|
| 0E hex | Get_Attribute_Single | Read one attribute |
| 10 hex | Set_Attribute_Single | Write one attribute |
| 01 hex | Get_Attribute_All | – |
| 4C hex | Get_And_Clear | Same than Get_Attribute_Single |

## Optional Attributes List

| Service code | Access | Name | Data Type | Description |
|---|---|---|---|---|
| 08 hex | Get | Interface State | USINT | Current State |
| 09 hex | Get/Set | Admin State | USINT | Administrative State: Enable or Disable |

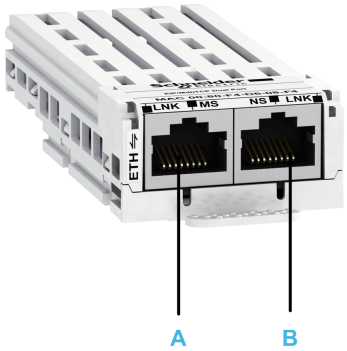
# Hardware Setup

## Hardware Presentation

### Ethernet Dual Port

The figure shows VW3A3720 Ethernet Module equipped with 2 RJ45 connectors:

**NOTE:** The VW3A3721 module has the same comportment as the VW3A3720.




| Item | Description | Comment |
|---|---|---|
| A | Port A | RJ45 connector |
| B | Port B | RJ45 connector |

## Firmware Version

### VW3A3720 Compatibility

ATS480 soft starters with, at least, V1.1IE01 software version, are only compatible with VW3A3720 Ethernet module versions V2.1 and higher.

# Installation of the Module

## Before Starting

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

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

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

**⚠⚠DANGER**

**ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION**

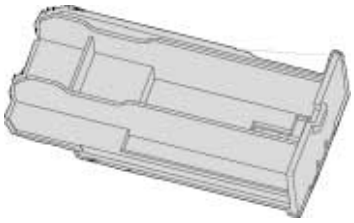
Do not use damaged products or accessories.

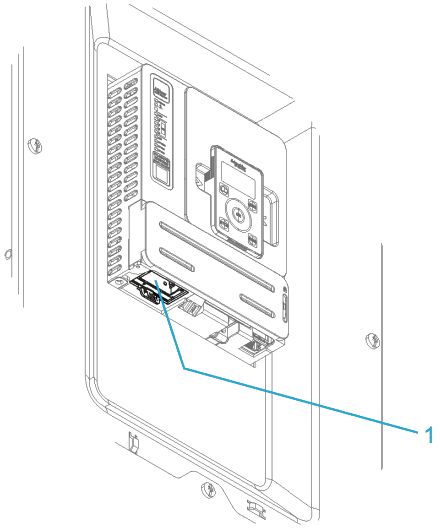
**Failure to follow these instructions will result in death or serious injury.**

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

## Insertion of the Fieldbus Module

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

| Step | Action |
|---|---|
| 1 | Ensure that the power is off. |
| 2 | Locate the fieldbus module slot on the bottom of the control part. |
| 3 | Remove the false module (VY1G480C01) with the help of a screwdriver.  |
| 4 | Insert the module. |
| 5 | Check that the module is correctly inserted and locked mechanically in the soft starter. |
| 6 | Add the corresponding sticker on the LED front panel of the soft starter. |




**1** Fieldbus Module Slot

### Removal of the Fieldbus Module

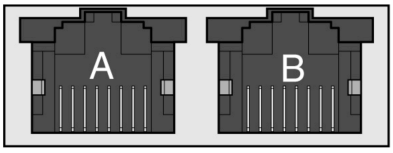
The table provides the procedure for removal of the fieldbus module from the soft starter:

| Step | Action |
|---|---|
| 1 | Ensure that the power is off. |
| 2 | Press the strip.<br>  |
| 3 | Remove the module while maintaining the strip pressed. |

# Electrical Installation

## Pin Layout

The VW3A3720 Ethernet module is equipped with 2 RJ45 female sockets for the Ethernet connection.




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

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

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

## Cable Specification

Cable specifications are as follows:

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

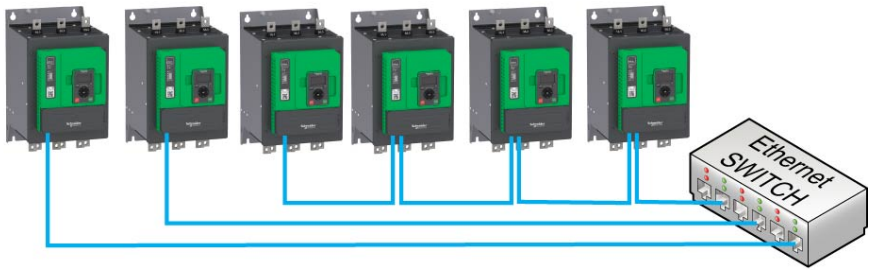
**NOTE:** RSTP function is not compatible with half duplex configuration. All devices involved in the RSTP topology shall be RSTP capable and configured.

# Cable Routing Practice

## Installation Topology

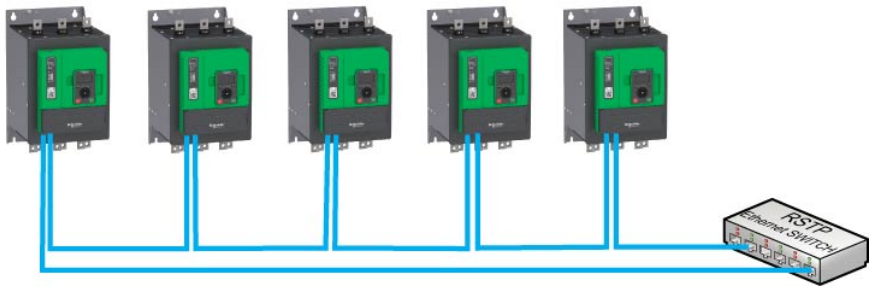
The Ethernet adapter enables several wiring solutions:

- Daisy chain and/or Star topology

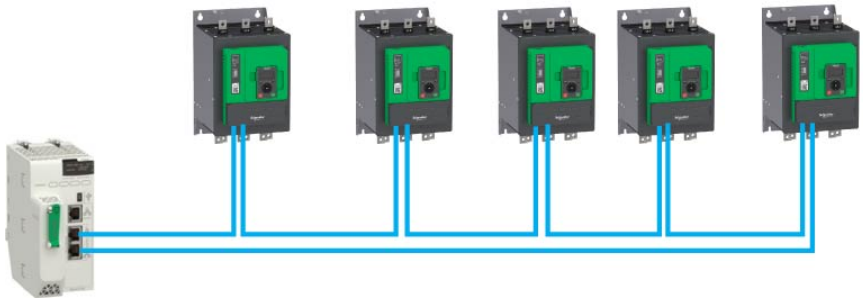



**NOTE:** In daisy chain topology, if one soft starter is turned off, an **[Fieldbus Com Interrupt]** CNF error is triggered in the other soft starters connected to the same topology. To keep the integrity of Ethernet daisy chain network when one or more soft starters are powered off, add an external permanent 24VDc supply to the control block of the soft starter.

- Redundant ring topology with RSTP (with a RSTP switch)

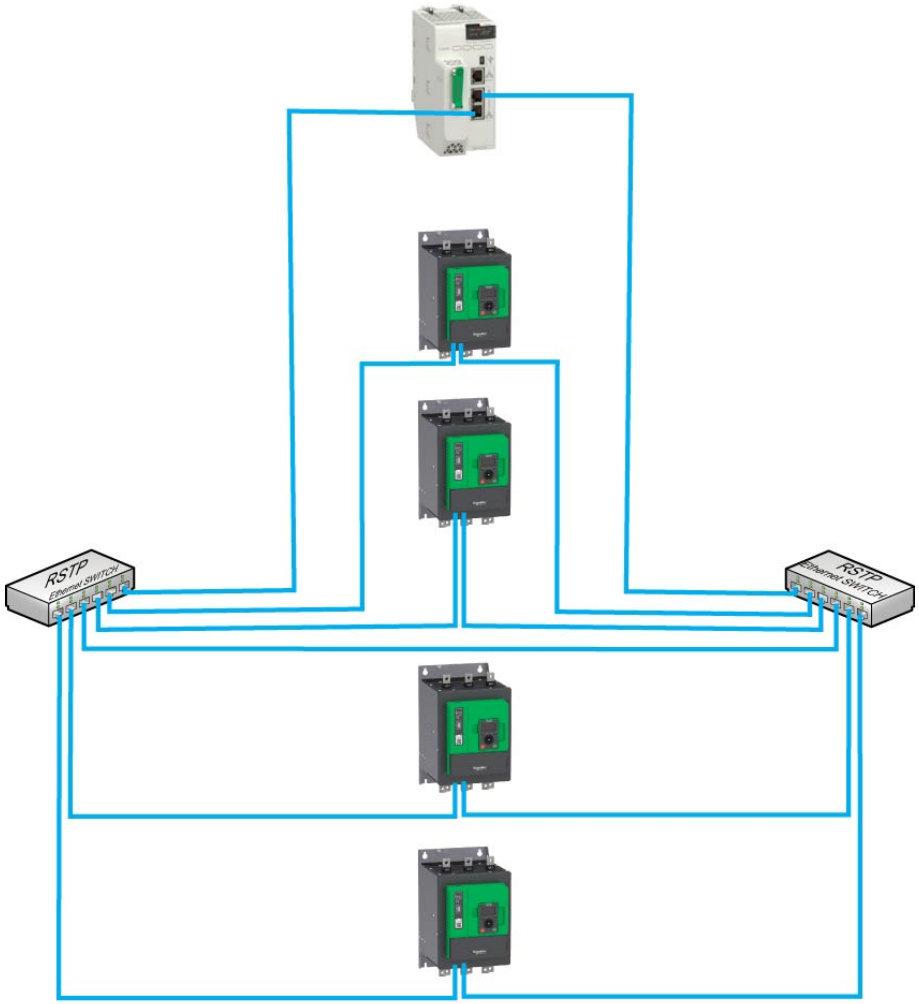


- Redundant ring topology with RSTP (with a RSTP PLC)

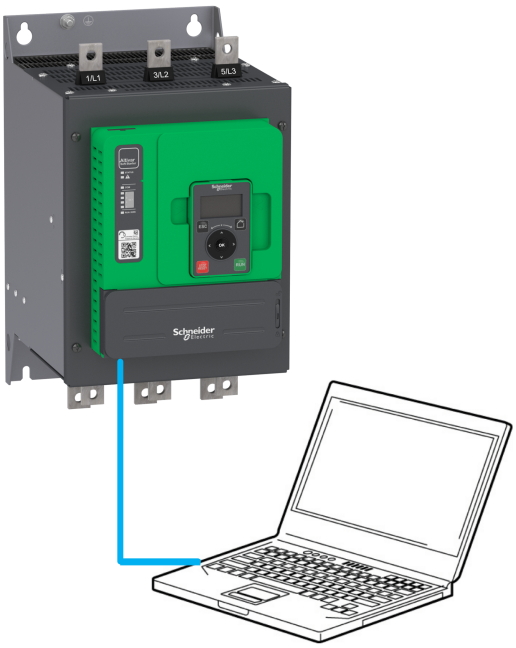


**NOTE:** When using the ring topology, all the drives in the ring must have RSTP configuration enabled.

- Redundant star topology with RSTP



The following figure shows the direct connection between the soft starter and PC.




# Accessories Presentation

## Information

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

# Software Setup

## Basic Settings

### Structure of the Parameter Table

#### General Legend

| Pictogram | Description |
|---|---|
|  | This parameter can be set during operation or when stopped.<br>**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]**<br>**[additional informations]** | **Factory setting**:<br>**[Short Label]** CODE |
| ***[Long label]***<br>Access path: **[Menu]** ➡ **[Sub-menu]**<br>Reference exclusivity and required optional modules.<br>Example: Fieldbus Module VW3A3607 is required.<br>Description of the parameter.<br>Parameter incompatibilities and / or required configuration.<br>Example: This parameter can be accessed it **[Short Label]** CODE is set to **[Short Label]** CODE.<br>This parameter is not compatible with **[Short Label]** CODE.<br>Impact on other parameters.<br>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.

# IP Parameter Settings

## Assigning IP Parameters

If not using IPV6 functionalities for DPWS, following parameters shall be configured:

- The soft starter IP address.
- The subnet mask.
- The gateway IP address.

These IP addresses can be entered using the display terminal, the embedded webserver, or the DTM-based PC software.

They can be also provided by:

- A BOOTP server (correspondence between the MAC address and the IP addresses).
- Or a DHCP server (correspondence between device name **[Device Name]** PAN and the IP addresses).

If an IP address other than 0.0.0.0 has been entered manually, assignment using a server is disabled. Regardless of the type of IP address assignment, if the address is modified, then the IP address is effective the next time the soft starter is turned on (control voltage if a separate power supply is being used).

## Entering IP Parameters in the Display Terminal

**NOTE:** To modified **[ETH Option IP]**, **[ETH Option Subnet Msk]** and **[ETH Option Gate Add]**:
**[ETH Option IP Mode]** IM10 need to be set on **[Fixed]** MANU.

In the **[Communication]** COM and **[Eth Module Config]** ETO submenu, enter the following IP addresses:

- **[ETH Option IP]** IC11, IC12, IC13, IC14.
- **[ETH Option Subnet Msk]** IM11, IM12, IM13, IM14.
- **[ETH Option Gate Add]** IG11, IG12, IG13, IG14.

If this address is modified, the new IP address entered is displayed.

## Configuring BOOTP

The BOOTP service is used to assign IP addresses based on the MAC address. The MAC address consisting of 6 hexadecimal digits (MM-MM-MM-XX-XX-XX) must be entered in the BOOTP server. The MAC address appears on the fieldbus adapter dedicated menu on the display terminal.

In the **[Communication]** COM and **[Eth Module Config]** ETO submenu:

- Leave the IP address **[ETH Option IP]** IC11, IC12, IC13, IC14 at the value **[0.0.0.0]** 0 0 0 0.
- Do not enable the FDR service.

## Configuring DHCP

The DHCP service is used to assign IP addresses and FDR configuration file path based on the device name **[Device Name]** PAN .

The device name consisting of an alphanumeric string must be entered in both the DHCP server and the soft starter.

In the **[Communication]** COM and **[Eth Module Config]** ETO submenu, enter the **[Device Name]** PAN

# [Eth Module Config] ETO

## Access

This menu is accessible via **[Communication]** COM.

## Possible Settings

The table presents the parameter settings:

| HMI label | Setting | |
|---|---|---|
| **[Device Name]** PAN | – | |
| This parameter is used to set the device name.<br>The FDR (Fast Device Replacement) service is based on identification of the device by a **Device Name**. In the case of the Altivar soft starter, this is represented by the **[Device Name]** PAN parameter. Verify that all the network devices have different **Device Name**.<br>**NOTE:** The **[Device Name]** PAN is common for both Ethernet interfaces. | | |
| **[ETH Option IP Mode]** IM10 | Logic address: FBC2 hex = 64450 | Type: WORD (Enumeration)<br>Read/write: R/W |
| ***Ethernet option IP mode***<br>This parameter is used to select the IP address assignment method:<br>**[Fixed]** MANU: Manually set the IP address.<br>**[BOOTP]** BOOTP: Automatically gets the IP address from the Bootp or DHCP server using the MAC address.<br>**[DHCP]** DHCP: Automatically gets the IP address from the DHCP server using the device name **(factory setting)**. | | |
| **[ETH Option IP]** IC11, IC12, IC13, IC14 | Logic address IC11: FBC3 hex = 64451<br>Logic address IC12: FBC4 hex = 64452<br>Logic address IC13: FBC5 hex = 64453<br>Logic address IC14: FBC6 hex = 64454 | Type: INT<br>Read/write: R/W |
| ***Ethernet option IP***<br>This parameter is used to set the IP address and can be edited only when the IP mode is set to fixed address.<br>The modification of the setting value is effective when you restart the soft starter. | | |
| **[ETH Option Subnet Msk]** IM11, IM12, IM13, IM14 | Logic address IM11: FBC7 hex = 64455<br>Logic address IM12: FBC8 hex = 64456<br>Logic address IM13: FBC9 hex = 64457<br>Logic address IM14: FBCA hex = 64458 | Type: INT<br>Read/write: R/W |
| ***Ethernet option subnet mask***<br>This parameter is used to set the IP subnet mask and can be edited only when IP mode is set to fixed address. | | |
| **[ETH Option Gate Add]** IG11, IG12, IG13, IG14 | Logic address IG11: FBCB hex = 64459<br>Logic address IG12: FBCC hex = 64460<br>Logic address IG13: FBCD hex = 64461<br>Logic address IG14: FBCE hex = 64462 | Type: INT<br>Read/write: R/W |
| ***Ethernet option gateway address***<br>This parameter is used to set the default gateway address and can be edited only IP mode is set to fixed address.<br>The modification of the setting value is effective when you restart the soft starter. | | |

| HMI label | Setting | |
|---|---|---|
| **[Ethernet Timeout]** TOUT | Logic address: FAD3 hex = 64211<br>Range: 0.1...60.0 s<br>Factory setting: 10.0 s | Type: UINT (Unsigned16)<br>Read/write: R/WS<br>Unit: 0.1 s |

***Ethernet timeout***
The time-out is triggered if the adapter does not receive any cyclic messages within a predefined time period.

This period is managed by the controller (not by the soft starter) and is configured in its module properties box.

The duration of the time-out is defined by the **[Ethernet Timeout]** TOUT.

| | | |
|---|---|---|
| **[Fieldbus Interrupt Resp]** CLL | Logic address: 1B67 hex = 7015<br>CIP Path: 84/01/10 hex = 132/01/16 | Type: WORD (Enumeration)<br>Read/write: R/WS |

***Response to Fieldbus module communication interruption***
This parameter defines the fieldbus error stop mode.

- **[Ignore]** NO : Detected error ignored (in this case, the warning **[Fieldbus Com Warn]** CLLA is activated).
- **[Freewheel Stop]** YES : Motor triggers in error and is stopped in freewheel **(factory setting)**.
- **[Per STT]** STT : Motor is stopped according to **[Type of stop]** STT parameter.
- **[Deceleration]** DEC : Motor is stopped in deceleration and triggers in error at the end of stop.
- **[Braking]** BRK : Motor is stopped in dynamic braking and triggers in error at the end of stop.

**⚠WARNING**

**LOSS OF CONTROL**

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

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

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

| | | |
|---|---|---|
| **[Product restart]** RP | Logic address: 1BD8 hex = 7128<br>CIP Path: 84/01/81 hex = 132/01/129 | Type: WORD (Enumeration)<br>Read/write: R/WS |

***Product restart***

Restart the device. Can be used to clear a detected error or refresh a modified parameters that requires a device restart.

- **[No]** NO: No restart **(factory setting)**.
- **[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.**

## [Fast Device Rep.] FDRO

### Access

This menu is accessible via: **[Communication]** COM ➡ **[Eth Module Config]** ETO

These parameters can be accessed if **[ETH Option IP Mode]** IM10 is set to **[DHCP]** DHCP.

### Possible Settings

The table presents the parameter settings:

| HMI label | Setting | |
|---|---|---|
| **[Enable FDR]** FDV1 | Logic address: FBBD hex = 64445 | Type: WORD (Enumeration)<br>Read/write: R/WS |
| ***Enable FDR function***<br>This parameter is used to enable or disable the FDR service.<br>**[No]**: FDR service disabled **(factory setting)**.<br>**[Yes]**: FDR service enabled. | | |
| **[FDR Action]** FDA1 | Logic address: FBBC hex = 64444 | Type: WORD (Enumeration)<br>Read/write: R/W |
| ***FDR action***<br>This parameter is used to select the FDR action that needs to be performed.<br>**[NOT ACTIVE]**: No FDR action.<br>**[SAVE]**: FDR save command.<br>**[REST]**: FDR restore command. | | |
| **[FDR Operating State]** FDS1 | Logic address: FBBB hex = 64443 | Type: WORD (Enumeration)<br>Read/write: R |
| ***FDR operating state***<br>This parameter is used to display the FDR operating state.<br>**[Initialization]** INIT: Initialization.<br>**[Not Active]** IDLE: Function not active.<br>**[Operational]** OPE: Operational.<br>**[Ready]** RDY: Ready.<br>**[IP Configuration]** IPC: IP configuration.<br>**[Not Configured]** UNCF: Function not configured.<br>**[Reading Configuration]** GET: Download the current configuration.<br>**[Writing Configuration]** SET: Save the current configuration.<br>**[Applying Configuration]** APP: Applying the configuration to the soft starter. | | |

| HMI label | Setting | |
|---|---|---|
| **[FDR Error Status]** FDR1 | Logic address: FBBA hex = 64442 | Type: WORD (Enumeration)<br>Read/write: R |

***FDR error status***
This parameter is used to display the FDR error status.

**[No Error]** NO: No error.

**[Server Timeout]** TOUT: Server timeout.

**[Server No File]** SNF: No file on server.

**[Server Corrupt File]** CRPT: Corrupted file on server.

**[Server Empty File]** EPTY: Empty file on server.

**[Device Invalid File]** HINV: Invalid file on soft starter.

**[CRC Error]** CRC: CRC error.

**[Version Incompatibility]** VRM: Version incompatibility between soft starter and file.

**[Device No File]** HNF:No file on soft starter.

**[Server Reading Size]** SIZE: File size reading error on server.

**[Device Opening File]** OPEN: Soft starter cannot open the file.

**[Device Reading File]** READ: Soft starter cannot read the file.

**[Incompatibility]** SCNT: File incompatibility.

**[Device Invalid Name]** NINV: Soft starter name is invalid.

**[Server Incorrect File Size]** FSIZ: Incorrect file size on server.

**[Device Writing File]** HWF: Soft starter cannot write the file.

**[Server Writing File]** SWF: Server cannot write the file.

**Remedy:**

To eliminate the FDR error, the following steps must be performed:

- Change **[ETH Option IP Mode]** IM10 to **[DHCP]** DHCP and restart the soft starter.
- FDR is active and **Automatic Syncho Cycle** is off.
- Disable the FDR and restart the soft starter.
- Change the **[ETH Option IP Mode]** IM10 to **[Fixed]** MANU and restart the soft starter.

# [Ethernet Module Diag] MTE

## Access

This menu is accessible via: **[Communication]** COM ➡ **[Communication map]** CMM

## Possible Settings

The table presents the parameter settings:

| HMI label | Setting | |
|---|---|---|
| **[MAC @]** MACO | – | |
| This parameter displays the MAC address of the device in the format **[MM-MM-MM-XX-XX-XX]**. | | |
| **[ETH opt Rx frames]** ERXO | Logic address: FBD2 hex = 64466 | Type: UINT (Unsigned32)<br>Read/write: R |
| ***Ethernet option Rx frames***<br>This parameter displays the Ethernet module received Rx frames counter. | | |
| **[ETH opt Tx frames]** ETXO | Logic address: FBD4 hex = 64468 | Type: UINT (Unsigned32)<br>Read/write: R |
| ***Ethernet option Tx frames***<br>This parameter displays the Ethernet module transmitted frames counter. | | |
| **[ETH opt error frames]** EERO | Logic address: FBD6 hex = 64470 | Type: UINT (Unsigned32)<br>Read/write: R |
| ***Ethernet option error frames***<br>This parameter displays the Ethernet module error frames counter. | | |
| **[Actual rate]** ARD | Logic address: FB0A hex = 64266 | Type: WORD (Enumeration)<br>Read/write: R |
| ***Actual rate and duplex***<br>This parameter displays the Ethernet module actual rate.<br>**[Auto]**: Data rate is auto detected depending on the first data packet received **(factory setting)**.<br>**[10M. full]**: Data rate is set to 10 Mbit/s full.<br>**[10M. half]**: Data rate is set to 10 Mbit/s half.<br>**[100M. full]**: Data rate is set to 100 Mbit/s full.<br>**[100M. half]**: Data rate is set to 100 Mbit/s half. | | |
| **[Fieldbus Error]** EPF2 | Logic address: FBBA hex = 64442 | Type: WORD (Enumeration)<br>Read/write: R |
| ***External error detected by Fieldbus***<br>An external error has been triggered.<br>The parameter can be:<br>• Bit 0: Invalid IP settings | | |

| HMI label | Setting | |
|---|---|---|
| • Bit 1: Detected duplicated IP<br>• Bit 2: FDR error<br>• Bit 4: Configuration file error<br>• Bit 5-7: (reserved)<br><br>**Remedy:**<br>• A faulty or duplicate address can cause conflicting issues.<br>• Try setting a different fixed IP address | | |
| **[Fieldbus Com Interrupt]** CNF  | Logic address: 1BE8 hex = 7144<br>CIP Path: 84/01/91 hex = 132/01/145 | Type: UINT (Unsigned16)<br>Read/write: R |
| ***Fieldbus communication interruption***<br>This error is caused by the timeout and appears when the communication is stopped or interrupted with the module.<br>The parameter can be:<br>• Bit 0: Modbus timeout (linemonitoring) : recoverable<br>• Bit 1: (reserved)<br>• Bit 2: EIP timeout (linemonitoring) : recoverable<br>• Bit 3: EIP idle (controlsupervisor) : recoverable<br>• Bit 4: EIP fault trip (controlsupervisor) : recoverable<br>• Bit 5-7: (reserved)<br>• Bit 8: UAP exception (cpu fault) : recoverable<br>• Bit 9: UAP reboot device : unrecoverable<br>• Bit 10-12: (reserved)<br>• Bit 13: reboot device : unrecoverable<br>• Bit 14: Fatal exception (cpu fault) : unrecoverable<br>• Bit 15: (internal usage only)<br><br>**Remedy:**<br>Increase the value of **[Ethernet Timeout]** TOUT. | | |
| **[InternCom Error1]** ILF1  | Logic address: 1BDE hex = 7134<br>CIP Path: 84/01/87 hex = 132/01/135 | Type: UINT (Unsigned16)<br>Read/write: R |
| ***Internal communication interruption 1***<br>Communication interruption between the Ethernet module and the soft starter.<br><br>**Remedy:**<br>• Verify the connections.<br>• Replace the Ethernet module.<br>This detected error requires a power reset. | | |

# 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<br>CIP Path: 7B/01/03 hex = 123/01/03 | Type: WORD (BitString16)<br>Read/write: R<br>Unit: - |
| ***Logic inputs states***<br>• Bit0 : "DI1" Digital inputs real image<br>• Bit1 : "DI2" Digital inputs real image<br>• Bit2 : "DI3" Digital inputs real image<br>• Bit3 : "DI4" Digital inputs real image | | |
| **[Logic Outputs States]** OL1R | Logic address: 145C hex = 5212<br>CIP Path: 7B/01/0D hex = 123/01/13 | Type: WORD (BitString16)<br>Read/write: R/W<br>Unit: - |
| ***Logic outputs states***<br>• Bit0 : "R1" relay real image<br>• Bit1 : "R2" relay real image<br>• Bit2 : "R3" relay real image<br>• Bit8 : "DQ1" digital outputs real image<br>• Bit9 : "DQ2" digital outputs real image<br><br>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<br>CIP Path: 7B/01/2B hex = 123/01/43 | Type: INT (Signed16)<br>Read/write: R<br>Unit: - |
| ***Physical value AI1***<br>AI1 customer image (1mV, 0.001mA)<br>• (AI1T == "PTC") : 0.01 kOhm<br>• (AI1T == "1PT2") : 0.1 Ohm<br>• (AI1T == "1PT23") : 0.1 Ohm<br>• else : 0.001 V | | |
| **[Analog Input 1 Standardized Value]** AI1R | Logic address: 1470 hex= 5232<br>CIP Path: 7B/01/21 hex = 123/01/33 | Type: INT (Signed16)<br>Read/write: R<br>Unit: - |
| ***Analog input 1 standardized value***<br>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<br>CIP Path: 7B/01/48 hex = 123/01/72 | Type: INT (Signed16)<br>Read/write: R/W<br>Unit: - |
| ***AQ1 physical value***<br>AQ1 customer image (1mV, 0.001mA) | | |
| **[Analog Output 1 Standardized Value]** AO1R | Logic address: 148D hex = 5261<br>CIP Path: 7B/01/3E hex = 123/01/62 | Type: INT (Signed16)<br>Read/write: R/W<br>Unit: - |
| ***Analog output 1 standardized value***<br>AQ1 real application image | | |

## Base Monitoring

| Code | Settings | |
|---|---|---|
| **[Status Register]** ETA | Logic address: 0C81 hex = 3201<br>CIP Path: 71/01/02 hex = 113/01/02 | Type: WORD (BitString16)<br>Read/write: R<br>Unit: - |
| ***Status Register***<br>• Bit0 = 1 : Ready to switch on<br>• Bit1 = 1 : Switched on<br>• Bit2 = 1 : Operation enabled<br>• Bit3 = 1 : Detected error<br>• Bit4 = 1 : Voltage enabled<br>• Bit5 = 0 : Quick stop active<br>• Bit6 = 1 : Switch on disabled<br>• Bit7 = 1 : Alarm present<br>• Bit8 : Reserved<br>• Bit9 = 0 : Local mode control<br>• Bit10 to Bit13: Reserved<br>• Bit14 = 1 : Stop imposed by STOP key<br>• Bit15 : Reserved | | |
| **[Motor Current]** LCR | Logic address: 0C84 hex = 3204<br>CIP Path: 71/01/05 hex = 113/01/05 | Type: UINT (Unsigned16)<br>Read/write: R<br>Unit: 0.1 A |
| ***Motor current***<br>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<br>CIP Path: 91/01/1F hex = 145/01/31 | Type: UINT (Unsigned16)<br>Read/write: R<br>Unit: 1 % |
| ***Motor thermal state***<br>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.<br><br>Refers to the ATS480 User Manual NNZ85515 for more information. | | |
| **[Motor Run Time]** RTH | Logic address: 0CAC hex = 3244<br>CIP Path: 71/01/2D hex = 113/01/45 | Type: UINT (Unsigned32)<br>Read/write: R<br>Unit: 1 s |
| ***Motor run time***<br>This parameter monitors how long the motor has been energized. | | |
| **[Elc Energy Cons]** OCK | Logic address: 299C hex = 10652<br>CIP Path: 96/01/35 hex = 150/01/53 | Type: UINT (Unsigned32)<br>Read/write: R/WS<br>Unit: kWh |
| ***Electrical energy consumed by the motor (kWh)*** | | |

| Code | Settings | |
|---|---|---|
| **[Active Command Channel]** CCC | Logic address: 20FA = 8442<br>CIP Path: 8B/01/2B = 139/01/43 | Type: WORD (BitString16)<br>Read/write: R<br>Unit: - |
| ***Active command channel***<br>Active command channels status<br>• Bit0 = 1 : Terminal board<br>• Bit2 = 1 : Deported keypad<br>• Bit3 = 1 : Modbus<br>• Bit6 = 1 : CANopen<br>• Bit9 = 1 : COM option board<br>• Bit14 = 1 : Indus<br>• Bit15 = 1 : SoMove | | |

## Command Register

| Code | Settings | |
|---|---|---|
| **[Cmd Register]** CMD | Logic address: 2135 hex = 8501<br>CIP Path: 8B/01/66 hex = 139/01/102 | Type: WORD (BitString16)<br>Read/write: R/W<br>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]**<br>CMI | Logic address: 2138 hex = 8504<br>CIP Path: 8B/01/69 hex = 139/01/105 | Type: WORD (BitString16)<br>Read/write: R/W<br>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

# Additional Settings

## [EnableOptWeb] EWE

### Access

This parameter is accessible via: **[Device Management]** DMT ➡ **[Cybersecurity]** CYBS ➡ **[Access control]** CSAC

### Possible Settings

The table presents the parameter settings:

| HMI label | Setting | |
|---|---|---|
| **[EnableOptWeb]** EWE | Logic address: FB08 hex = 64264 | Type: WORD (Enumeration) |
| This parameter is used to manage the fieldbus module Web services.<br>**[No]**: Web services disabled.<br>**[Yes]**: Web services enabled. | | |

## User Authentication Settings

### [Access control] CSAC- menu

This menu is accessible in the **[Device Management]** DMT ➡ **[Cybersecurity]** CYBS ➡ **[Access control]** CSAC menu via the graphic display terminal if VW3A3720 Ethernet option module has been inserted.

These following parameters are used to acknowledge and configure user authentication to access your soft starter through PC software tools.

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

### [Eth Opt User Auth.] SCPO

This parameter is used to enable or disable the user authentication feature (for Ethernet option module).

Disabling this feature, no credentials will be required to access your process or machine. This setting is saved with the configuration and will be active if a configuration is loaded or copied.

**⚠WARNING**

**UNAUTHENTICATED ACCESS AND MACHINE OPERATION**

Do not disable the feature if your machine or process is accessible to unauthorized personnel either directly or via a network.

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

| Setting | Code/ Value | Description |
|---|---|---|
| **[No]** | NO | User authentication disabled. Connection to PC software tools provided by Schneider-Electric (such as SoMove FDT / DTM) with Modbus TCP (via Ethernet option port) is unlocked. |
| **[Yes]** | YES | User authentication enabled. Connection to PC software tools provided by Schneider-Electric (such as SoMove FDT / DTM) with Modbus TCP (via Ethernet option port) is locked by a password.<br>**NOTE:** If the PC software tool is not update to the latest version, the connection to PC software tool can be locked.<br>**Factory setting** |

## [Reset Password] SRPW

Reset ethernet option password.

For ethernet option, it resets the user authentication password and the administrator access (ADMIN) webserver password to the default value. Once reset, the default password can be read using **[Default Pwd Eth Opt]** **SDPW**.

| Setting | Code/ Value | Description |
|---|---|---|
| **[No]** | NO | Password reset not requested.<br>**Factory setting** |
| **[Yes]** | YES | Password reset requested.<br>The parameter switches back to **[No]** NO when the operation is done. |

## [Default Pwd Eth Opt] SDPW

It provides the eight characters default password used for both webserver connection (Administrator access) and PC software tool connection (user authentication).

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

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

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

Once modified, this password is not displayed anymore. The new defined password is applicable for both administrator webserver access and PC software tool access.


**NOTE:** The default password is displayed on the Graphic Display Terminal. The Graphic Display Terminal is an accessory for cabinet integration product .

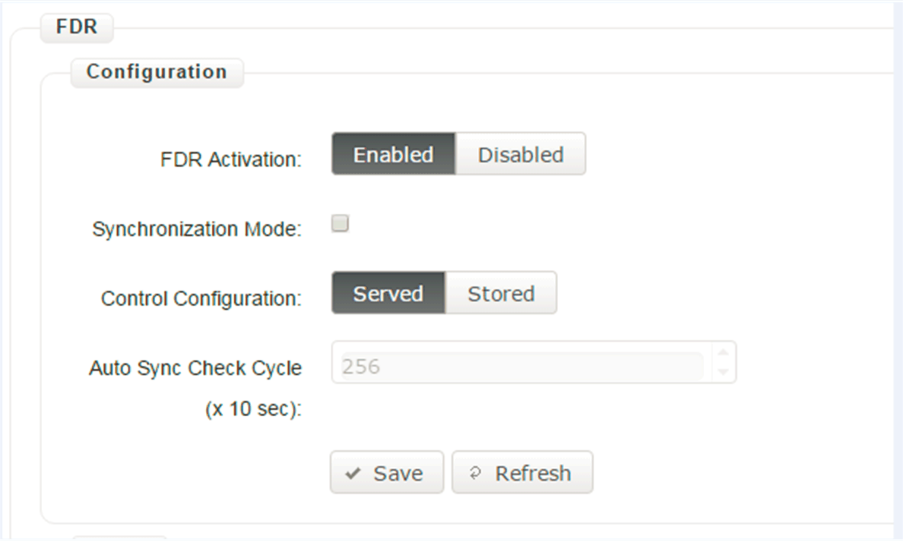
# FDR Settings

## Access

The parameters are accessible via the webserver or the DTM-based PC software

## FDR Configuration

The following figure shows FDR settings via webserver:




The table presents the **FDR Configuration** settings:

| Parameter | Description | Settings |
|---|---|---|
| **FDR Activation** | This parameter is used to enable or disable the FDR service<br>**NOTE:** You can enable FDR only if the **IP assignment mode** selected is DHCP. | **Enabled**: FDR service enabled<br>**Disabled**: FDR service disabled.<br>**Factory setting**: Enabled |
| **Control Configuration** | This parameter is used to select the server or local configuration. | **Served**: Transfers the configuration file from server to sot starter at power-up.<br>**Stored**: uses the configuration stored in the sot starter at power-up.<br>**Factory setting:** served |
| **Automatic Syncho Cycle (x 10 Sec)** | Allows you to select the interval for periodic synchronization of the soft starter with the FDR server.<br>**NOTE:** You can configure automatic Synchro cycle only if **Synchronization mode** check box is selected. | 100...655350 sec<br>**Factory setting**: 100 sec |

# RSTP Settings

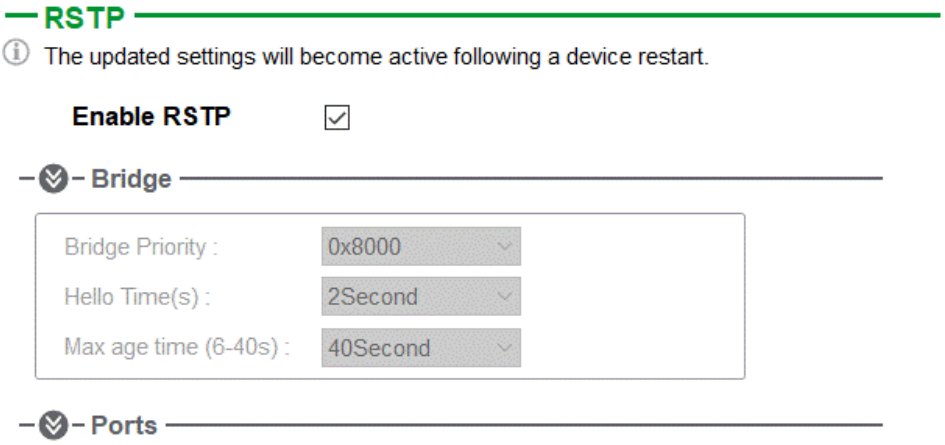
## Access

The parameters are accessible via the DTM-based PC software.

# Bridge Settings & Ports Configuration

## Bridge Settings

The following figure shows the bridge settings using the DTM:

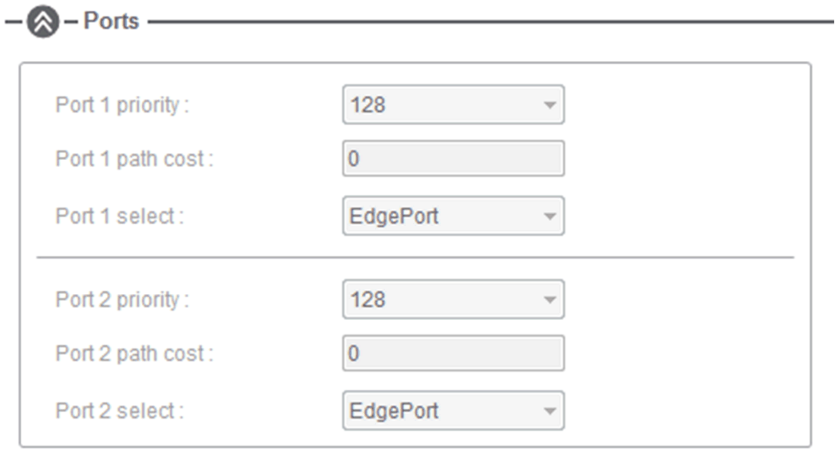



The table presents the **Bridge** configuration

| Parameters | Description | Settings | |
|---|---|---|---|
| **Bridge Priority** | The bridge priority is used to control which bridge is elected as the root bridge.<br><br>Bridge with the smallest (lowest) bridge ID is elected as the root bridge. Bridge ID consists of the configurable priority and the MAC address of the bridge.<br><br>To compare 2 bridge ids, bridge priorities are compared first. If the bridge priorities are equal, then the MAC addresses are compared.<br><br>The bridge priority can be set only in increments of 4096 | 0<br>4096<br>8192<br>12288<br>16384<br>20480<br>24576<br>28672<br>32768<br>36864<br>40960<br>45056<br>49152<br>53248<br>57344<br>61440 | 0 hex<br>1000 hex<br>2000 hex<br>3000 hex<br>4000 hex<br>5000 hex<br>6000 hex<br>7000 hex<br>8000 hex<br>9000 hex<br>A000 hex<br>B000 hex<br>C000 hex<br>D000 hex<br>E000 hex<br>F000 hex |
| **Hello Time(S)** | The hello time parameter corresponds to the time interval at which the root bridge transmits configuration Bridge Protocol Data Units (BPDU)s. | 1...10 sec | |
| **Max age time (6-40 s)** | The maximum age time correspond to the maximum expected arrival time of hello BPDUs. If the timer expires, the bridge detects acommunication interruption to the root bridge and initiates a topology convergence.The maximum age timer should be longer than the configured hello time. | 6...40 sec | |

## Ports Configuration

The following figure shows the port settings:




The table provides the **Ports** settings

| Parameters | Description | Settings |
|---|---|---|
| **Port Priority** | Allows you to define the priority of the interface to the other going to same subnet. | 0...240<br>**NOTE:**<br>• The port priority can be set only in increments of 16<br>• Soft starter takes the value in account after a product restart. |
| **Port Path Cost** | Allows you to define the cost of sending spanning tree traffic through the interface.<br>RSTP uses path cost to determine the topology with the smallest total path cost between each point of the tree and the root bridge. | 0...1,569,325,055<br>**NOTE:** If the port path cost is set to 0 (auto), the path cost is based on the port link speed maximum, for details see the following table. |
| **Port Select** | Allows you to select the type of ports. With the port types defined, RSTP can quickly reconfigure a network when a change in network topology is detected. | **RSTP Port**<br>**Edge Port** |

Table provides the value of the path cost based on the port link maximum speed

| Port Link Maximum Speed | Automatic Path Cost |
|---|---|
| 10 Gb/s (Not supported by the adapter) | 2000 |
| 1 Gb/S (Not supported by the adapter) | 20000 |
| 100 Mb/s | 200000 |
| 10 Mb/s | 2000000 |

# Configuring I/O Scanning

## Description

The soft starter I/O scanning service can be enabled or disabled with the DTM-based PC software.

It is not possible to modify the assignment of the I/O scanning periodic variables using the display terminal. To configure I/O scanning, use the DTM-based PC software.

# DNS Settings

## Description

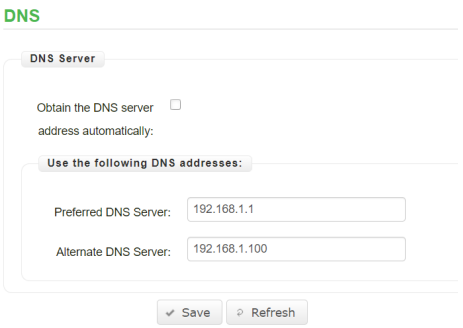
The Domain Name System (DNS) is a distributed naming system for devices connected to the network.

It translates domain names to IP addresses for locating the devices easily on the network.

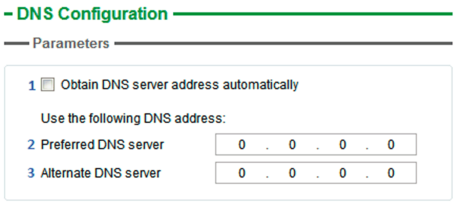
## DNS Configuration

The DNS configuration can be done using the DTM-based PC software.

The following figure shows the DNS configuration window:




DNS Configuration window by the Web Server




DNS Configuration window by the DTM

The table presents the **DNS Configuration** settings:

| Item | Description |
|---|---|
| 1 | **Obtain DNS Server address automatically**: When checked, the function is enabled and allows getting automatically the IP address from the DNS server. |
| 2 | **Preferred DNS server**: Enter the IP address of the preferred DNS server. |
| 3 | **Alternate DNS server**: Enter the IP address of the alternate DNS server.<br>**NOTE:** The alternate IP address is used only if the first server is unavailable. |

**NOTE:** The changes must be applied to the module configuration by clicking the  button.

# SNTP Settings

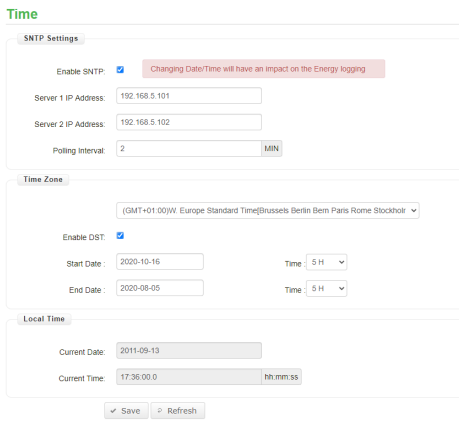
## Description

The Simple Network Time Protocol (SNTP) is networking protocol for clock synchronization of devices connected to the network.

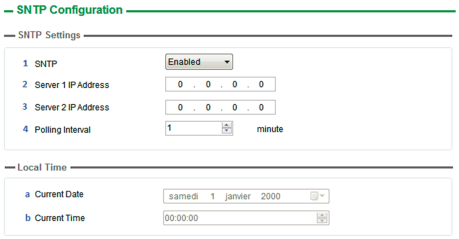
## SNTP Configuration

The SNTP configuration can be done using the DTM-based PC software.

The following figure shows the SNTP Configuration window:




SNTP Configuration window by the Web Server




SNTP Configuration window by the DTM

The **SNTP Configuration** window is divided in 2 zones:

- **SNTP Settings**
- **Local Time**

The table presents the **SNTP settings**:

| Item | Description |
|---|---|
| 1 | **Enabled**: Enables SNTP service.<br>**Disabled**: Disables SNTP service. |
| 2 | **Server 1 IP Address**: Enter the IP address of the first preferred SNTP server. |
| 3 | **Server 2 IP Address**: Enter the IP address of the second preferred SNTP server.<br>**NOTE:** This IP address is used for SNTP only if the first server is unavailable. |
| 4 | **Polling Interval**: Allows you to select the scanning interval for checking the time change. |

The table presents the **Local Time** settings:

| Item | Description |
|---|---|
| a | **Current Date**: Allows you to enter the current date |
| b | **Current Time**:Allows you to select the current time |

**NOTE:** The changes must be applied to the module configuration by clicking the  button.

# SNMP Settings

## Description

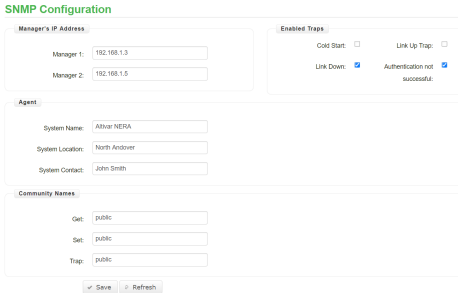
Simple Network Management Protocol (SNMP) is an internet-standard protocol used to manage devices on IP networks.

It is used for collecting and organizing information about the devices on the network.

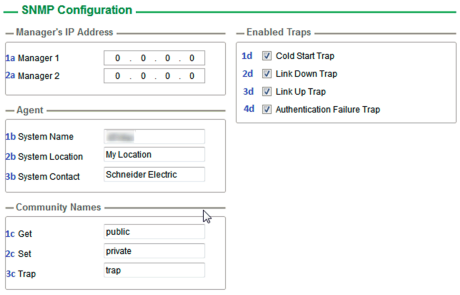
## SNMP Configuration

The SNMP configuration can be done using the DTM-based PC software.

The following figure shows the SNTP Configuration window:




SNMP Configuration window by the Web Server




SNMP Configuration window by the DTM

The **SNMP Configuration** window is divided in 4 zones:

- **Manager's IP Address**
- **Agent**
- **Community Names**
- **Enabled Traps**

## Manager's IP Address

SNMP manager is a central system used for monitoring and controlling the SNMP agents.

The table presents **Manager's IP Address** settings:

| Item | Description |
|---|---|
| 1a | **Manager 1**: SNMP manager is a central system, which is used for monitoring and controlling the SNMP agents. |
| 2a | **Manager 2**: Enter the IP address of SNMP manager 2. |

## Agents

Agents are the devices which are connected to the network. The SNMP manager monitors these devices.

The table presents the **Agents** settings:

| Item | Description |
|---|---|
| 1b | **System Name**: Enter the system name used by the soft starter. |
| 2b | **System Location**: Enter the system location of the soft starter. |
| 3b | **System Contact**:Contact point to get the information about the system.<br>Enter the system contact of the soft starter. |

## Community Names

Community names are used to identify the commands that can be performed by an SNMP manager on a device.

The table presents the **Community Names** settings:

| Item | Description |
|---|---|
| 1c | **Get**: Requests send from manager to agent to retrieve data. |
| 2c | **Set**: Requests send from manager to agent to change data. |
| 3c | **Trap**: Requests send from manager to agent to find the available data. |

## Enabled Traps

Traps are used to inform the SNMP manager of specific events occurring on device.

The table presents the **Enabled Traps** settings:

| Item | Description |
|---|---|
| 1d | **Cold Start**: The agent reinitialized its configuration tables. |
| 2d | **Link Down Trap**: A network interface card (NIC) on agent reinitializes. |
| 3d | **Link Up Trap**: A network interface card (NIC) on agent stops responding. |
| 4d | **Authentication Failure Trap**: SNMP agent gets a request from an unrecognized community name. |

# Fast Device Replacement

## Presentation

### FDR Service

The FDR (Fast Device Replacement) service is used to simplify the maintenance of soft starters connected to an Ethernet network. In the event of a soft starter not working correctly, this service automatically reconfigures its replacement.

The new soft starter (FDR client) retrieves:

- Its IP addresses and the FDR file path from a DHCP server
- The FDR file from an FTP server if the soft starter is not configured in local configuration

In practice, the DHCP server and the FTP server are the same device (PAC M580, M340 PLC, or dedicated PCs).

The FDR file contains:

- The Ethernet parameters (configuration of I/O scanning, FDR, and so on)
- The soft starter parameters (soft starter, functions, application, and so on)

The FDR service is based on identification of the device by a **Device Name**. In the case of the soft starter, this is represented by the **[Device Name]** PAN parameter.

The configuration of the FDR service is accessible via embedded webserver or DTM-based software or Graphic Display Terminal.

**NOTE:** Check that all the network devices have different **Device Name**.

The FDR server controls duplication of **Device Name** (it does not assign an IP address that has already been assigned and is active).

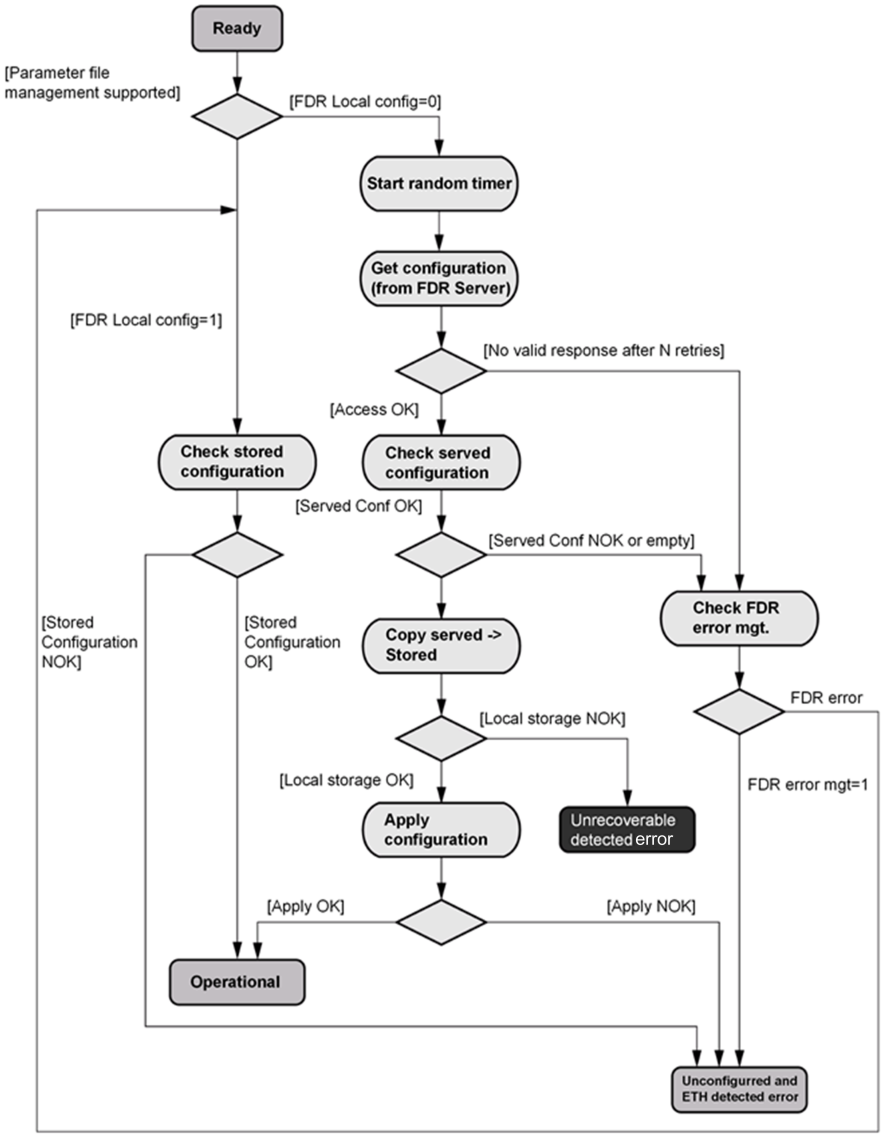
If the same IP address is supplied on 2 devices, the second should trigger an IP address duplication (network management detected error which triggers an **[Fieldbus Error]** EPF2 by default).

If the FDR service has been enabled, the Ethernet adapter attempts to restore its IP addresses on each power-up. Each time the procedure has detected error, the Ethernet adapter reiterates its FDR requests (DHCP).

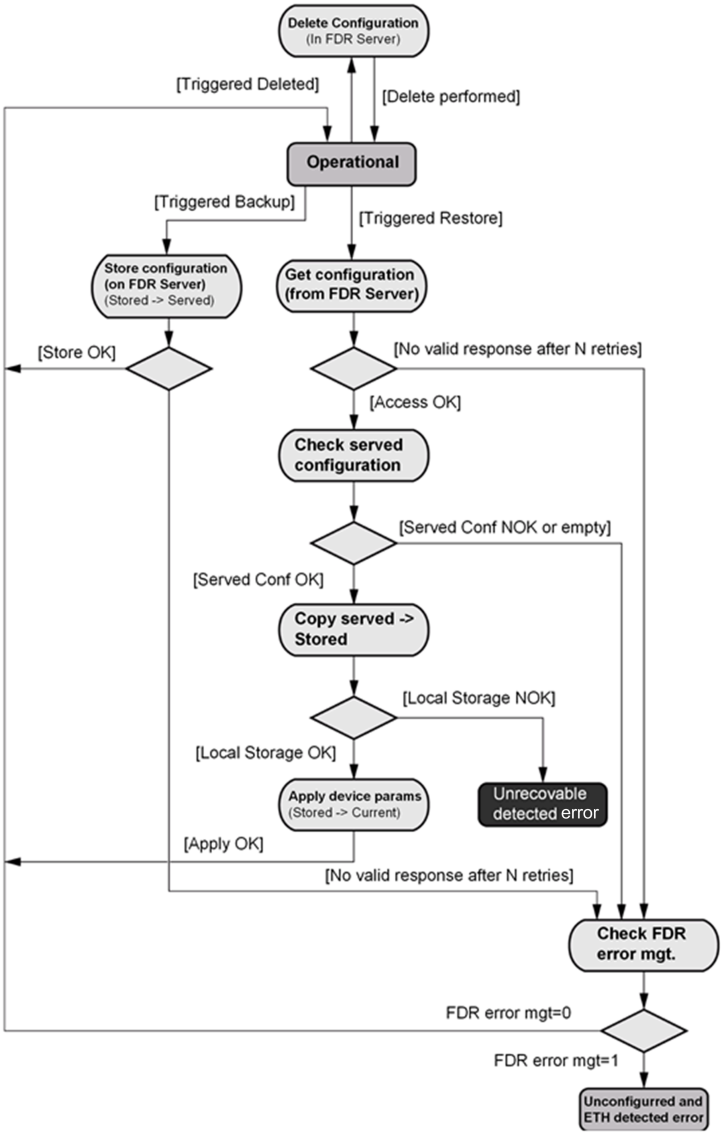
After assigning the Ethernet adapter IP addresses, if the configuration is not downloaded successfully, the Ethernet adapter triggers a **[FDR 2 Error]** FDR2.

# Startup Detailed Behavior

## Presentation

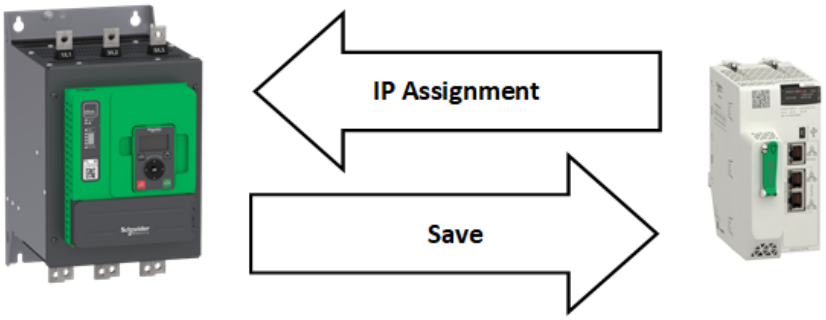


## FDR Operation Behavior



# Local Configuration

## Presentation




## IP Assignment Save

If the soft starter parameter configuration is local, the FDR server only assigns the following IP addresses:

- IP address,
- Subnet mask,
- Gateway IP address.

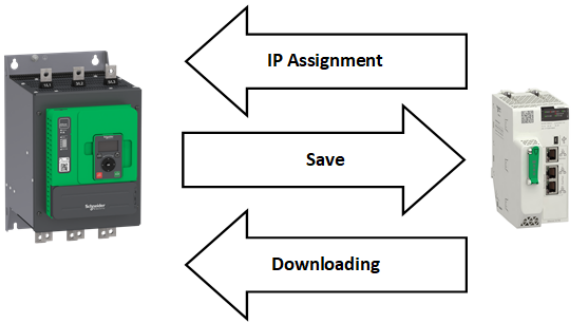
On connection to the network, the soft starter automatically saves its parameters in the FDR server.

## Soft Starter Connection Procedure

| Step | Action | Description |
|---|---|---|
| 1 | Configure the FDR server | See the PLC manual or the section on software setup using Unity |
| 2 | Configure the soft starter | This menu is accessible via **[Communication]** COM, **[Eth Module Config]** ETO submenu.<br>• Configure **[ETH Option IP Mode]** IM10 = **[DHCP]** DHCP<br>• Enable the FDR service via webserver or DTM-based software or Graphic Display Terminal.<br>• Select local soft starter configuration with webserver or DTM-based software.<br>• Enter the device name, **DEVICE NAME**, in the **[Communication]** COM, **[Eth Module Config]** ETO submenu. |
| 3 | Turn off the soft starter | Turn off the soft starter and then back on again (control voltage supply if a separate power supply is being used), otherwise the device name is not taken into account |
| 4 | Connect the soft starter to the network | Connect the soft starter and the FDR server (PLC) to the Ethernet network |

# Downloaded Configuration

## Presentation




## IP Assignment Save

If the soft starter parameter configuration has been downloaded, the FDR server assigns the following addresses:

- IP address,
- Subnet mask,
- Gateway IP address,
- FDR server IP address.

## Periodic Saving

Periodic saving of the soft starter configuration can be configured on the FDR server in either local configuration or downloaded configuration mode

Using the embedded webserver or the DTM-based software:

- Set FDR synchronization to automatic mode
- Set the synchronization cycle time

  **NOTE:** Saving too often overburden the fieldbus and adversely affects its performance (factory setting: 2.560 s.).

## Limitations

The FDR service is able to store the current configuration of the soft starter, but does not provide the possibility to store multi-parameters configurations.

## Soft starter Parameters (Configuration)

In the procedure described below, the configuration file is transferred to the FDR server, via the Ethernet network, using a manual save command.

| Step | Action | Description |
|---|---|---|
| 1 | Configure the soft starter | This menu is accessible via **[Communication]** COM, **[Eth Module Config]** ETO submenu.<br>• Leave the IP address **[ETH Option IP]** IC11, IC12, IC13, IC14 at the value **[0.0.0.0]** 0 0 0 0.<br>Using the embedded webserver or the DTM-based software:<br>• Set FDR synchronization to manual mode.<br>• Before the first connection, select local soft starter configuration. The soft starter needs first to push the configuration to the server.<br>• Enter the device name, **DEVICE NAME**, in the **[Communication]** COM, **[Eth Module Config]** ETO submenu. |
| 2 | Turn off the soft starter | Turn off the soft starter and then back on again (control voltage if a separate power supply is being used), otherwise the device name is not taken into account |
| 3 | Connect the soft starter to the fieldbus | Connect the soft starter and the FDR server (PLC) to the Ethernet fieldbus. |
| 4 | Configure the FDR server (see the PLC manual) | The server downloads the IP addresses to the Ethernet adapter.<br>Check that the operation has proceeded correctly: you can also check, in the **[Communication]** COM, **[Eth Module Config]** ETO submenu.<br>Whether the **[ETH Option IP]** IC11,IC12, IC13, IC14, **[ETH Option Subnet Msk]** IM11,IM12, IM13, IM14 and **[ETH Option Gate Add]** IG11,IG12, IG13, IG14 parameters have values other than **[0.0.0.0]** 0 0 0 0. |
| 5 | Supply the FDR server with the configuration file | Using the embedded webserver or the DTM-based software<br>• Specify that the soft starter configuration is downloaded from the FDR server on each power-up<br>• Send a save command to the FDR server. |
| 6 | Check that the system is operational | If the save operation has not been successful, the adapter detects a communication error which, in factory settings mode, triggers a **[FDR 2 Error]** FDR2. |

## Replacing a soft starter

For replacing a soft starter, it is necessary to follow the procedure below:

| Step | Action | Action |
|---|---|---|
| 1 | Configure the soft starter | This menu is accessible via **[Communication]** COM, **[Eth Module Config]** ETO submenu.<br>• Leave the IP address **[ETH Option IP]** IC11, IC12, IC13, IC14 at the value **[0.0.0.0]** 0 0 0 0.<br>Using the embedded webserver or the DTM-based software:<br>• Set FDR synchronization to manual mode.<br>• Before the first connection, select served soft starter configuration. The soft starter needs first to transfer the configuration from the server.<br>• Enter the device name, **DEVICE NAME**, in the **[Communication]** COM, **[Eth Module Config]** ETO submenu. |
| 2 | Turn off the soft starter | Turn off the soft starter and then back on again (control voltage if a separate power supply is being used), otherwise the device name is not taken into account |

| Step | Action | Action |
|---|---|---|
| 3 | Connect the soft starter to the fieldbus | Connect the soft starter and the FDR server (PLC) to the Ethernet fieldbus |
| 4 | Check that the soft starter is operational | Check that the operation has proceeded correctly.<br><br>If downloading has not been possible after a period of 2 min following assignment of the IP addresses, the adapter detects a communication error which, in factory settings mode, triggers an **[FDR 2 Error]** FDR2. |

# Embedded Webserver

## Overview

### Webserver

The Ethernet adapter provides an integrated Web server (in six languages) which allows several functions like: display, parameter settings, and diagnostics. This chapter describes the services provided by this webserver.

The webserver can be accessed from standard browsers like Internet Explorer, Chrome, Safari, or Firefox.

## Connection to the Webserver

### Access

The webserver can be accessed from standard browsers.

In the following example, the soft starter has received the IP address 10.0.0.5:


First connect the computer to the soft starter by typing http:// followed by the soft starter IP address.

You are asked to first enter a **User Name** and a **Password**.

By default the user name is ADMIN. If you are connecting to the webserver for the first time, the password is available:

- on the sticker of the ethernet option module.
- with the Graphic Display Terminal in the **[Cybersecurity]** CYBS submenu and **[Access control]** CSAC submenu.

Once logged in you are asked to change the default connection ID (Password), according to the default security access rule. Access rules can be modified in the Setup/Access Management web page.

Once connected, the webserver home page is displayed.

Using IPV6 network discovery service, there is no need to set IP parameters. The soft starter appears automatically in the network explorer of the PC while physically connected.

The soft starter is identified as ATS••••••••-XXXX where XXXX is the two last bytes of the MAC address.

Right-click and select **Display device web page** to open the webserver.

**NOTE:** If the soft starter was first connected to the SoMove-DTM via the Ethernet option module, and this user's authentication password has been changed, the default password is no longer applicable. The new password is set. This new password is not displayed on the Graphic Display Terminal.

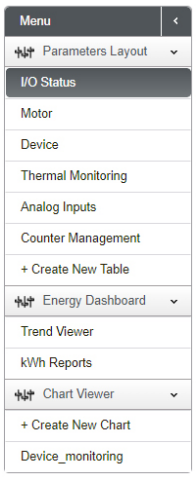
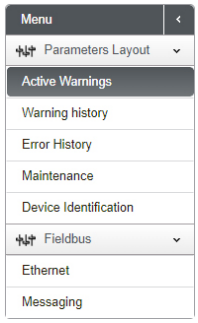
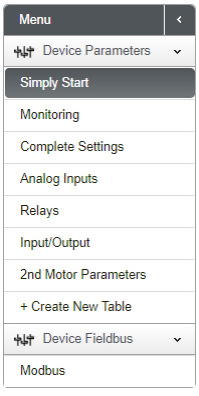
## User Rights - Password and User Names

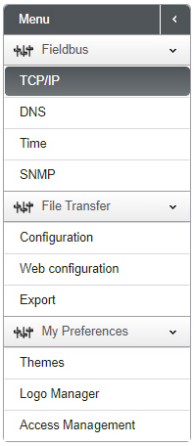
A new password is required if you are connecting to the webserver for the first time. Default security access rule requires minimum eight characters for the new password.

The user names and the password of both level can be modified from the administration section.

## Web Server Site Map

The descriptions of the Web server pages are shown in the following table:

| Page | Menu | Description |
|---|---|---|
| **My Dashboard** | – | This page can be customized, adding or removing Widgets that are designed for a quick overview of the soft starter data. |
| **Display**<br>  | Parameters Layout | Soft starter parameters are displayed in data tables. Customized tables can be created. |
| | Energy Dashboard | Trends show information about the energy consumption of the soft starter. |
| | Chart Viewer | Soft starter parameters are displayed in charts. Customized charts can be created. |
| **Diagnostics**<br>  | Parameters Layout | Soft starter diagnostics are displayed. |
| | Fieldbus | Communication diagnostics are displayed. |
| **Parameters Layout**<br>  | Device Parameters | Soft starters settings can be modified. |
| | Device Fieldbus | Communication settings can be modified. |

| Page | Menu | Description |
|---|---|---|
| **Setup**<br>  | Fieldbus | Soft starter Ethernet settings can be modified. |
| | File Transfer | Soft starter configuration and reports can be downloaded or loaded between a computer and the soft starter. |
| | My Preferences | Webserver access and appearance can be handled. |

**NOTE:** A soft starter's configuration with a firmware version or higher can not be transfered via Webserver to an drive with a firmware version or lower.

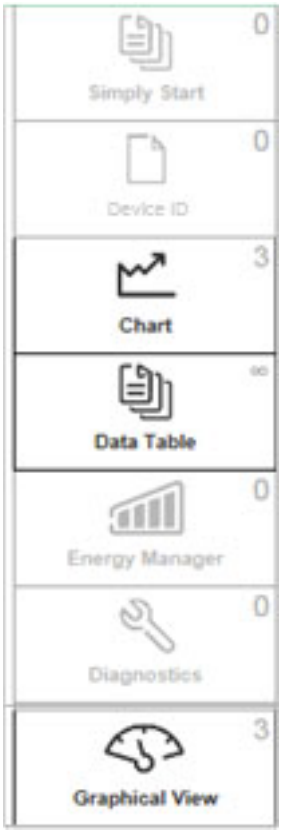
# My Dashboard

## Overview

The following table provides the procedure to add the widget to this page:

| Step | Action |
|---|---|
| 1 | Click the **add a widget** button. |
| 2 | Drag a widget to the desired location. |

The following figure shows the widgets that can be added. Various widgets of a same category are available.



# Display - Device

## Data Table

The following table provides the procedure to create data tables of soft starter parameters.

| Step | Action |
|---|---|
| 1 | Type the name of the table. Spaces are not allowed in this field. |
| 2 | Select a parameter by clicking the top of the parameter or typing the code and clicking the  button. To delete a parameter while creating the table click the parameter. |
| 3 | Click the **Add Table** button. To remove a table click the  button, only visible when the table is selected. |

## Chart Viewer

The following table provides the procedure to create a chart viewer.

| Step | Action |
|---|---|
| 1 | Type the name of the chart. Spaces are not allowed in this field. |
| 2 | Select the plot frequency. |
| 3 | Select the plot frequency unit. |
| 4 | Select the number of plot points. |
| 5 | Select a parameter by clicking the top of the parameter or typing the code and clicking the  button. To delete a parameter while creating the chart click the parameter. Maximum of five parameters can be selected. |
| 6 | Click the **Create Chart** button. To remove a chart click the  button, only visible when chart is selected. |

# Setup - My Preference

## User Access

In this menu, the access to the Web server can be managed by users with administrator rights. These users can add, remove, block, unblock, and modify the access rights of other users.

The following table shows the description of the buttons located in this menu:

| Button | Description |
|---|---|
|  | Add a new user, typing the name of the user; the password and the access rights. |
|  | Block and unblock the access of a user to the webserver. |
|  | Change the password. The administrator can change the password of other users. |

## Themes

In this menu, the aspect of the Web server can be changed. Predefined themes are available, which can be customized.

The following table provides the procedure for creating new themes

| Step | Action |
|---|---|
| 1 | Click the  button. |
| 2 | Type the name of the theme. Spaces are not allowed in this field. |
| 3 | Type the description of the theme. |
| 4 | Upload a logo by clicking the  button. |
| 5 | Type name of the website. |
| 6 | Click the **Save** button. |

## Access Management

Select if login credentials are required or not to access to the web server.

# Fieldbus Integration Using Control Expert (M580)

## Introduction

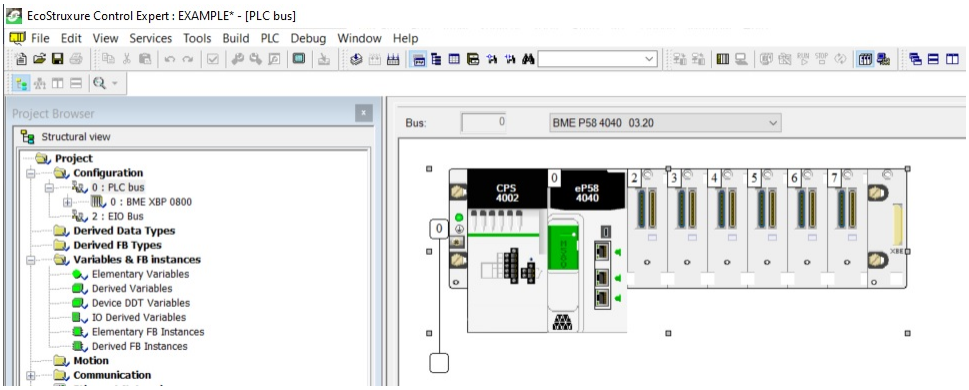
### Overview

The following figure shows the basic configuration to control the soft starter with a M580 PLC.

## EtherNet/IP Configuration

### Ethernet Port Configuration

From the project browser, open the EtherNet/IP port configuration by double-clicking the Ethernet port.

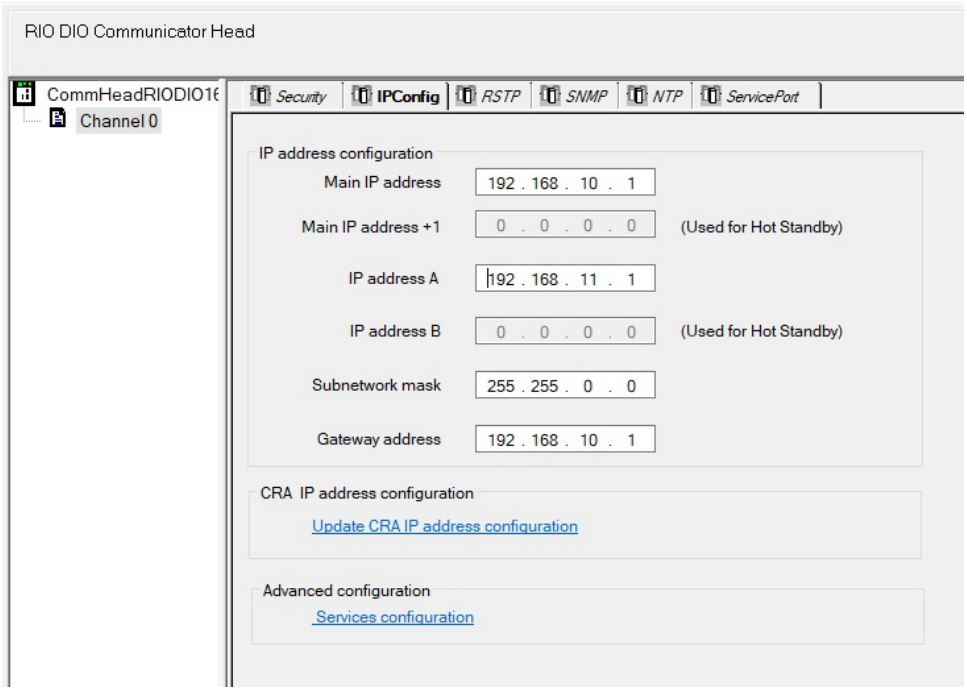


# Configuration of the Client

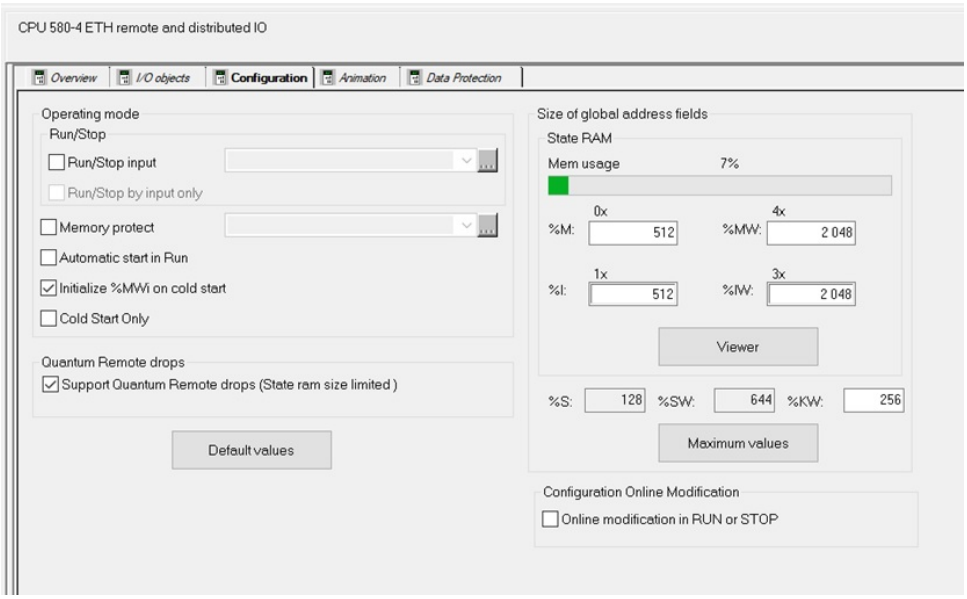
## PLC Configuration

Click on the active port:


The IP address can be managed in the **IPConfig** tab.




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



# Soft Starter Configuration with Control Expert

## Overview

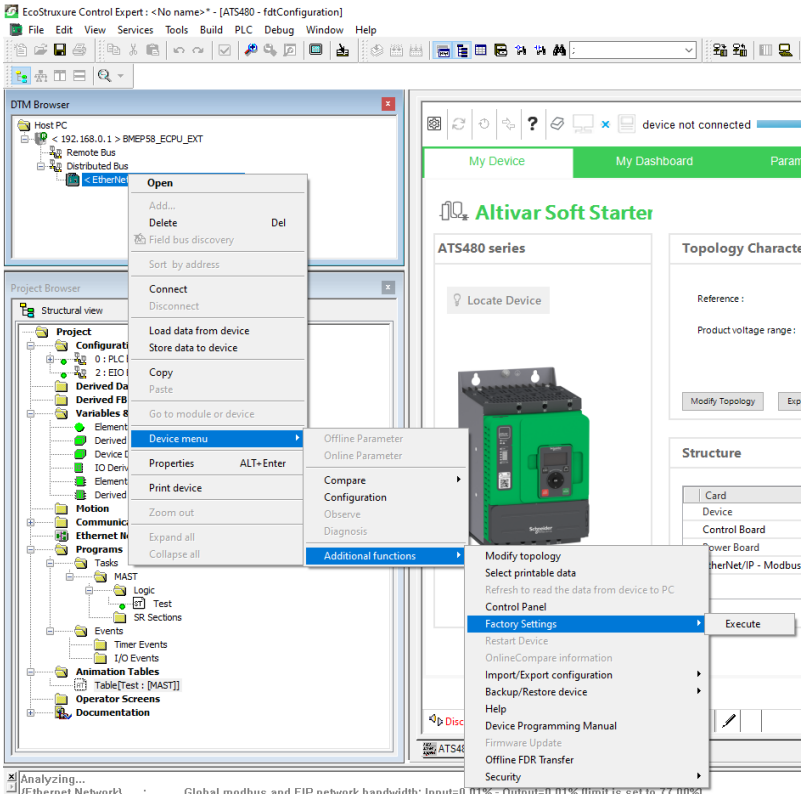
In the following example, the soft starter configuration must be done as follows in-order to establish communication between the soft starter and the M580.

The soft starter configuration is done using the Control Expert software.

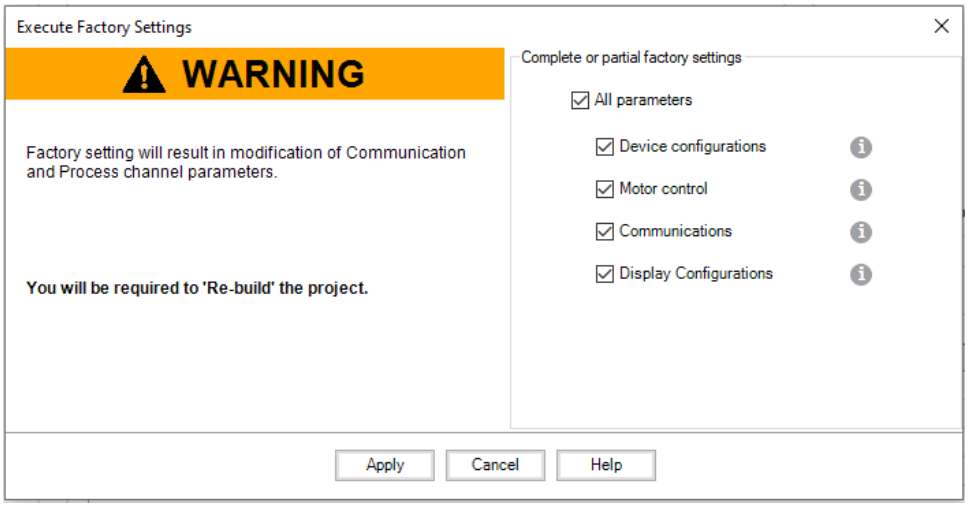
## Factory Settings

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

- Right click on the device, select **Device menu > Additional functions > 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

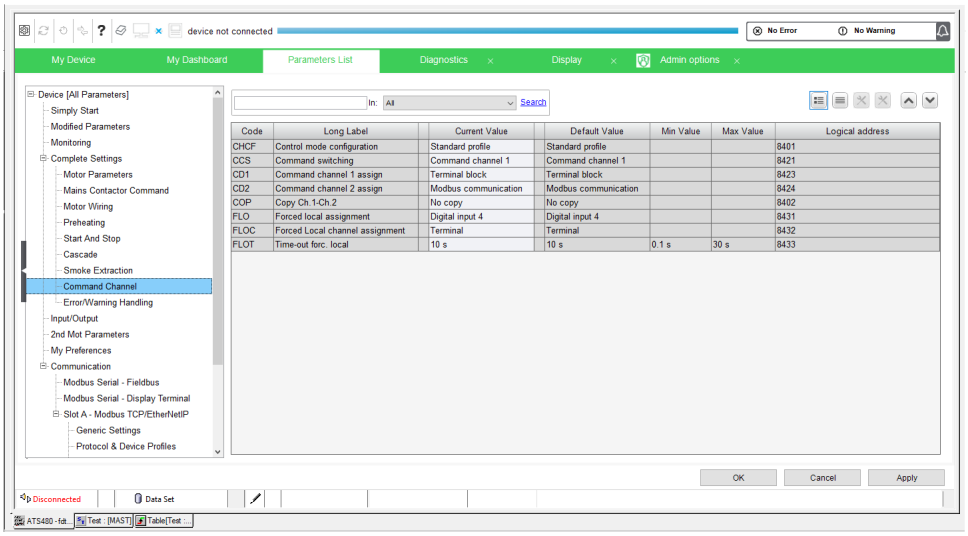
## Command Configuration

To control the soft starter with an Ethernet scanner, select Ethernet scanner as active command.

Go to:

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

**Result:** Following window is displayed:

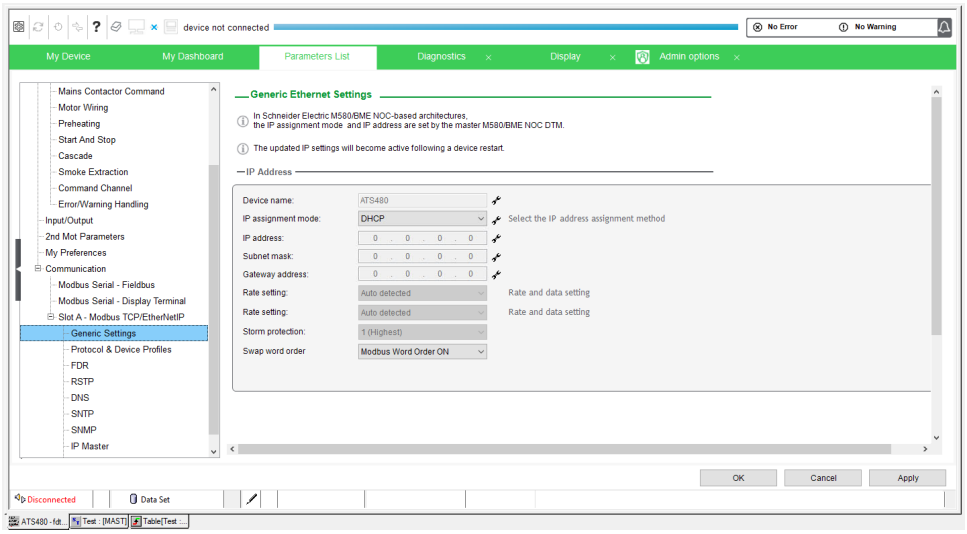



## Ethernet Configuration

To set the Ethernet address of the soft starter, go to:

- **Communication, Slot A - Modbus TCP/EtherNetIP, Generic Setttings.**

**Result:** Following window is displayed:




Perform the configuration according to the network settings.

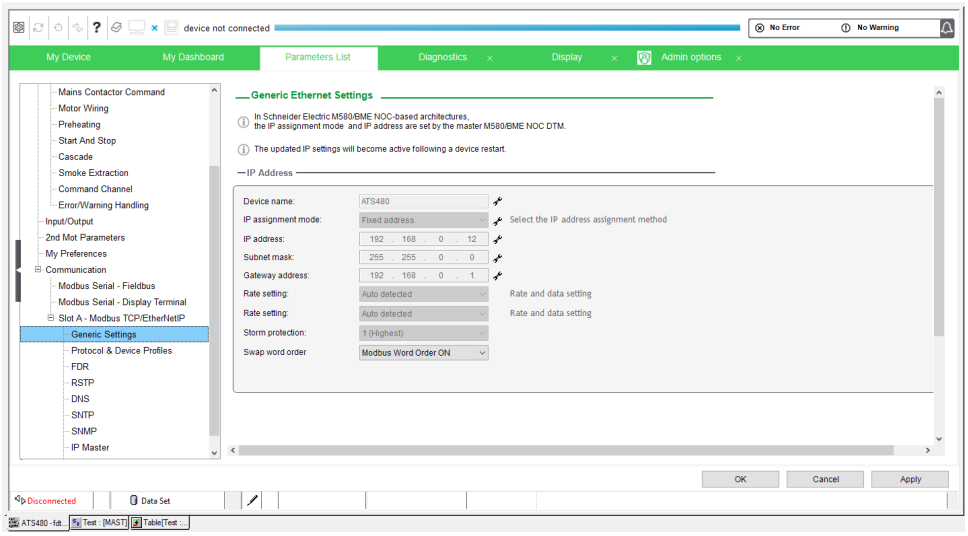
In this example, the soft starter is configured with following data:

- Fixed IP
- IP address: 192.168.0.12
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.0.1

**NOTE:**

Click on **Apply** button to validate the configuration then restart the soft starter.

**Result:** After setting the previous data, following configuration is entered:




## Assemblies Configuration

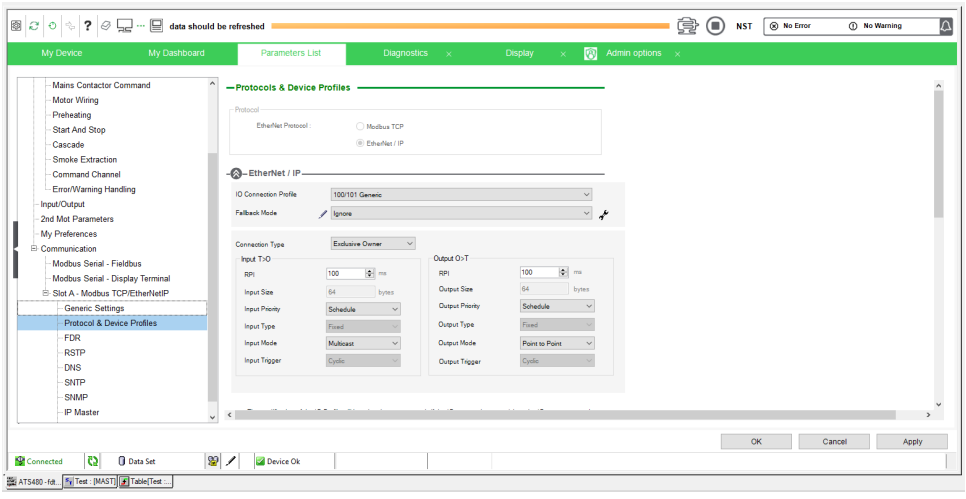
To configure the assemblies used for EtherNet/IP fieldbus, go to:

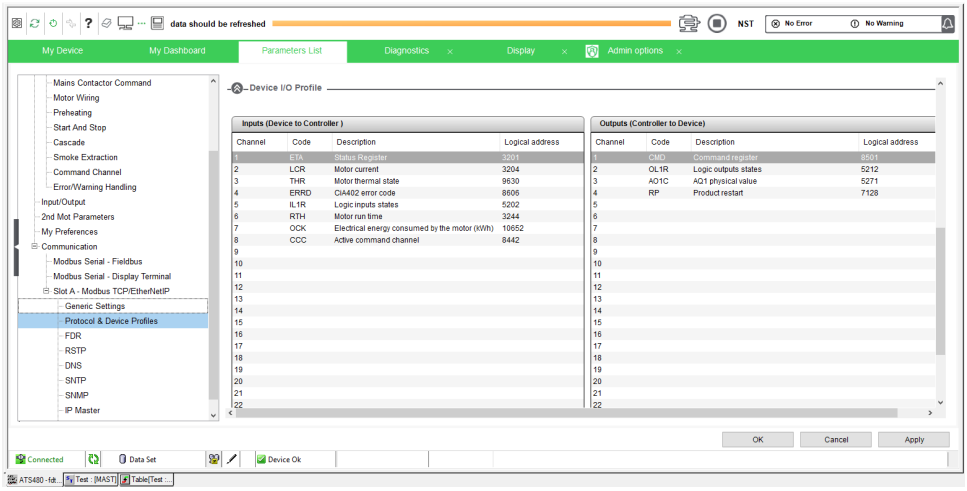
- **Communication, Slot A - Modbus TCP/EtherNetIP, Protocol & Device Profiles.**

Perform the configuration according to the assemblies used in the application.

In this example, assemblies used are 100 and 101.

**Result:** Following windows are displayed:






**NOTE:**

Click on **Apply** button if needed to validate the configuration then restart the soft starter.

## DTM Library

### Configuring the Soft Starter Using Control Expert

Before configuring the soft starter using Control Expert, verify that the DTM and the soft starter firmware are compatible.

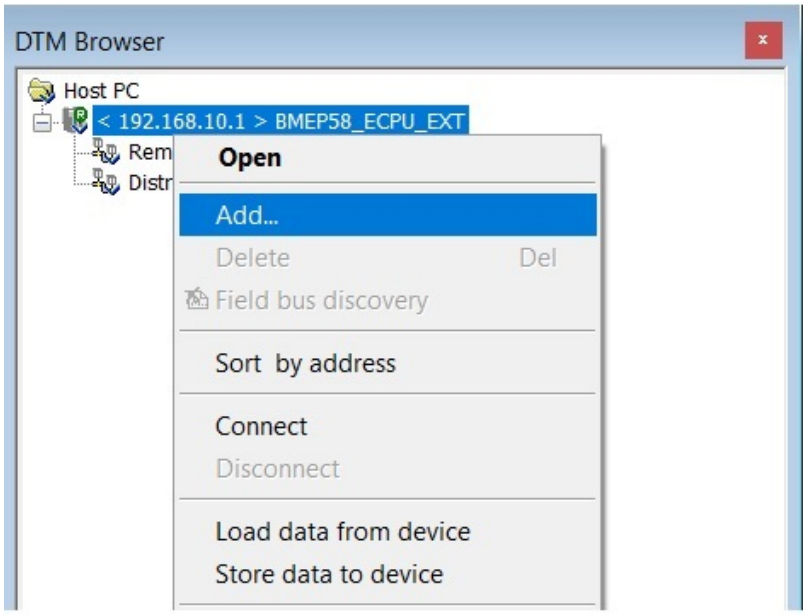
The DTM libraries are available on *www.se.com*.

## DTM Browser

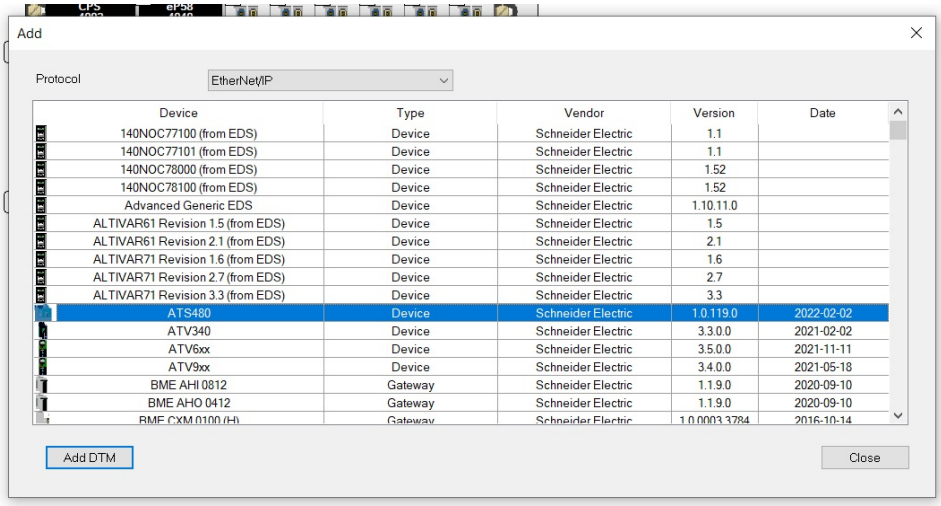
### Launch the DTM Using Control Expert

After installing the DTM library on your PC, restart the Control Expert to add the DTM to the Control Expert libraries.

Open the DTM browser to add the soft starter to the configuration, as shown in the following figure:

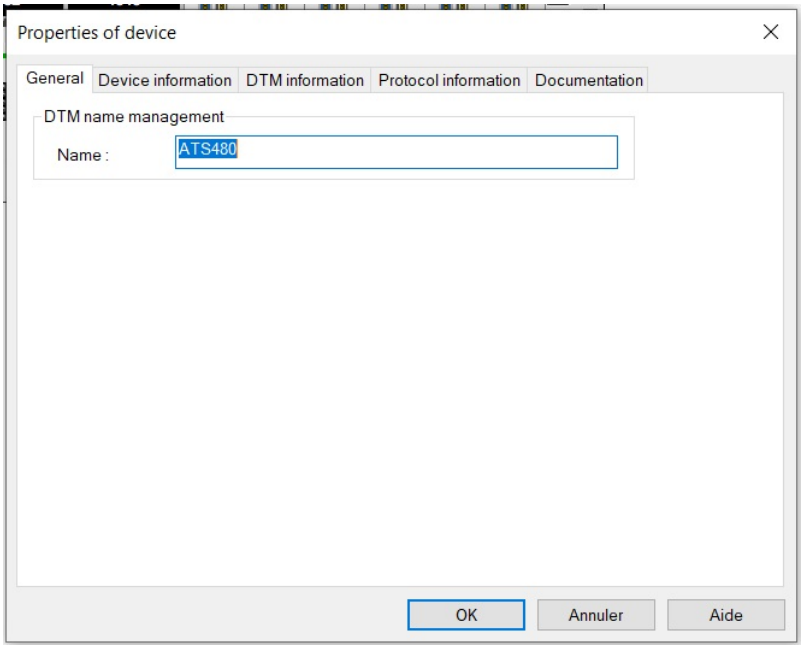



Select the soft starter from the list and click the **Add DTM** button to add the DTM.




You can select even Modbus or EtherNet/IP communication with this configuration.

Finally the soft starter used in the configuration can be named with an alias in order to differentiate it in the case of using other soft starters. The alias name is used by default as device name for FDR service. The DTM online help is available in this window.



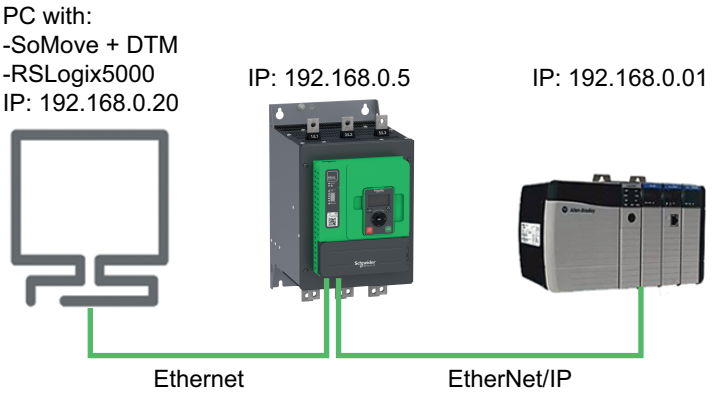
# Software Setup with Allen-Bradley PLC

## Introduction

### Overview

In the following example:

- Soft Starter is connected to an Allen-Bradley Control Logix PLC.
- Communication protocol used is EtherNet/IP with assemblies 100/101.
- Soft Starter can be controlled through the PLC.




## 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 PLC.

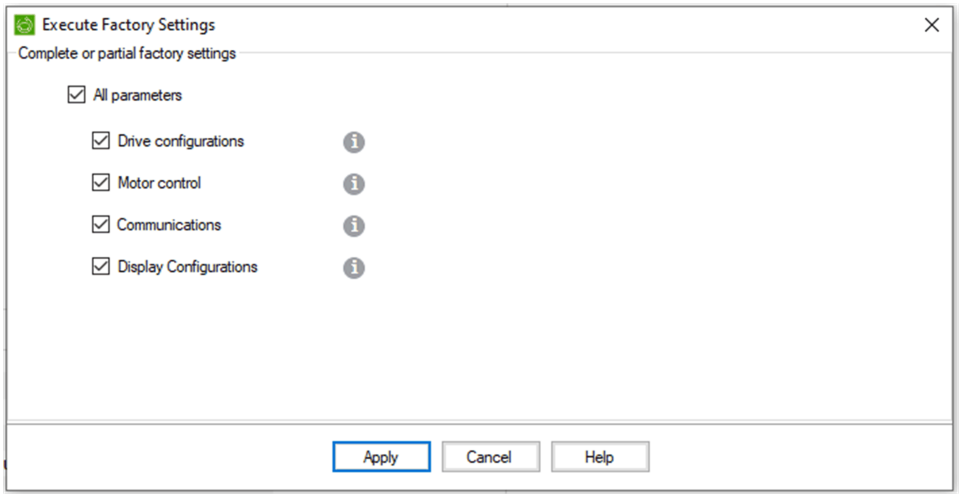
The soft starter configuration is done using the soft starter DTM with SoMove software.

### Factory Settings

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

- On the menu bar, select **Device > 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

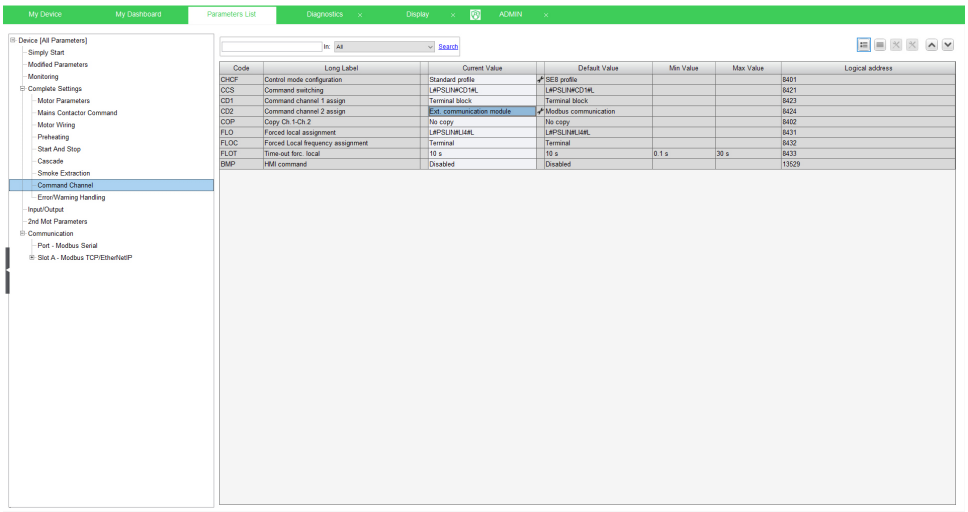
## Command Configuration

To control the soft starter with an Ethernet scanner, select Ethernet as active command.

Go to:

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

**Result:** Following window is displayed:

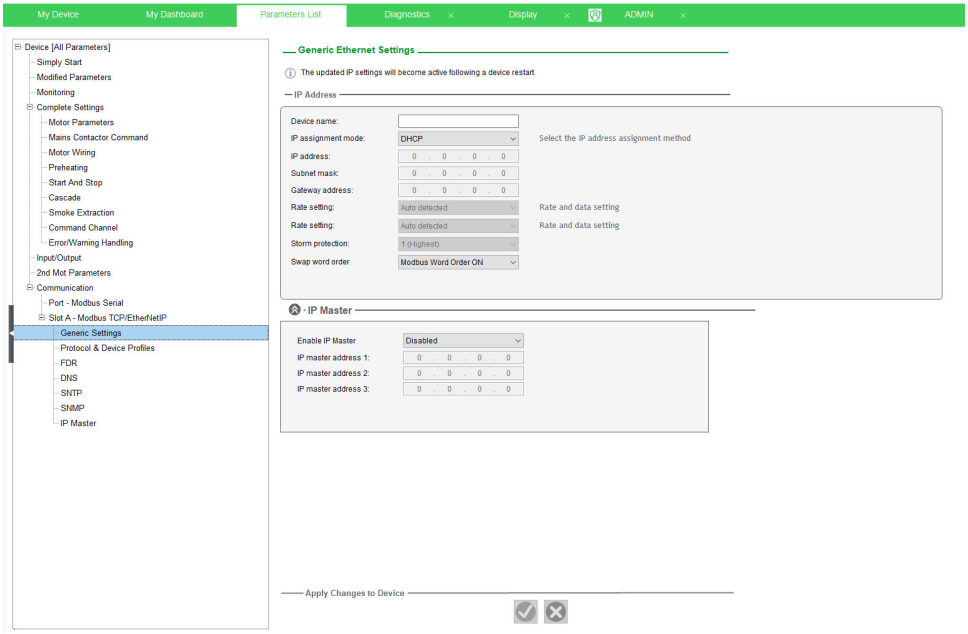



## Ethernet Configuration

To set the Ethernet address of the soft starter, go to:

- **Communication, Slot A - Modbus TCP/EtherNetIP, Generic Setttings.**

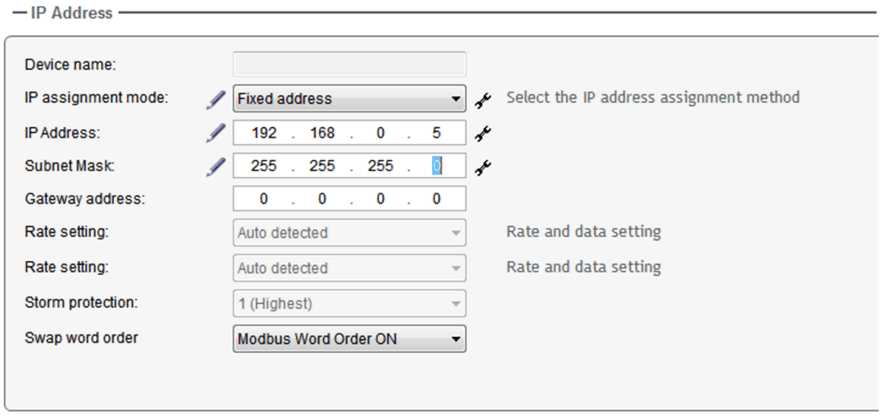
**Result:** Following window is displayed:




Perform the configuration according to the network settings. In this example, the soft starter is configured with following data:

- Fixed IP
- IP address: 192.168.0.5
- Mask: 255.255.255.0

**Result:** After setting the previous data, following configuration is entered:



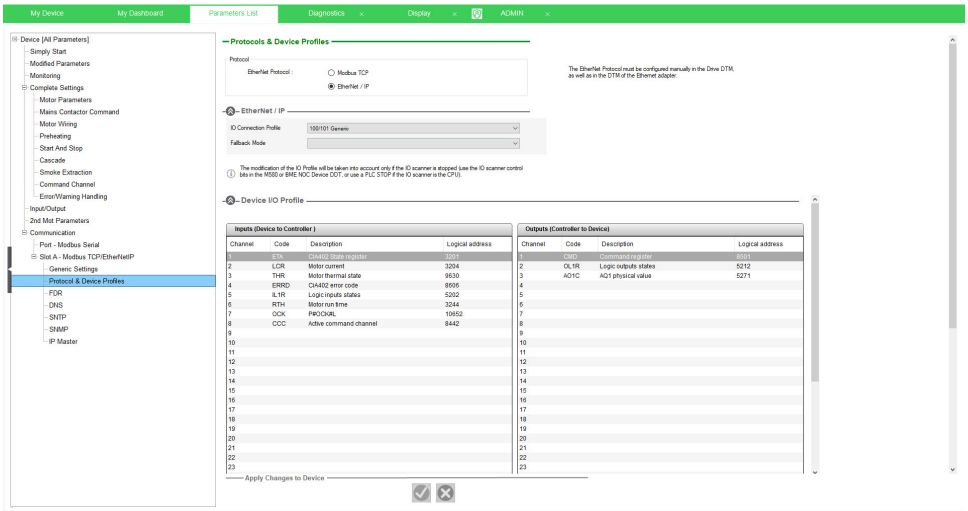

## Assemblies Configuration

To configure the assemblies used for Ethernet/IP fieldbus, go to:

- **Communication, Slot A - Modbus TCP/EtherNetIP, Protocol & Device Profiles.**

Perform the configuration according to the assemblies used in the application. In this example, assemblies used are 100 and 101.

**Result:** Following window is displayed:




**NOTE:**

Click on **Apply** button if needed to validate the configuration then restart the soft starter.

# PLC Configuration

## Overview

In the following example, the PLC is configured to use both types of exchanges available through Ethernet/IP fieldbus:

- Explicit data exchange
- Implicit data exchange

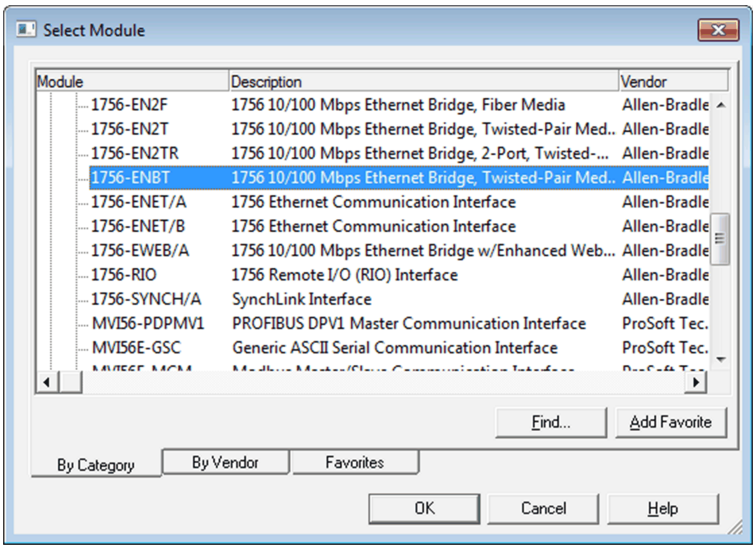
## Adding Ethernet Module

On RSLogix, insert the Ethernet module matching with the hardware configuration.

In this example, the module used is: 1756-ENBT.

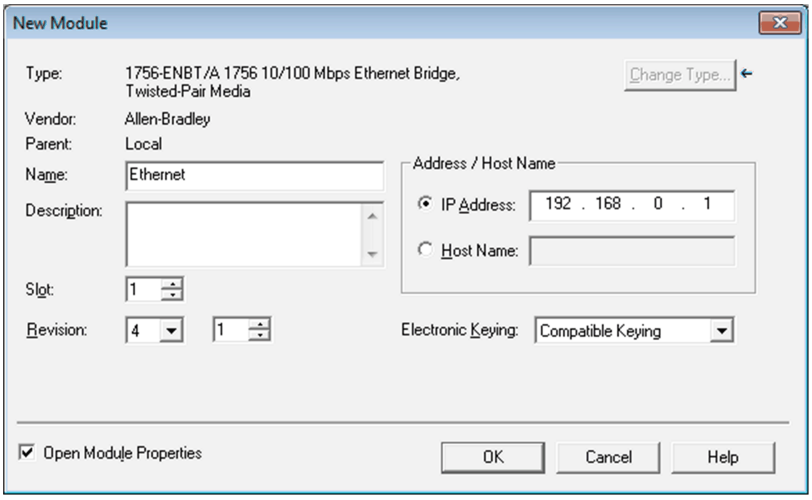
Make a right click on the Backplane and click on **New Module**.

**Result:** Following window is displayed:




Select the corresponding Ethernet module and click on **Create**.

**Result:** Following window is displayed:

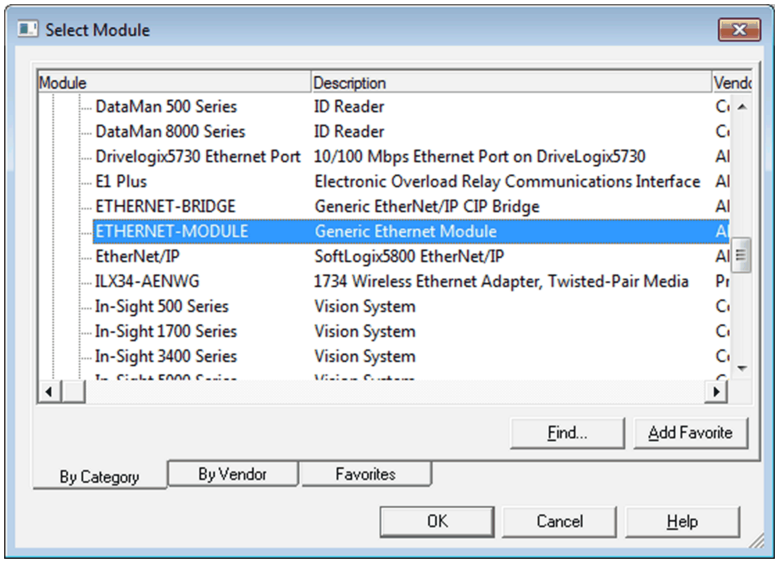



Enter IP address of the module.

## Adding Soft Starter

Make a right click on Ethernet and click on **New Module**.

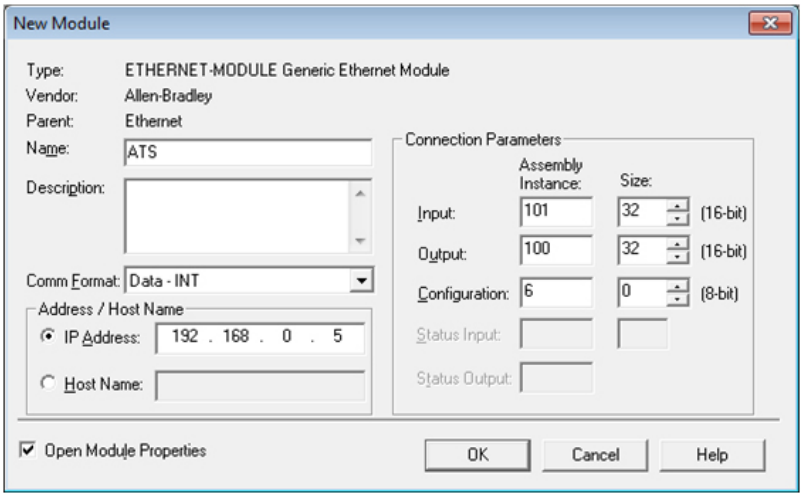
**Result:** Following window is displayed:




Select a Generic Ethernet Module and enter the following information:

- Name: **ATS**
- IP address: **192.168.0.5**
- Input assembly instance: **101**, size: **32 words**
- Output assembly instance: **100**, size: **32 words**
- Configuration instance: **6**

**Result:** Following window is displayed:

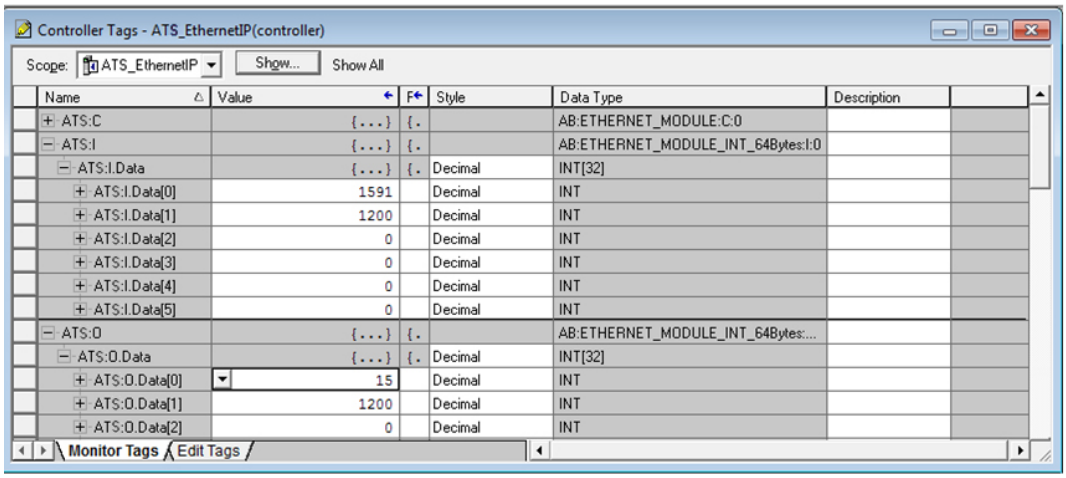



Connect online to the PLC, download the program and run it.

## Explicit Data Exchange

It is possible to verify that explicit data exchange is working by clicking on **Controller Tags**.

The values are refreshed and soft starter can be controlled

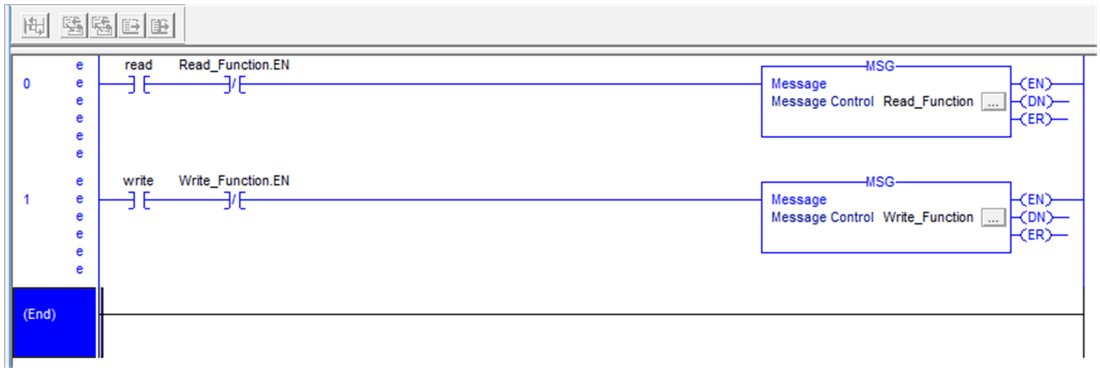



## Implicit Data Exchange

To configure the implicit data exchange, insert a *MSG* block inside a routine.

The following procedure describe how to read and write the value of parameter **[Acceleration]** ACC.

- Create a Routine and do the following program:




The *Read* Boolean will trigger the *Read_Function* to read the **[Acceleration]** ACC parameter.

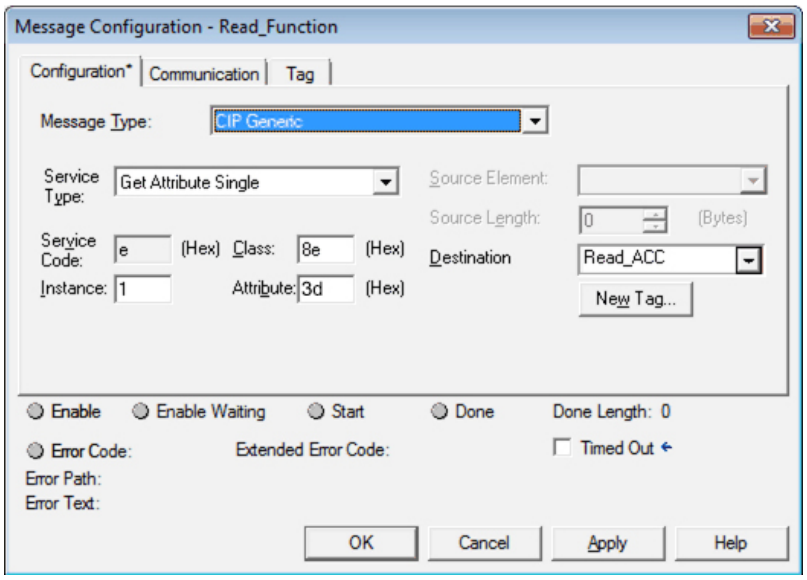
The *Write* Boolean will trigger the *Write_Function* to write the **[Acceleration]** ACC parameter.

**Configuration of *Read_Function*:**

- Click on the **"..."** button of *Read_Function* block and do the following configuration:

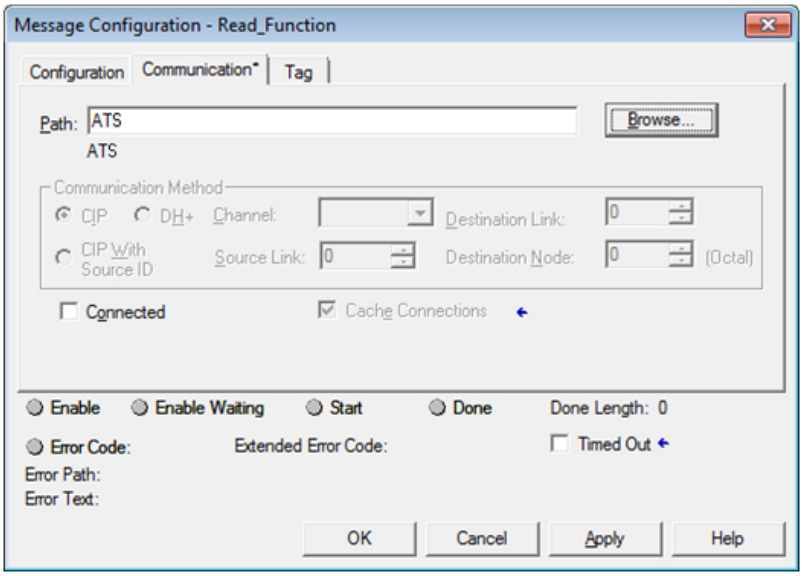
  On the Configuration tab:

  - Enter the CIP address of **[Acceleration]** ACC parameter: 16#8E/01/3D.
  - The value of the parameter will be stored in the variable *Read_ACC*.




On the Communication tab:

- Configure the Path of the device by clicking on **Browse** button.

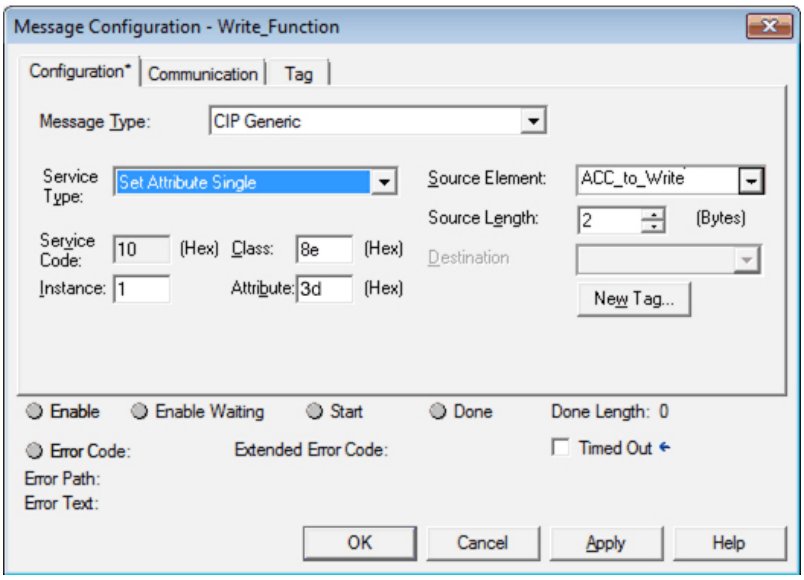



**Configuration of *Write_Function*:**

- Click on the **"..."** button of *Write_Function* block and do the following configuration:

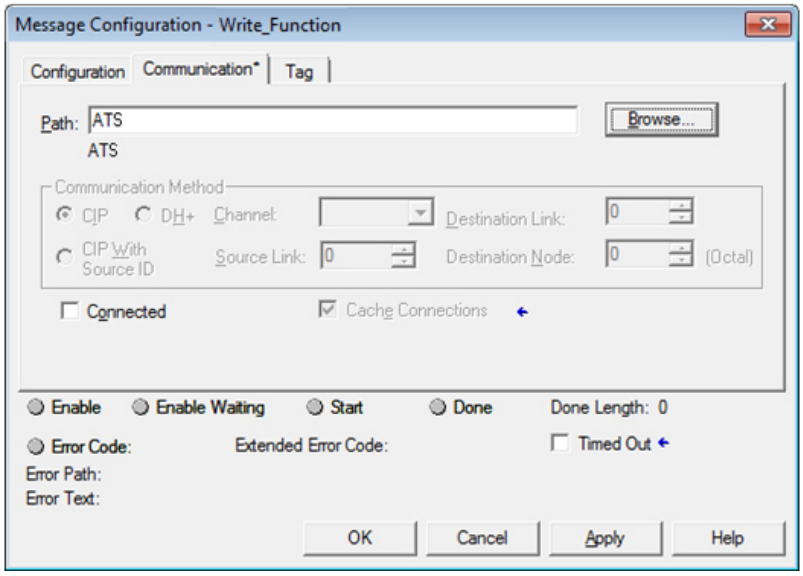
  On the Configuration tab:

  - Enter the CIP address of **[Acceleration]** ACC parameter: 16#8E/01/3D.
  - Enter the variable where the value to write will be stored (here: *ACC_to_Write*)

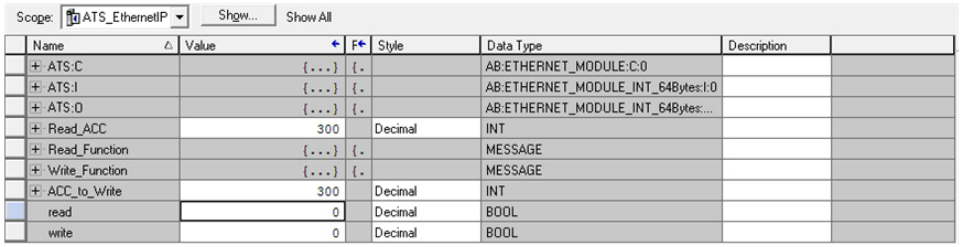



On the Communication tab:

- Configure the Path of the device by clicking on **Browse** button.




It is possible to read or write the **[Acceleration]** ACC parameter by toggling the *Read* or *Write* bits.



# Operations

## Operating States

| ⚠WARNING |
| --- |
| **LOSS OF CONTROL**<br>Perform a comprehensive commissioning test to verify that communication monitoring properly detects communication interruptions<br>**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 **[Fieldbus Interrupt Resp]** CLL parameter.

The values of the **[Fieldbus Interrupt Resp]** CLL parameter, which triggers a soft starter detected error **[Fieldbus Com Interrupt]** CNF are:

| Value | Meaning |
| --- | --- |
| **[Freewheel Stop]** YES | Motor triggers in error and is stopped in freewheel.<br>**Factory setting** |
| **[Deceleration]** DEC | Motor is stopped in deceleration and triggers in error at the end of stop.<br>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.<br>The values are set to **[Braking Level]** BRC and **[DC Braking To Stop]** EBA. |

The values of the **[Fieldbus Interrupt Resp]** CLL parameter which does not trigger a detected error are:

| Value | Meaning |
|---|---|
| **[Ignore]** NO | Detected error ignored (in this case, the warning **[Fieldbus Com Warn]** CLLA 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, fieldbus module communication monitoring is disabled.

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

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

## Detected Errors

Access via :**[Diagnostics]** DIA ➡ **[Diag. data]** DDT ➡ **[Last Error]** LFT

| Parameter | Description | Possible Value | Terminal Display |
|---|---|---|---|
| **[Fieldbus Com Interrupt]** CNF | This parameter is used to indicate that fieldbus error has been detected.<br>When the detected error is active, the value corresponds to the cause of the error.<br>When the cause of the error is no longer active, the value is reset to 0. | • Bit 0: Modbus timeout (linemonitoring) : recoverable<br>• Bit 1: Network Overload<br>• Bit 2: EIP timeout (linemonitoring) : recoverable<br>• Bit 3: EIP idle (controlsupervisor) : recoverable<br>• Bit 4: EIP error trigger (controlsupervisor) : recoverable<br>• Bit 5-7: (reserved)<br>• Bit 8: UAP exception (cpu error) : recoverable<br>• Bit 9: UAP reboot device : recoverable<br>• Bit 10-12: (reserved)<br>• Bit 13: reboot device : unrecoverable<br>• Bit 14: Fatal exception (cpu error) : unrecoverable<br>• Bit 15: (internal usage only) | – |
| **[Fieldbus Error]** EPF2 | – | 1: Invalid IP address<br>2: Duplicate IP address | |
| **[FDR 2 Error]** FDR2 | This parameter is used to indicate that an error has been detected during FDR procedure. Details about this error are provided using **[FDR 1 Error]** FDR1 parameter. | • 0: No error<br>• 1: Server timeout<br>• 2: No file on server<br>• 3: Corrupted file on server<br>• 4: Empty file on server<br>• 5: Invalid file on soft starter<br>• 6: CRC error<br>• 7: Version incompatibility between soft starter and file.<br>• 9: No file on soft starter<br>• 10: File size reading error on server<br>• 11: Soft starter cannot open the file<br>• 12: Soft starter cannot read the file<br>• 13: File incompatibility<br>• 14: Soft starter name is invalid<br>• 15: Incorrect file size on server<br>• 16: Soft starter cannot write the file<br>• 17: Server cannot write the file | • **[No Error]** NO<br>• **[Server Timeout]** TOUT<br>• **[Server No File]** SNF<br>• **[Server Corrupt File]** CRPT<br>• **[Server Empty File]** EPTY<br>• **[Device Invalid File]** HINV<br>• **[CRC Error]** CRC<br>• **[Version Incompatibility]** VRM<br>• **[Device No File]** HNF<br>• **[Server Reading Size]** READ<br>• **[Device Opening File]** OPEN<br>• **[Device Reading File]** FSIZ<br>• **[Incompatibility]** SCNT<br>• **[Device Invalid Name]** NINV<br>• **[Server Incorrect File Size]** FSIZ<br>• **[Device Writing File]** HWF<br>• **[Server Writing File]** SWF |

# 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:

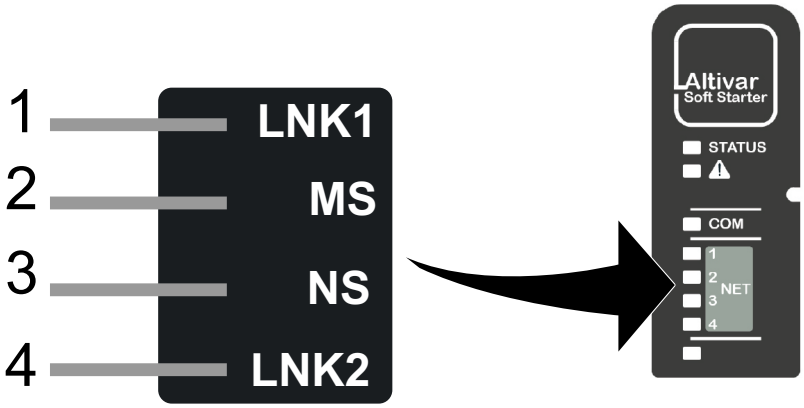
- **[Control Mode]** CHCF is set to **[Standard Profile]** STD.
- Check if **[Cmd channel 1]** CD1 (or **[Cmd channel 2]** CD2) is set on according to the communication source (**[Com. Module]** NET).

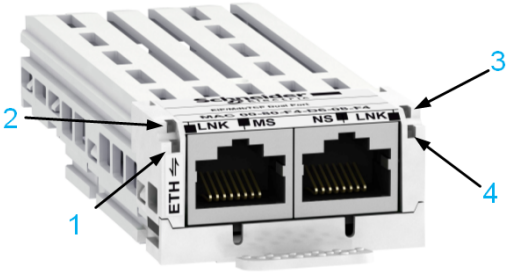
# Diagnostics and Troubleshooting

## Fieldbus Status LEDs

### LED Indicators

The following figure describes the LEDs status for fieldbus monitoring:




### LED Description

| Item | LED | Description |
|---|---|---|
| 1 | **LNK1** | Indicates port A activity. |
| 2 | **MS** | Indicates module status. |
| 3 | **NS** | Indicates network status. |
| 4 | **LNK2** | Indicates port B activity. |

### LNK1 and LNK2

These LEDs indicate the status of the Ethernet adapter ports:

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

| Color & status | Description |
|---|---|
| Blinking Green | Fieldbus activity at 100 Mbit/s |
| Blinking Yellow | Fieldbus activity at 10 Mbit/s |

## NS: Network Status

This LED indicates the status of the fieldbus.

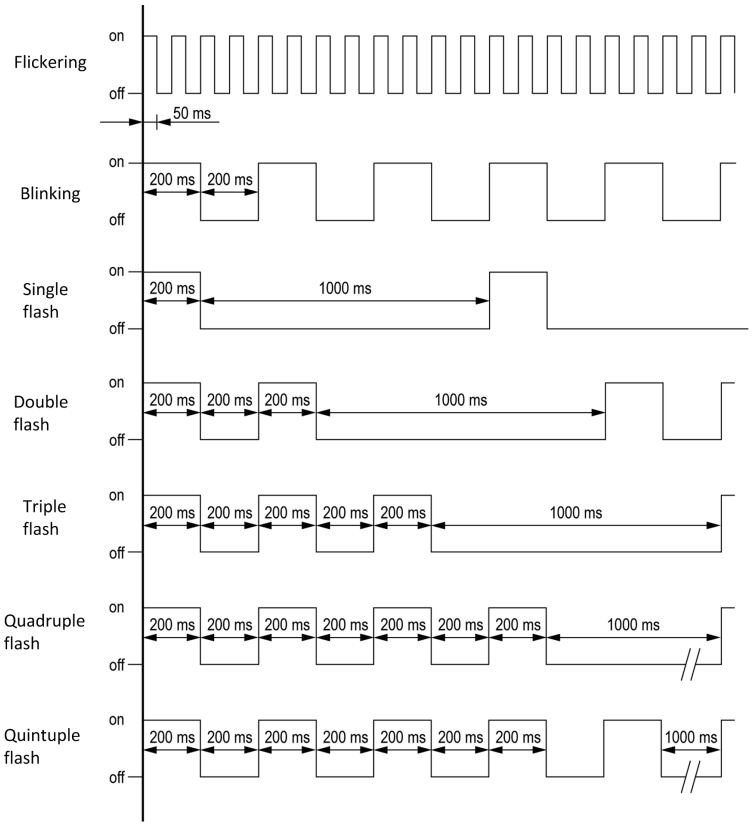
| Color & status | Description |
|---|---|
| OFF | The device does not have an IP address or powered off |
| Blinking Green/ Red | Power on testing |
| Green ON | A connection is established to control the command word. |
| Blinking Green | Device has a valid IP, but no command word connection. |
| Red ON | Duplicated IP |
| Blinking Red | An established connection to control the command word is closed or timed out |

## MS: Module Status

This LED indicates the status of the adapter.

| Color & status | Description |
|---|---|
| OFF | No power is supplied to the device |
| Blinking Green/ Red | Power on testing |
| Green ON | The device is operating correctly. |
| Blinking Green | Device has not been configured. |
| Blinking red | The device has detected a recoverable minor detected error. |
| Red ON | The device has detected a non-recoverable major detected error. |

## LED Behavior



# Connection problem with the fieldbus module

## Description

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

Verify the following:

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

# 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 |

## Network Monitoring Criteria

The table provides the details of the detected errors:

| Protocol | Error Code | Criteria | Remedy |
|---|---|---|---|
| Ethernet module | **[Fieldbus Error]** EPF2 | An external error has been triggered. | • A faulty or duplicate address can cause conflicting issues.<br>• Try setting a different fixed IP address |
| | **[Fieldbus Com Interrupt]** CNF | This error is triggered by the timeout and appears when the communication is stopped or interrupted with the module. | Increase the value of **[Ethernet Timeout]** TOUT. |
| | **[FDR 2 Error]** FDR2 | Ethernet fieldbus module FDR error. | To eliminate the FDR error, the following steps must be performed:<br>• Change **[ETH Option IP Mode]** IM10 to **[DHCP]** DHCP and restart the soft starter.<br>• FDR is active and **Automatic Syncho Cycle** is off.<br>• Disable the FDR and restart the soft starter.<br>• Change the **[ETH Option IP Mode]** IM10 to **[Fixed]** MANU and restart the soft starter. |

## 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.

# Control-Signal Diagnostics

## Introduction

On the display terminal, the **[Communication]** COM — **[Communication map]** CMM submenu can be used to display control-signal diagnostic information between the soft starter and the controller:

- Active command channel **[Command Channel]** CMDC
- Value of the control word **[Cmd Register]** CMD from the active command channel **[Command Channel]** CMDC
- Value of the operating state word **[Status Register]** ETA
- Specific data for all available fieldbusses are in dedicated submenus.
- In the **[Command word image]** CWI submenu: control words from all channels

## Control Word Display

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

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

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

## Operating State Word Display

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

The table provides the bit details of ETA parameter:

| Bit | Description |
|---|---|
| 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 | Warning |
| Bit8 | Reserved |
| Bit9 = 0 | Local mode control |
| Bit10 | Reserved |
| Bit11 | Reserved |
| Bit12 | Reserved |
| Bit13 | Reserved |
| Bit14 = 1 | Stop imposed via **STOP** key |
| Bit15 | Reserved |

# 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.

## D

**DC:**

Direct Current

**dec.:**

Decimal

**DP:**

Decentralized Periphery

**DPWS:**

Device Profile for Web Service

## 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

## L

**LSB:**

Least Significant Byte

## M

**MIB:**

A management information base **(MIB)** is a database used for managing the entities in a communication network.

**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.

**MSB:**

Most Significant Byte

## P

**Parameter:**

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

**PELV:**

Protective Extra Low Voltage, low voltage with isolation. For more information: IEC 60364-4-41.

**PLC:**

Programmable logic controller.

**Power stage:**

The power stage controls the motor. The power stage generates current for controlling the motor.

## Q

**QoS:**

Quality of Service

**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.

**SNMP:**

Simple Network Management Protocol

**SNTP:**

Simple Network Time Protocol

**SYNC:**

Synchronization Object

## 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.



NNZ85540.02 – 04/2022