

Altivar Process ATV900

Variable Speed Drives

CIP Safety Manual – VW3A3809

JYT89146.01
03/2023



Legal Information

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

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

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

As part of a group of responsible, inclusive companies, we are updating our communications that contain non-inclusive terminology. Until we complete this process, however, our content may still contain standardized industry terms that may be deemed inappropriate by our customers.

Table of Contents

Safety information and About the Book	4
Safety Information	5
About the Book	10
General System Description	15
Introduction	16
Accessories	18
Certifications	19
Cyber Security	20
Basics	22
Safety Function Capability	25
Technical Data	26
Installation of the CIP Safety Drive	27
Installation Topology	29
Safety Function STO (Safe Torque Off)	30
Overview	31
Limitations	32
CIP Safety objects	33
Introduction	34
Object map	34
Display	40
Dedicated Safety Function menu in the Display Terminal	41
Commissioning and Display	44
Configuration of the safety system	45
Prerequisites to Configure the Safety drive	46
Configuration with the commissioning software	46
M580 Safety Configuration	47
Configuration of the CIP Safety Drive	50
Acceptance Test	60
Operating and maintenance	62
Operation with CIP Safety configuration	63
Reset Ownership	65
Diagnostics and Troubleshooting	66
Operating states	67
Detected Errors	68
Maintenance and decommissioning	75
Remove or replace the safety drive	76
Remove or replace the safety controller	78
Clone the safety drive	79
Reset safety configuration of the safety drive	80
Decommission the safety drive	81
Glossary	82

Safety information and About the Book

What's in This Part

Safety Information	5
About the Book	10

Safety Information

What's in This Chapter

Qualification of Personnel6
 Intended Use6
 Product Related Information.....6

Important Information

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



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



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

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

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

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

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

Please Note

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

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

Qualification of Personnel

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

Intended Use

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

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

Product Related Information

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

DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

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

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

⚡⚠ DANGER**HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH**

Before performing work on the drive system:

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

Before applying voltage to the drive system:

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

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

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

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

⚡⚠ DANGER**ELECTRIC SHOCK OR UNANTICIPATED EQUIPMENT OPERATION**

Do not use damaged products or accessories.

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

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

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

⚠ DANGER**POTENTIAL FOR EXPLOSION**

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

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

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

As a designer/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 drive cannot provide all safety-related functionality for your entire application, you must ensure that the required Performance Level and/or Safety Integrity Level is reached by installing all necessary additional equipment.

▲ WARNING

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

- Conduct a risk assessment according to EN ISO 12100 and all other standards that apply to your application.
- Use redundant components and/or control paths for all critical control functions identified in your risk assessment.
- Implement all monitoring functions required to avoid any type of hazard identified in your risk assessment, for example, slipping or falling loads, in particular, if you do not operate the drive in closed loop mode which provides certain internal monitoring functions such as BRH3 [BRH b3], BRH4 [BRH b4] and BRH5 [BRH b5].
- 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.

A specific application note NHA80973 is available on hoisting machines and can be downloaded on se.com.

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

▲ WARNING

UNANTICIPATED EQUIPMENT OPERATION

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

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

⚠ WARNING**LOSS OF CONTROL**

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

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

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

About the Book

What's in This Chapter

Document Scope.....	11
Validity Note.....	11
Related Documents.....	12
Terminology.....	14
Contact us.....	14

Document Scope

The purpose of this document is to provide information about the CIP safety module and supported safety function.

Validity Note

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

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

This documentation is valid for the Altivar Process drives.

Except for:

- ATV930••••• Three-phase: 500...690 V (kW/HP)
- ATV9•0C11N4• and ATV9•0C16N4•
- ATV9•0M10••
- ATV993
- ATV9A0,ATV9B0, ATV9L0

The technical characteristics of the devices described in the present document also appear online. To access the information online, go to the Schneider Electric home page www.se.com/ww/en/download/.

The characteristics that are described in the present document 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 document and online information, use the online information as your reference.


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

Related Documents

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

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

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

Title of Documentation	Catalog Number
Catalog: Variable speed drives Altivar Process ATV900	DIA2ED2150601EN (English) DIA2ED2150601FR (French)
ATV930, ATV950 Getting Started	NHA61578 (English) NHA61579 (French) NHA61580(German) NHA61581 (Spanish) NHA61724 (Italian) NHA61582 (Chinese) NHA61578PT (Portuguese) NHA61578TR (Turkish)
ATV900 Getting Started Annex (SCCR)	NHA61583 (English)
Video: Getting Started with Altivar Process ATV900	FAQ000240081 FAQ (English) 
ATV930, ATV950 Installation manual	NHA80932(English) NHA80933 (French) NHA80934(German) NHA80935 (Spanish) NHA80936 (Italian) NHA80937 (Chinese) NHA80932PT (Portuguese) NHA80932TR (Turkish)
ATV900 Programming manual	NHA80757 (English) NHA80758 (French) NHA80759(German) NHA80760 (Spanish) NHA80761 (Italian) NHA80762 (Chinese) NHA80757PT (Portuguese) NHA80757TR (Turkish)
ATV900 Embedded Modbus Serial Link manual	NHA80939 (English)
ATV900 Embedded Ethernet manual	NHA80940 (English)
ATV900 PROFIBUS DP manual (VW3A3607)	NHA80941 (English)
ATV900 DeviceNet manual (VW3A3609)	NHA80942 (English)
ATV900 PROFINET manual (VW3A3627)	NHA80943 (English)
ATV900 CANopen manual (VW3A3608, 618, 628)	NHA80945 (English)
ATV900 EtherCAT manual (VW3A3601)	NHA80946 (English)
ATV900 POWERLINK manual (VW3A3619)	PHA99693 (English)
ATV900 Communication Parameters addresses	NHA80944 (English)
ATV900 DC Bus Sharing Technical Note PHA25028	PHA25028 (English)

Title of Documentation	Catalog Number
ATV900 Embedded Safety Function manual	NHA80947 (English)
ATV900 Safety functions manual with Module VW3A3802	NVE64209 (English) NVE64210 (French) NVE64211(German) NVE64212 (Spanish) NVE64213 (Italian) NVE64214 (Chinese) NVE64209PT (Portuguese) NVE64209TR (Turkish)
ATV900 Braking unit for Frame Size 6 manual (MFR66979)	MFR66979 (English)
ATV900 Braking unit for Frame Size 7 manual (VW3A7101)	1757084 (English)
Drive Systems ATV960 handbook	NHA37115 (English) NHA37114 (German)
Drive Systems ATV980 handbook	NHA37117 (English) NHA37116 (German)
Drive Systems Installation manual	NHA37119 (English) NHA37118(German) NHA37121(French) NHA37122 (Spanish) NHA37123 (Italian) NHA37124 (Dutch) NHA37126(Polish) NHA37127(Portuguese) NHA37129 (Turkish) NHA37130 (Chinese)
Altivar Application Note for Hoisting	NHA80973 (English)
ATV600F, ATV900F Installation Instruction sheet	NVE57369 (English)
ATV600, ATV900 ATEX manual	NVE42416 (English)
ATV61-71 to ATV600-900 Migration Manual	EAV64336 (English)
Modicon M580, Safety Manual	QGH46982 (English)
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)
ATV900: DTM	ATV9xx_DTM_Library_EN(English - to be installed first) ATV9xx_DTM_Lang_FR (French) ATV9xx_DTM_Lang_DE (German) ATV9xx_DTM_Lang_SP (Spanish) ATV9xx_DTM_Lang_IT (Italian) ATV9xx_DTM_Lang_CN (Chinese)
Recommended Cybersecurity Best Practices	CS-Best-Practices-2019-340 (English)
Schneider Electric VDMA66413 reliability values Libraries	Catalog: Reliability_values (English)
EDS file: CIP_Safety_EDS_VW3A3809_V1.1IE03	CIP_Safety_EDS_VW3A3809_V1.1IE03 (English)

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

Terminology

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

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

Among others, these standards include:

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

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

Also see the glossary at the end of this manual.

Contact us

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

Schneider Electric Industries SAS

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

France

General System Description

What's in This Part

Introduction.....	16
Accessories	18
Certifications.....	19
Cyber Security	20
Basics	22
Safety Function Capability	25

Introduction

Overview

The safety function STO (Safe Torque Off) does not remove power from the DC bus. The safety function STO only removes power to the motor. The DC bus voltage and the mains voltage to the drive are still present.

DANGER

HAZARD OF ELECTRIC SHOCK

- Do not use the safety function STO for any other purposes than its intended function.
- Use an appropriate switch, that is not part of the circuit of the safety function STO, to disconnect the drive from the mains power.

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

When the safety function STO is triggered, the power stage is immediately disabled. It forces the motor to stop in freewheel.

WARNING

INSUFFICIENT DECELERATION OR UNINTENDED EQUIPMENT OPERATION

Verify that decelerating in freewheel when the safety function STO is triggered does not result in unsafe conditions.

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

When the safety function STO is triggered, the power stage is immediately disabled. In the case of vertical applications or external forces acting on the motor shaft, you may have to take additional measures to bring the motor to a standstill and to keep it at a standstill when the safety function STO is used, for example, by using a service brake.

WARNING

INSUFFICIENT DECELERATION OR UNINTENDED EQUIPMENT OPERATION

- Verify that using the safety function STO does not result in unsafe conditions.
- If standstill is required in your application, ensure that the motor comes to a secure standstill when the safety function STO is used.

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

▲ WARNING

INEFFECTIVE SAFETY FUNCTIONS

- Verify that a risk assessment as per ISO 12100-1 and/or any other equivalent assessment has been performed before this product is used.
- Verify that only persons who are trained and certified experts in safety engineering and who are familiar with all safety-related standards, provisions, and regulations such as, but not limited to, IEC 61800-5-2 work with this product.
- Verify that only persons who are thoroughly familiar with the safety-related applications and the non-safety-related applications as well as the hardware used to operate the machine/process, work with this product.
- After any transfer of safety configuration to the safety drive, verify the correct operation and effectiveness of all functions by performing comprehensive tests for all operating states, the defined safe state, and all potential error situations.

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

▲ WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Only start the machine/process if there are no persons or obstructions in the zone of operation.
- Only make modifications of any type whatsoever, including, but not limited to, parameter values, settings, configurations, hardware, if you fully understand all effects of such modifications.
- Verify that modifications do not compromise or reduce the Safety Integrity Level (SIL), Performance Level (PL) and/or any other safety-related requirements and capabilities defined for your machine/process.
- After modifications of any type whatsoever, restart the machine/process and verify the correct operation and effectiveness of all functions by performing comprehensive tests for all operating states, the defined safe state, and all potential error situations.
- If you have to commission or recommission the machine/process, perform a commissioning test pursuant to all regulations, standards, and process definitions applicable to your machine/process.
- Document all modifications in compliance with all regulations, standards, and process definitions applicable to your machine/process.

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

CIP Safety module (VW3A3809) provides a networked STO (Safe Torque Off) function via an Ethernet/IP network.

The STO safety function supported by the CIP safety module is intended to maintain the safe condition or prevent hazardous conditions. In some cases, external safety-related systems (for example a mechanical brake) may be necessary to maintain the safe condition when electrical power is removed.

The configuration of the CIP safety module can only be done via the commissioning software Ecostruxure Control Expert and Altivar DTM.

The CIP safety module is compliant with the software version from **V2.1IE82** of Altivar Process ATV900 drives. If this requirement is not respected, the safety module is ignored by the drive.

The Altivar Process ATV900 drives are compliant with the requirements of the standards in terms of implementation of STO safety functions.

Accessories

Additional Module Support

Description	Weight in kg (lb)	Order No.
Additional module support: to add a slot for an CIP Safety module.	0.4 (0.89)	VW3A3800

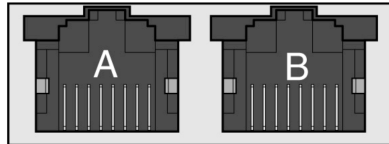
Ethernet cable for CIP Safety connection

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)
- RJ45 Connector, 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)

Pin Layout of the RJ45 female sockets for the Ethernet connection

The drive 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	–	–

Certifications

EC Declaration of Conformity

The EC Declaration of Conformity for the EMC Directive can be obtained on www.se.com.

Functional Safety Certification

The integrated safety functions are compatible and certified according to IEC 61800-5-2 Ed.2 Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional.

IEC 61800-5-2, as a product standard, sets out safety-related considerations of Power Drive System Safety Related PDS (SR)s in terms of the framework of the IEC 61508 Ed.2 series of standards.

Compliance with the IEC 61800-5-2 standard, for the safety functions described below, facilitate incorporation of a PDS (SR) (Power Drive System suitable for use in safety-related applications) into a safety-related control system using the principles of IEC 61508, or IEC 13849-1, as well as IEC 62061 for process systems and machinery.

The defined safety functions are:

- SIL2 and SIL3 capability in compliance with IEC 61800-5-2 and the IEC 61508 Ed.2 series.
- Performance level d and e in compliance with ISO 13849-1.
- Compliant with Category 3 and 4 of ISO 13849-1.

Also refer to safety function Capability.

The safety demand operating mode is considered to be high demand or continuous mode of operation according to the IEC 61800-5-2 standard.

The functional safety certificate is accessible on www.se.com.

Cyber Security

Overview

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

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

The basic components of this approach are:

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

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.

Security Policy

The device does not have the capability to transmit data encrypted using the CIP Safety protocol. If other users gained access to your network, transmitted information can be disclosed or subject to tampering.

⚠ WARNING

CYBERSECURITY HAZARD

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

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

For detailed information about cybersecurity policy for the CIP safety environment, please refer to the ATV900 Programming manual, page 12.

Basics

Functional Safety

Automation and safety engineering are two areas that were completely separate in the past but have recently become more and more integrated.

The engineering and installation of complex automation solutions are greatly simplified by integrated safety functions.

Usually, the safety engineering requirements depend on the application.

The level of requirements results from the risk and the hazard potential arising from the specific application.

IEC 61508 Standard

The standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems covers the safety-related function.

Instead of a single component, an entire function chain (for example, from a sensor through the logical processing units to the actuator) is considered as a unit.

This function chain must meet the requirements of the specific safety integrity level as a whole.

Systems and components that can be used in various applications for safety tasks with comparable risk levels can be developed on this basis.

SIL - Safety Integrity Level

The standard IEC 61508 defines 4 safety integrity levels (SIL) for safety functions.

SIL1 is the lowest level and SIL4 is the highest level.

A hazard and risk analysis serves as a basis for determining the required safety integrity level.

This is used to decide whether the relevant function chain is to be considered as a safety function and which hazard potential it must cover.

PFH - Probability of a Dangerous Hardware Failure Per Hour

To maintain the safety function, the IEC 61508 standard requires various levels of measures for avoiding and controlling detected faults, depending on the required SIL.

All components of a safety function must be subjected to a probability assessment to evaluate the effectiveness of the measures implemented for controlling detected faults.

This assessment determined the PFH (Average frequency of dangerous failure) for a safety system.

This is the probability per hour that a safety system fails in a hazardous manner and the safety function cannot be correctly executed.

Depending on the SIL, the PFH must not exceed certain values for the entire safety system.

The individual PFH values of a function chain are added. The result must not exceed the maximum value specified in the standard.

Safety Integrity Level	Average frequency of dangerous failure (PFH) at high demand or continuous demand
4	$\geq 10^{-9} \dots < 10^{-8}$
3	$\geq 10^{-8} \dots < 10^{-7}$
2	$\geq 10^{-7} \dots < 10^{-6}$
1	$\geq 10^{-6} \dots < 10^{-5}$

PL - Performance Level

The standard ISO 13849-1 defines 5 Performance levels (PL) for safety functions. a is the lowest level and e is the highest level.

Five levels (a, b, c, d, and e) correspond to different values of Average frequency of dangerous failure.

Performance level	Probability of a dangerous Hardware Failure per Hour
e	$\geq 10^{-8} \dots < 10^{-7}$
d	$\geq 10^{-7} \dots < 10^{-6}$
c	$\geq 10^{-6} \dots < 3 * 10^{-6}$
b	$\geq 3 * 10^{-6} \dots < 10^{-5}$
a	$\geq 10^{-5} \dots < 10^{-4}$

HFT - Hardware Fault Tolerance and SFF - Safe Failure Fraction

Depending on the SIL for the safety system, the IEC 61508 standard requires a specific hardware fault tolerance HFT in connection with a specific proportion of safe failures SFF (Safe Failure Fraction).

The hardware fault tolerance is the ability of a system to execute the required safety function in spite of the presence of one or more hardware faults.

The SFF of a system is defined as the ratio of the rate of safe failures and dangerous detected failures to the total failure rate of the system.

$$SFF = (\Sigma\lambda_s + \Sigma\lambda_{Dd}) / (\Sigma\lambda_s + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$$

$\Sigma\lambda_s$: Safe failures

$\Sigma\lambda_{Dd}$: Dangerous detected failures

$\Sigma\lambda_{Du}$: Dangerous undetected failures

According to IEC 61508, the maximum achievable SIL of a system is partly determined by the hardware fault tolerance HFT and the safe failure fraction SFF of the system.

IEC 61508 distinguishes two types of subsystem (type A subsystem, type B subsystem).

These types are specified on the basis of criteria which the standard defines for the safety-relevant components.

SFF	HFT type A subsystem			HFT type B subsystem		
	0	1	2	0	1	2
< 60%	SIL1	SIL2	SIL3	—	SIL1	SIL2
60%...< 90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90%...< 99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

PFD - Probability of Failure on Demand

The standard IEC 61508 defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL.

The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. To achieve a given SIL, the device must meet targets for the maximum probability of dangerous failure and a minimum Safe Failure Fraction. The concept of 'dangerous failure' must be rigorously defined for the system in question, normally in the form of requirement constraints whose integrity is verified throughout system development. The actual targets required vary depending on the likelihood of a demand, the complexity of the device(s), and types of redundancy used.

The PFD (Probability of Failure on Demand) and RRF (Risk Reduction Factor) of low demand operation for different SILs are defined in IEC 61508 are as follows:

SIL	PFD	PFH (power of ten	RRF
1	0.1 - 0.01	10 ⁻¹ - 10 ⁻²	10 - 100
2	0.01 - 0.001	10 ⁻² - 10 ⁻³	100 - 1000
3	0.001 - 0.0001	10 ⁻³ - 10 ⁻⁴	1000 - 10,000
4	0.0001 - 0.00001	10 ⁻⁴ - 10 ⁻⁵	10,000 - 100,000

In high demand or continuous operation, these changes to the following:

SIL	PFH	PFH (power of ten	RRF
1	0.00001 - 0.000001	10 ⁻⁵ - 10 ⁻⁶	100,000 - 1,000,000
2	0.000001 - 0.0000001	10 ⁻⁶ - 10 ⁻⁷	1,000,000 - 10,000,000
3	0.0000001 - 0.00000001	10 ⁻⁷ - 10 ⁻⁸	10,000,000 - 100,000,000
4	0.00000001 - 0.000000001	10 ⁻⁸ - 10 ⁻⁹	100,000,000 - 1,000,000,000

The hazards of a control system must be identified then analyzed in a risk analysis. These risks are gradually mitigated until their overall contribution to the hazard is deemed to be acceptable. The tolerable level of these risks is specified as a safety requirement in the form of a target probability of a dangerous failure over a given period, stated as a discrete SIL level.

Fault Avoidance Measures

Systematic errors in the specifications, in the hardware and the software, usage faults and maintenance faults in the safety system must be avoided to the maximum degree possible. To meet these requirements, IEC 61508 specifies a number of measures for fault avoidance that must be implemented depending on the required SIL. These measures for fault avoidance must cover the entire life cycle of the safety system, i.e. from design to decommissioning of the system.

Safety Function Capability

PDS (SR) Safety Functions are Part of an Overall System

If the qualitative and quantitative safety objectives determined by the final application require some adjustments to ensure safe use of the safety functions, the integrator of the BDM (Basic Drive Module) is responsible for these additional changes (for example, managing the mechanical brake on the motor).

Also, the output data generated by the use of safety functions (fault relay activation, error codes, or information on the display, and so on) is not considered to be safety-related data.

SIL and PL Table for the Safety Functions

The following table provides the SIL and PL details for the safety functions of the CIP safety module:

Safety Function	Safety integrity level (SIL)	Performance Level (PL)
STO	SIL3	PL e

Note: Verify that all the components used in the application that have different SIL Level (mix Level) reach the intended level for the Overall Application by performing comprehensive tests for all operating states, the defined safe state, and all potential error situations.

Summary of the Reliability Study

The following table provides the SIL and PL details for the safety functions of the CIP safety module:

Safety Function	Standard	Attribute	Value
STO	IEC 61508 Ed.2	SFF	>90%
		PFD20y	$4,8 \cdot 10^{-05}$
		PFHequ_1y	$3,1 \cdot 10^{-10}$
		Type	B
		HFT	1
		DC	>90%
	ISO 13849-1	Category	3
	MTTFd in years	>100	

Technical Data

What's in This Part

Installation of the CIP Safety Drive.....	27
Installation Topology.....	29

Installation of the CIP Safety Drive

Before You Begin

Before you install the module, ensure that the

- Catalog number given on the label of the module is the same as that on the delivery note corresponding to the purchase order
- CIP safety module is not damaged
- Additional module support (VW3A3800) is available.
- Ethernet cable for the CIP safety module is available.
- Software version of the drive is compatible with the CIP safety module.
- The drive software version compatible with CIP Safety is the **V2.1IE82**.
- Both the drive configuration (see ATV900 Programming manual, page 12) and CIP Safety module configuration (see Reset safety configuration of the safety drive, page 80) must be reset to clear any previous configuration.

Mechanical data

Weight:

- CIP safety module VW3A3809: 0.02 kg (0.044 lb)
- Additional Module Support VW3A3800: 0.4 kg (0.89 lb)

Dimensions:

- CIP safety module VW3A3809: 41 x 109 x 23.25 mm (1.61 x 4.29 x 0.91 in)
- Additional Module Support VW3A3800: 128 x 147 x 65 mm (5.04 x 5.79 x 2.56 in)
- The use of an additional module support increases the depth values of the drive by maximum of 50.5 mm (1.97 in) depending on the catalog number of the drive. The additional module support takes place between the Graphic Display Terminal and the drive, causing the depth value to be increased.

Ambient Conditions

The ambient conditions to be met for the CIP safety module correspond to the ambient conditions for the drive, see the installation manual, page 12 of the drive.

▲ WARNING

LOSS OF SAFETY FUNCTION CAUSED BY FOREIGN OBJECTS

Conductive foreign objects, dust or liquids may cause safety functions to become inoperative.

- Do not use a safety function unless you have protected the system against contamination by conductive substances.

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

Installation of the Additional module support (VW3A3800)

Refer to the Additional module support Instruction Sheet (NHA80733) to install the Additional module support on the drive.

Installation or removal of the CIP Safety Module (VW3A3809)

The CIP Safety Module (VW3A3809) can only be recognized on the slot proposed by the additional module support. Install the additional module support before installing the CIP safety module.

Refer to the CIP Safety Module Instruction Sheet (JYT89145) to install or remove the CIP safety module from the drive.

Degree of protection

The safety drive must be installed in a control cabinet with degree of protection IP54 (or higher). This is required to avoid cross faults and short circuits between terminals, connectors, tracks and safety-related circuitry caused by foreign objects.

Installation Topology

The safety system is composed of a Safety Drive (drive ATV9●● + CIP Safety module VW3A3809) and a safety controller (M580 PLC). For more details about the M580 controller, refer to Modicon M580 Safety Manual.

The different components of the system can be connected as shown in the following architecture:

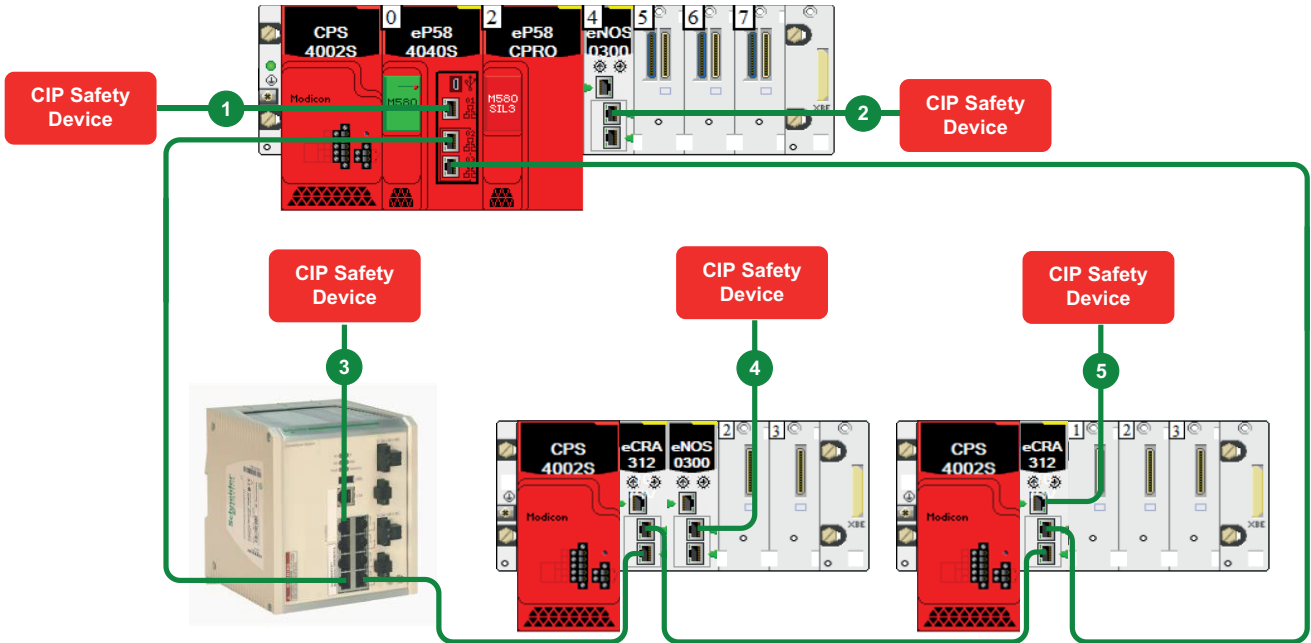


Figure : Design – CIP Safety Devices architecture

- 1 On the service port of the CPU
- 2 On a BMENOS module in the main rack
- 3 On a Connexium DRS switch
- 4 On a BMENOS module in a drop
- 5 On the service port of a BMECRA

CPU service port: Standalone M580 Safety CPUs support CIP Safety devices in DIO clouds. No CIP Safety device currently supports RSTP, so CIP Safety devices cannot be attached to the Ethernet ports under the service port of the CPU. They can only be attached to the CPU service port.

BMENOS0300: When the BMENOS0300 is configured in "Access - DIO Ports" mode. Again, with no support for the RSTP protocol, do not attach CIP Safety devices in a ring from a BMENOS0300. Only daisy-chaining is possible.

BM•CRA312•0 service port: Use the service port of the eX80 Ethernet I/O adapter module in an ERIO drop to attach CIP safety devices.

Ethernet switch: Do not connect CIP Safety devices in a ring from an Ethernet switch. Only daisy-chaining is possible.

Note: refer to the Modicon M580 Safety System Planning Guide for the recommended limitations of number of CIP safety drives to connect in a M580 safety controller architecture.

After installing the safety system, the CIP Safety module must be unplugged before performing wiring tests.

Verify that the safety drive firmware version is compliant with CIP safety module (V2.1IE82), otherwise the module is ignored and a firmware update is required.

The firmware update can only be done by Schneider Electric Services. For more information contact your local Schneider Electric Services.

Safety Function STO (Safe Torque Off)

What's in This Part

Overview	31
Limitations	32
CIP Safety objects	33
Display	40
Dedicated Safety Function menu in the Display Terminal	41

Overview

STO is a Safe Torque Off defined by IEC 61800-5-2.

The Safe Torque Off (STO) function is the standard function embedded to the drive. Refer to the Embedded Safety Function manual of the drive for further information.

The CIP safety module is an option module of the drive. If the CIP safety module is inserted then the safety function STO cannot be activated with the STO inputs of the drive (**STO \bar{A}** and **STO \bar{B}**). In this case, the STO inputs of the drive (**STO \bar{A}** and **STO \bar{B}**) must be short-circuited to 24V. Otherwise, a **SIOF** is triggered by the CIP safety module when safe torque off is requested via the CIP safety assembly.

STO with the CIP safety module

STO is activated by default.

It can only be deactivated by enabling a CIP Safety Safe Torque Off command through the CIP Safety assembly.

For more information refer to Operation with CIP Safety configuration, page 63.

Safety Profile

The communication specifications are shown in the following table:

Safety Drive I/O	Number of concurrent connection: 3
CIP I/O	1 connection
CIP Safety I/O	1 connection Safety Input 1 connection Safety Output
Safety open type	Type 2a, Type 2b
Conformity Test	CT 18-ES
Safety Level	Safety Torque Off (STO) SIL3/PL e

TCP and UDP Protocol Connections

The Ethernet adapter supports up to 32 concurrent TCP/IP and/or TCP/UDP connection.

Limitations

Prerequisites for Using STO Safety Function

Following conditions have to be fulfilled for correct operation with the CIP safety module:

- The motor size is adequate for the application and is not at the limit of its capacity.
- The drive has been correctly chosen for the line supply, sequence, motor, and application and is not at the limit of their capacities as stated in the catalog.
- If required, the appropriate options are used.

Disable Error Detection

The errors linked to the CIP safety module (**SIOF**, **SAVF**, **SCFF**) cannot be inhibited by the function **[Error Detection Disable] INH-**. For more information, refer to *Detected Errors*, page 68.

Configuration transfer to Safety drive

A drive configuration with firmware version different than CIP safety firmware (**V2.1IE82**) is not compatible for a transfer to a safety drive, otherwise a **[Conf Transfer Error] CF12** will be triggered.

CIP Safety objects

What's in This Chapter

Introduction.....	34
Object map	34

Introduction

In addition to the objects supported by EtherNet/IP, the following objects are added for CIP Safety.

These objects are accessed with Explicit message communication.

Instance No.	Class ID	Object name
1	39h	Safety Supervisor Object
2	3Ah	Safety Validator Object
1	300h	CIP Safety Module Object

Object map

The following section describes objects added for CIP Safety in addition to those supported by EtherNet/IP.

For details of objects supported by EtherNet/IP, refer to the ATV900 embedded Ethernet manual, page 12.

Note: The instance attribute 16: DN error mode of the Control Supervisor Object (29 hex) is not available for the CIP safety drive.

Safety Supervisor Object (39h)

Supported Class Attributes

Number	Access	Name	Description
1	Get	Revision	Revision of the Object

Supported Instance attribute

ID	Access	Name	Type	Value	Description
11	Get	Device Status	USINT	-	Represents the current state of the device. 1: Self-testing 2: Idle 3: Self-test exception 4: Executing 5: Abort 6: Critical Fault 7: Configuring 8: Waiting for TUNID
12	Get	Exception Status	BYTE	Fixed to 0.	Device diagnosis data
15	Set	Alarm Enable	BOOL	-	
16	Set	Warning Enable	BOOL	-	

ID	Access	Name	Type	Value	Description
25	Get	Configuration UNID	10 Octets	All fixed to 0xFF.	The owner of the device setting is identified. 0: Not set. All owners are accepted. 0xFF: Fixed value for STO only.
26	Get	Safety Configuration Identifier	10 Octets	-	The SCID is read.
27	Get	Target TUNID	10 Octets	-	The TUNID is read.
28	Get	Output Connection Point	10 Octets	-	UNID of the owner of the output resource. 0: Not owned. The owner is accepted
29	Get	Proposed TUNID	10 Octets	-	The UNID value that an Originator/tool is attempting to set in the device

Supported Services by the object

Service Code	Service Name	Description
0E Hex	Get_Attribute_Single	Read both class and Instance.
10 hex	Set_Attribute_Single	Write instance attribute. It allows to set the Alarm Enable and Warning Enable attributes.
54 hex	Safety_Reset Type 0	Type 0: power cycle.
	Safety_Reset Type 1	Type 1: Reset configuration and restart the safety drive.
56 hex	Propose_TUNID	Initialization of the TUNID setting. The safety drive is in SSO-Waiting for TUNID state.
57 hex	Apply_TUNID	Setting of the TUNID. The safety drive is in SSO-Idle state.

Safety Validator Object (3Ah)

Supported Class attribute

Number	Access	Name	Description
1	Get	Revision	Revision of the Object
8	Get	Safety Connection fault Count	Diagnostic counter of CIP Safety connection errors

Supported Instance attribute

ID	Access	Name	Type	Description
1	Get	Safety Validator state	USINT	Represents the state of CIP safety connection. 0: Unallocated 1: Initializing 2: Established 3: Connection unsuccessful
2	Get	Safety Validator Type	1 Octet	Present safety connection type Bit 7 <ul style="list-style-type: none"> 0: Producer (Safety Input) 1: Consumer (Safety Output) Bit 0 to 6 <ul style="list-style-type: none"> 0: Not connected 1: Single cast 2: Multicast 3-127: Reserved
3	Get	Ping Interval EPI Multiplier	UNIT	Number of Ping Count interval for a particular connection.
4	Get	Time Coord Msg Min Multiplier	UNIT	Minimum multiplier for the time coordination message.
5	Get	Network Time Expectation Multiplier	UNIT	Network time expectation multiplier.
6	Get	Timeout Multiplier	UNIT	Possible values: 1-4
7	Get	Max Consumer Number	UNIT	Number of consumer (Safety Output) 1: Single cast
12	Set	Max data age	UNIT	The data age of received packet data is defined as the difference between the consumer's clock and received Time Stamp at the time the packet is received.
13	Get	Application Data Path	EPATH	Safety data path for connection.
15	Get	Producer/ Consumer Fault Counters	UNIT	Number of errors detected.

Supported Services by the object

Service Code	Service Name	Description
4B hex	Reset all error counters	Used to reset the class attribute 8 (Safety Connection Fault Count) in all instances.
0E hex	Get_Attribute_Single	Read both class and Instance.
10 hex	Set_Attribute_Single	Write instance attribute. It allows to reset the MAX Data Age instance.

Safety Module Object (300h)**Supported Class attribute**

Number	Access	Name	Description
300 hex	Get	Vendor Specific	-

Supported Instance attribute

ID	Access	Name	Type	Description
1	Get	State SM	USINT	CIP Safety module state. More details in [Safety Module Status] SSTA parameter , page 41.
2	Get	SM Configuration State	USINT	CIP Safety module configuration state. More details in [Safety Config Status] SNCA , page 41
3	Get	Safety Function Active	USINT	CIP Safety module active function STO. More details in [Active Safety Fct] SFCA , page 42.
4	Get	STO trigger	USINT	Origin of Safe Torque Off activation: 0. [STO is not requested] 1. STO requested by [CIP Safety Controller] 2. Safety error 3. CIP Safety connection closed/lost

ID	Access	Name	Type	Description
5	Get	Safety Error Number		A variable-size structure of current CIP Safety module errors: <ul style="list-style-type: none"> • 2 bytes for each error code. • The latest error code shall be the first one.
6	Get	INTERNAL_FAULT	BOOL	Error Group: Internal Error 0: no error 1: error detected
7	Get	SAFETY_VIOLATION	BOOL	Error Group: Safety Violation 0: no error 1: error detected
8	Get	SAFETY_CONFIG	BOOL	Error Group: Safety Configuration 0: no error 1: error detected
9	Get	IO_FAULT	BOOL	Error Group: I/O error 0: no error 1: error detected

Supported Services by the object

Service Code	Service Name	Description
0E hex	Get_Attribute_Single	Read both class and Instance.
10 hex	Set_Attribute_Single	Write instance attribute.

Assembly Object (04 hex)

In addition to the Ethernet IP supported assemblies of the Assembly object (04 hex), Safety Output assembly (300hex) and Safety Input assembly (301hex) have been added for CIP Safety.

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.

Safety Output Data with STO assembly (300h)

Member List	Bit position	Description
Safe Torque Off	0	0: Disable Torque 1: Permit Torque Enables or disables energy to the motor which can generate torque.
Reserved	1–6	–
Safety Reset	7	Transition 0->1: To recover from a safety fault after the cause is corrected.

Safety Output Data with STO assembly (301h)

Member List	Bit position	Description
Torque Disabled	0	0: Torque permitted 1: Torque disabled
Reserved	1–5	–
Safety fault	6	0: No fault 1: Safety fault present
Restart required	7	0: Restart not required 1: Reset required to restart

Null instance assembly for Time coordination (c5h)

This assembly indicates the null connection point for the Time Coordination connection.

Instance ID	Name of assembly	Size of assembly in byte	Description
c5 hex	Null Connection point	0	Null Connection point shall reference the Time Coordination connection.

Identity Object (01 hex)

This object is supported by the standard Ethernet IP.

The safety drive only supports the instance service Reset (05h) when there is no established I/O connection, whether it is safety or standard.

Display

LED Indicator

The following table shows the behavior of the LED indicators when the CIP safety module is plugged:

LED	Color & status	Description
NS (Network Status)	Off	The device does not have an IP address or powered off.
	Green/Red flashing (250/250 ms pattern)	Proposed TUNID received but not yet applied.
	Green on	IP address is assigned and at least one connection has been established to control the command word (CIP safety, Modbus TCP or Ethernet IP) is established.
	Green flashing	Device has a valid IP, but no IO connection (CIP safety, Modbus TCP or Ethernet IP).
	Red flashing	Time-out on Modbus TCP or Ethernet IP or Output CIP safety connections.
	Red on	Duplicated IP.
MS (Module Status)	Off	No power is supplied to the device.
	Flashing red/green	The device is performing a self-diagnosis function, or Safety drive is not yet configured due to incomplete configuration (e.g. TUNID missing).
	Flashing Red	<ul style="list-style-type: none"> Safety drive has detected a recoverable error. Self test has not been successful. Safety drive is in SSO-Abort state.
	Red On	The device has detected a non-recoverable error.
	Flashing Green	The device has been configured and ready to establish CIP safety connection
	Green On	The device is operating correctly (CIP Safety connection established).
ASF	Solid Yellow	Indicates that the STO safety function is activated

NOTE:

Communication status LEDs are used only to check the status for test operation and during troubleshooting.

Do not use them as operation indicators. Communication status LEDs are not provided as included in the safety system.

Communication status LEDs may not be always correct.

Dedicated Safety Function menu in the Display Terminal

Overview

If the CIP safety module is inserted, the dedicated menu **[Safety Module] oSM-** accessible via the Display Terminal is displayed. The menu access is:

[Complete settings] → [Safety Module]

This menu allows you to:

- Visualize the real-time status of the safety module, the STO safety function, the CIP safety Network and Safety inputs/outputs assembly value.
- Read the current CIP safety module errors.

[Safety Module Status] SSTA

CIP safety module status. This is a read-only parameter.

The CIP safety module status is different from the drive status.

Setting	Code / Value	Description
[Starting]	STRT	Initialization ongoing but not completed.
[Not Rdy to Switch On]	NRSO	CIP Safety module initialization is completed.
[Switch On Disabled]	SOD	Safety module and drive initialization are completed but CIP safety controller has not opened the CIP Safety connection with the Safety drive.
[Ready to Switch On]	RTSO	Configuration of CIP safety module is completed.
[Operation Enabled]	OPEN	CIP Safety drive is in operational mode. STO is deactivated.
[Fault]	FLT	Safety error triggered.
[STO Active]	STO	Safety function STO is active.

[Safety Config Status] SCNA

Safety configuration status. This is a read-only parameter.

Setting	Code / Value	Description
[No Configuration]	NCNF	CIP Safety module has been plugged for the first time or the safety configuration has been reset.
[Configured Un-owned]	COUW	The safety drive is configured, but has never been connected to the Safety controller.
[Configured Owned]	COW	The safety drive is configured, and has already been connected to the Safety controller.

[Active Safety Fct] SFCA

Active safety function. This is a read-only parameter.

It shows the activation state of the STO function.

Setting	Code / Value	Description
[None]	None	No safety function is active.
[STO]	STO	Safety function STO is active.

[Safety Config Reset] SFRS

Reset of the safety configuration. It resets only the parameters related to the CIP safety module.

This parameter can be accessed if **[Access Level] LAC** is set to **[Expert] EPR**.

When activating this parameter, the safety drive performs a restart, which can clear a triggered error that is no longer relevant.

Setting	Code / Value	Description
[No]	NO	Not active.
[Yes]	YES	Request to reset the safety configuration. Note: This setting is possible only if the CIP SAFETY communication is not in executing state.

[Safety Module Errors] SME – menu

This menu contains additional information about the current detected errors related to the CIP safety module by.

- **[Safety Module Error] SMLE**, and/or
- **[Safety Module Error 0] SME0** to **[Safety Module Error 9] SME9**.

It corresponds to current errors triggered by CIP safety module. When **SME_x** is different than 0, the **[Safety Module Status]** is set to **[Fault] FLT**.

The list of error codes is available in the section [Detected Error](#), page 68.

[Sfty Supervisor Object] SSM0

This parameter represents the **[Safety Drive] sso** current state. This is a read-only parameter.

This parameter is only used to verify the status for test operation. **Do not use this parameter as operation indicator.**

The different safety drive states are:

Code / Value	Description
SSO-Self Testing	The safety drive performs a self-test during power up.
SSO-IDLE	No CIP Safety connection established between safety drive and safety controller.
SSO-Executing	Safety drive is operational. No error detected.
SSO-Abort	Major resettable error detected.

Code / Value	Description
SSO-init	The CIP Safety module is inserted but no IP address has been set in the safety drive.
SSO-Critical Fault	Non-resettable error detected.
SSO-Configuring	Configuring in progress.
SSO-Waiting For TUNID	Waiting for the set of the TUNID.

[Safety Com Map] SCM- menu

[Cmd Word x-x] scw_x:

[Cmd Word 1-0] scw₀ to [Cmd Word 13-12] scw₆.

Read-only parameter.

It defines the safety command word exchanged between PLC and the safety Drive.

NOTE: As the only available safety function is STO, the command word is stored in [Cmd Word 1-0] scw₀.

[Status Word x-x] ssw_x:

[Status Word 1-0] ssw₀ to [Status Word 13-12] ssw₆.

Read-only parameter.

It defines the safety status word exchanged between PLC and the safety Drive.

NOTE: As the only available safety function is STO, the command word is stored in [Status Word 1-0] ssw₀.

Commissioning and Display

What's in This Part

Configuration of the safety system	45
Acceptance Test.....	60

Configuration of the safety system

What's in This Chapter

Prerequisites to Configure the Safety drive46
 Configuration with the commissioning software.....46

Overview

To configure the safety drive, follow the following steps:

Step	With/ Without CIP Safety Module inserted	Action
1	Without	Configure the Drive Motor Control using SoMove or Graphic Display Terminal - including IP settings NOTE: The IP address of the safety drive should be configured with [IP address] I00 (path: [Communication] → [Comm parameters] → [Embd Eth Config]) For more information, refer to ATV900 Programming manual, page 12.
2	Without	Test Drive Motor control using with SoMove / Graphic Display Terminal.
3	—	Power off and insert CIP safety module.
4	With	Configure CIP Safety system using EcoStruxure Control Expert.
5	With	Test CIP Safety system.

Prerequisites to Configure the Safety drive

The drive firmware version to support the CIP safety module is **V2.11E82**.

After installing and plugging the CIP safety module in the drive, verify the drive firmware on the display terminal via **[Diagnostics] → [Diag. data] → [Identification]**.

When the drive has a firmware version that does not support CIP safety module, the CIP safety module is ignored and a firmware update is required.

The firmware update can only be done by Schneider Electric Services. For more information contact your local Schneider Electric Services.

Before starting to configure the parameters of the CIP safety module, configure the standard parameters of the drive.

This part can be configured using the Schneider_Electric_Altivar_Process_ATV9xx_DTM_Library_V3.8 compatible with the safety drive. For more details about parameters, refer to ATV900 Programming manual, page 12.

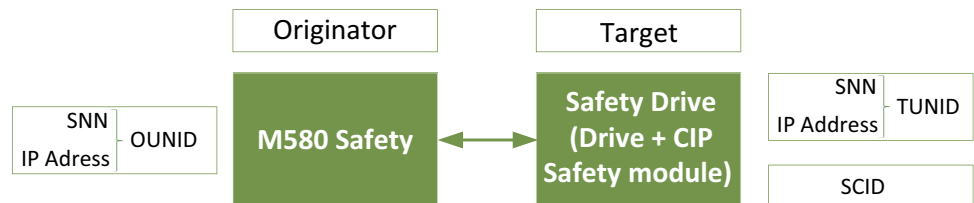
Use the links below to download these files:

Files	Links
SoMove: FDT	SoMove_FDT (English, French, German, Spanish, Italian, Chinese)
ATV900: DTM	ATV9xx_DTM_Library_EN (English - to be installed first) ATV9xx_DTM_Lang_FR (French) ATV9xx_DTM_Lang_DE (German) ATV9xx_DTM_Lang_SP (Spanish) ATV9xx_DTM_Lang_IT (Italian) ATV9xx_DTM_Lang_CN (Chinese)

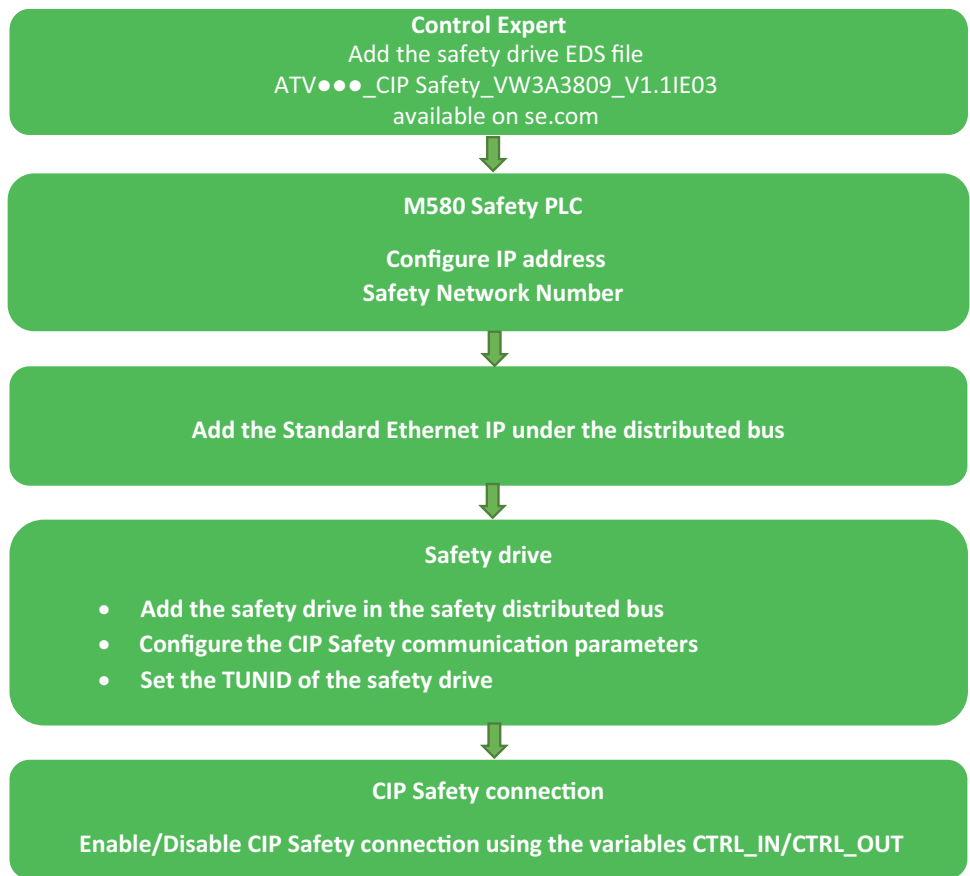
To configure the safety drive, it is necessary to download the EDS file ATV900_CIP_Safety_EDS_VW3A3809_V1.11E03 from se.com.

Configuration with the commissioning software

After plugging the CIP Safety module, the configuration of some parameters is required to establish CIP Safety communications between the M580 Safety PLC and the Safety drive.



The configuration is done via the M580 Safety engineering tool: EcoStruxure Control Expert.

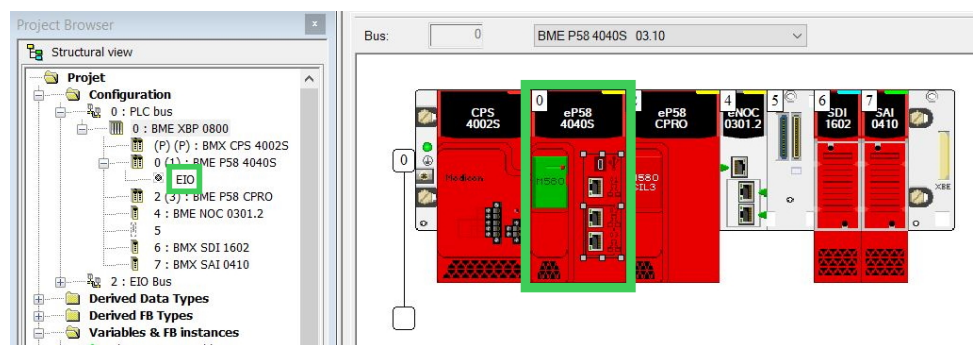


The following table presents more details about the originator and target identification parameters:

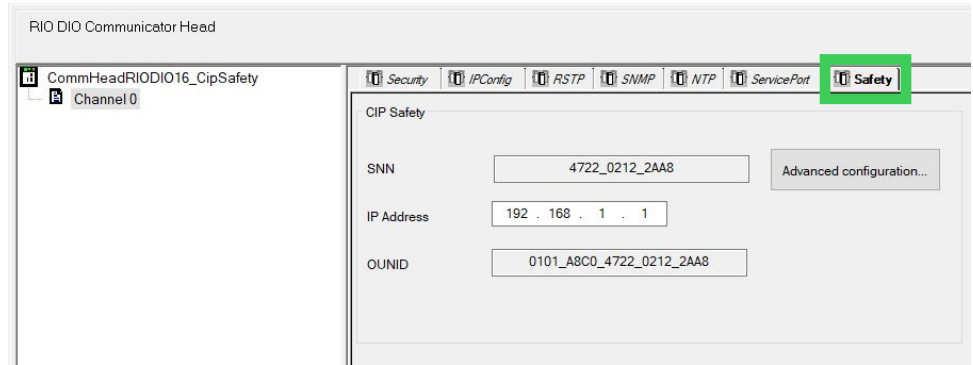
Parameter	Description
SNN	The unique SNN (Safety Network Number). It identifies a logical Network that includes an Originator (M580 Safety controller) and Targets (one or many Safety drives).
OUNID	Originator Unique Network ID. It is composed from the SNN and IP Address of the Originator (Safety controller).
TUNID	Target Unique Network ID. It is composed from the SNN and IP Address of the Target (safety drive).
SCID	Safety Configuration Identifier, page 55.

M580 Safety Configuration

After choosing an M580 Safety CPU in the Control Expert, double click on EIO in the Project Browser or the Ethernet interfaces in the Rack View:



After clicking on the EIO in the project browser, go to Safety Tab:

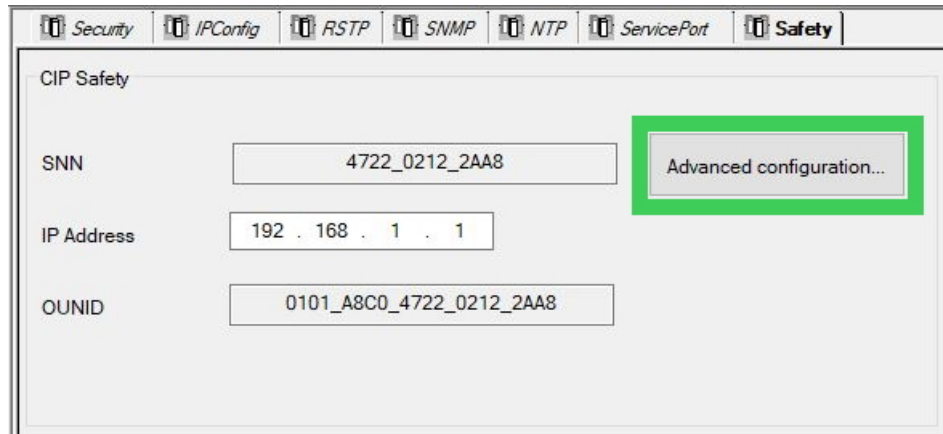


The CIP Safety Originator has a unique OUNID automatically generated when the application is created:

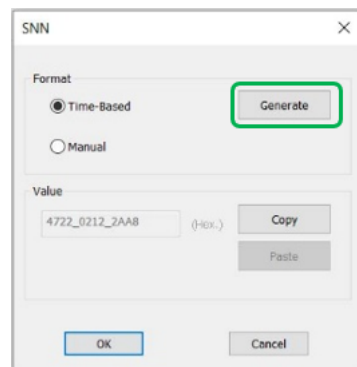
Note: The CIP Safety originator with an automatic SNN setting feature must only use this feature when the safety system is not relied upon.



The SNN can be modified by clicking on Advanced configuration button:



Generate a new one according to the desired format:



The IP address of the M580 Safety is part of the OUNID. Therefore, any modification of the M580 IP address affects the OUNID and requires a Reset Ownership of the CIP Safety devices whom the M580 was the unique possible Originator. Otherwise, the M580 Safety may be unable to open any CIP Safety communications with the new OUNID.

Configuration of the CIP Safety Drive

To verify and confirm that the configuration created using the Control Expert software was correctly downloaded to and saved in the M580 CIP Safety CPU as originator:

- A user-performed visual comparison (after the application download is complete) of the CIP Safety connection configuration parameters displayed in the target DDDT against the same parameters displayed in the target DTM.
- An automatic comparison, performed by the CPU and Copro, of the connection parameter CRC CPCRC calculated by the DTM against the CPCRC calculated by the CIP Safety stack (CSS) running in the CPU and Copro.

For more details, refer to Modicon M580 Safety Manual.

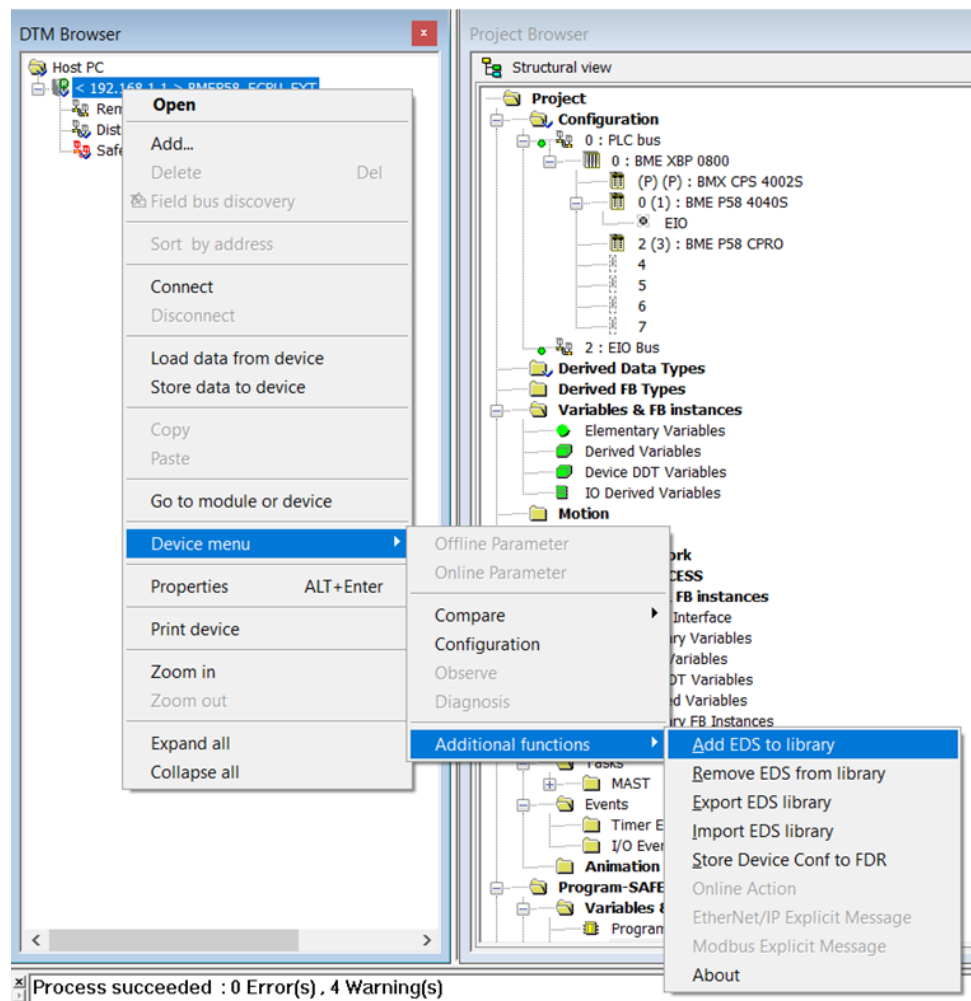
To add a CIP Safety device in the network configuration, set the corresponding Generic Device DTM in EcoStruxure Control Expert.

A specific EDS file `ATV900_CIP_Safety_EDS_VW3A3809_V1.1IE03` allows to generate Vendor DTM safety to configure the safety configuration and a vendor DTM to configure the standard Ethernet IP. This EDS can only be retrieved from `se.com` or distributed from your customer care center.

If the Drive EDS is not available in the DTM Library, add this EDS in the Library.

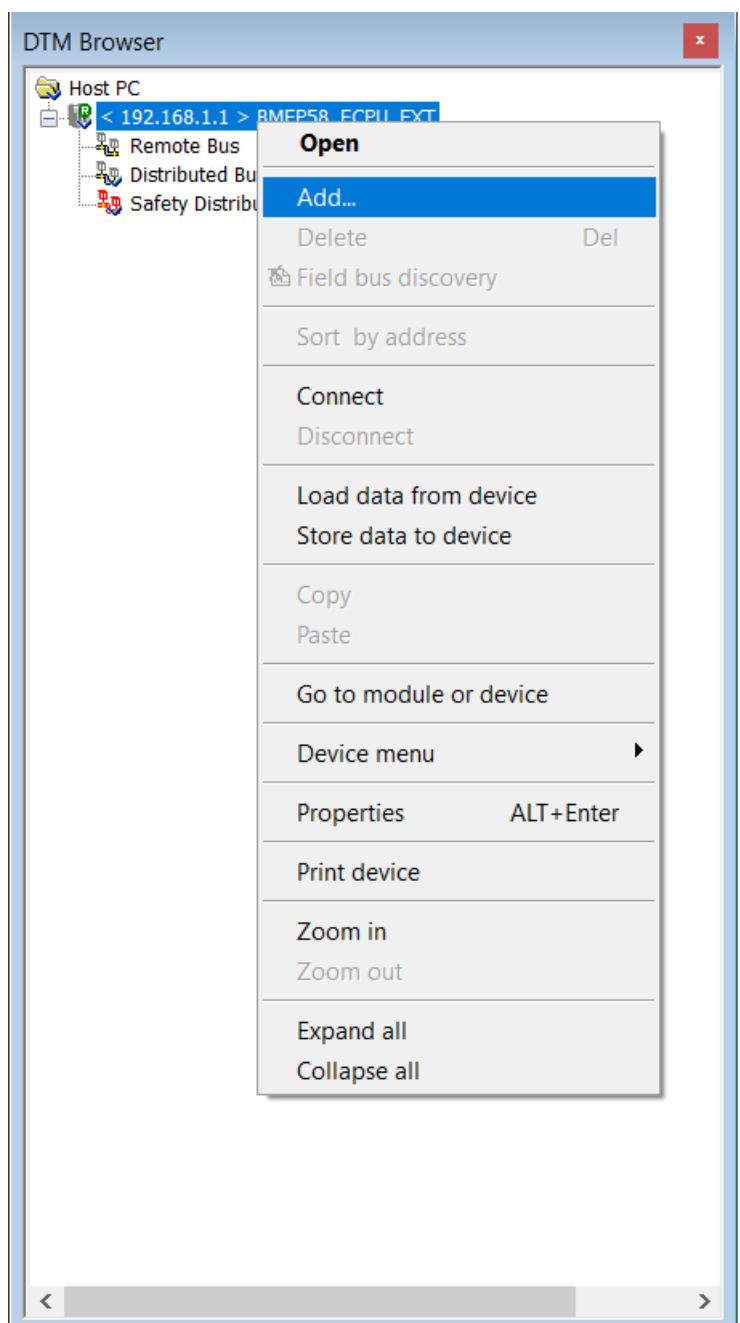
Add EDS to Library:

1. Go to "Device menu"
2. Click on "Additional functions"
3. Click on "Add EDS to Library" and follow the instructions.

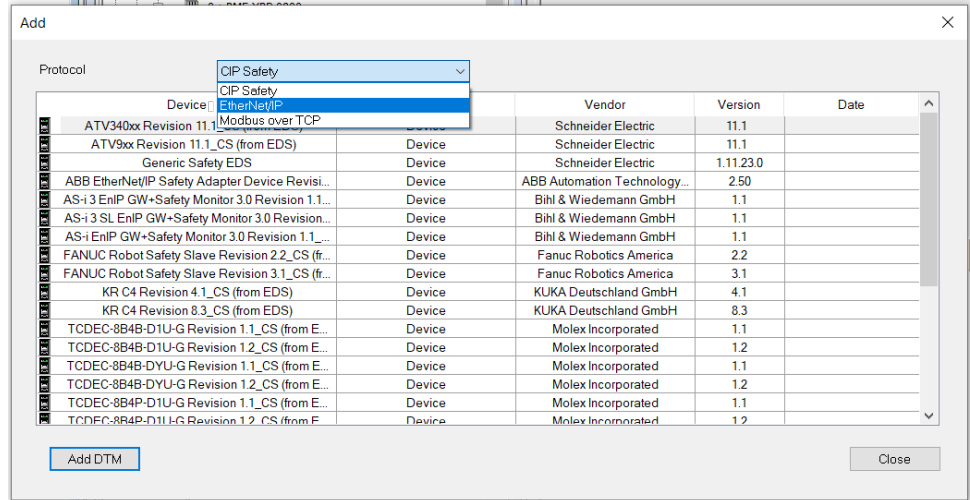


After the EDS file is imported, update the DTM library or restart the Ecostruxure Control Expert.

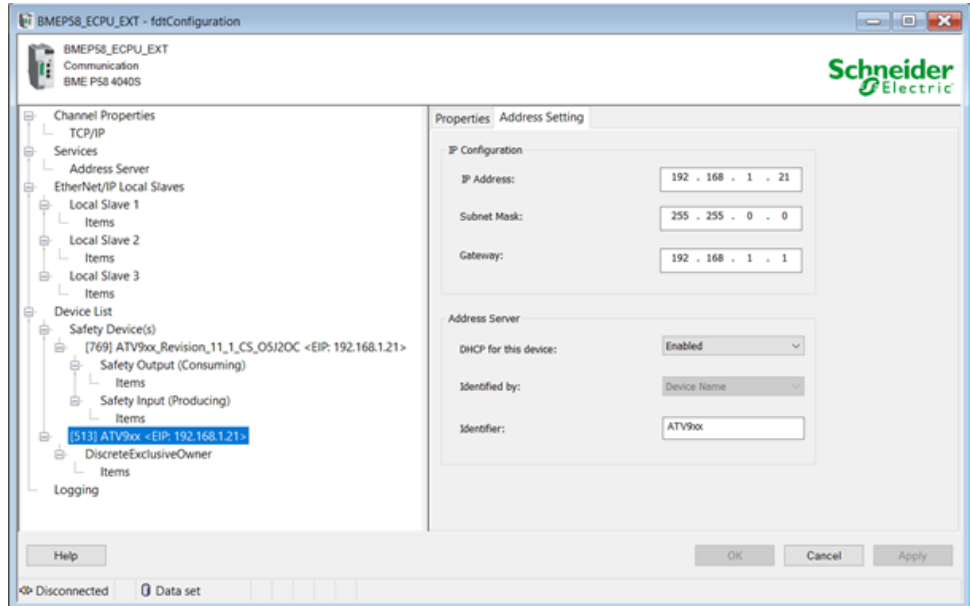
Click on “Add...”:



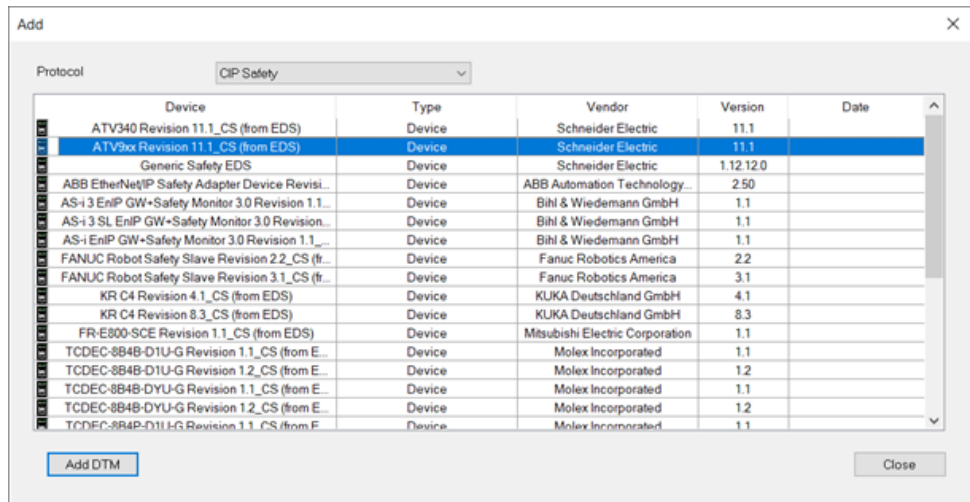
The standard Ethernet IP ATV9xx CIP Safety Revision 11.1 (from EDS) of the safety drive is added by choosing the “Ethernet IP” in the Protocol box list and click “ADD DTM”.



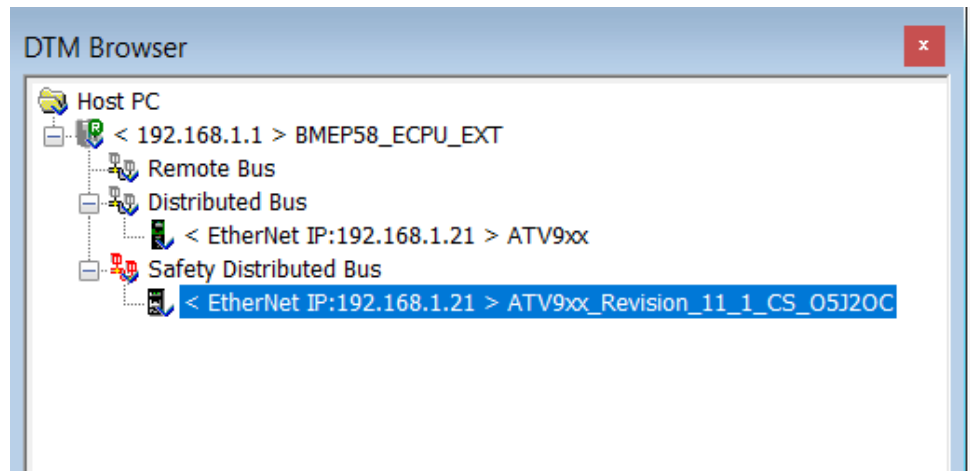
Set the IP address of the safety drive in the same network as the M580 PLC. For more details, refer to ATV900 embedded Ethernet manual, page 12.



To add the CIP Safety part of the safety drive, select the CIP Safety protocol on the box list, select the ATV9xx CIP Safety Revision 11.1_CS (from EDS), and click on “ADD DTM”. The safety drive will appear on the Safety Distributed bus Tab.



The IP address must be modified to match the IP address put in the Ethernet IP and drive.



A pop-up notification appears, indicating that the defined IP address already exists. Confirm the pop-up.

Generate safety drive SNN



In the General Tab, the SNN defines a TUNID (Target Unique Network ID) that is composed in this format: SNN + IP Address. It is generated automatically when the application is created.



If an SNN is assigned manually, the SNN has to be unique. Verify that the assigned SNN for each safety network or safety subnet are unique system-wide and not duplicated.

This SNN can be modified by clicking on the "...":

Safety

Safety Network Number: ...

Note: The format of Safety Network Number is XXXX_YYYY_ZZZZ (hex). XXXX is number of days from 01-Jan-1972, YYYY and ZZZZ is time in ms.

And generating a new SNN according to one of the Format presented:

Safety Network Number

Format

Time-Based Generate
08/02/2022 - 10:12:46 AM

Manual
Ethernet/IP (Decimal) Range: 1 - 999

Vendor Specific

Safety Network Number

SNN: (Hex) Copy

Paste

Set

OK Cancel Help

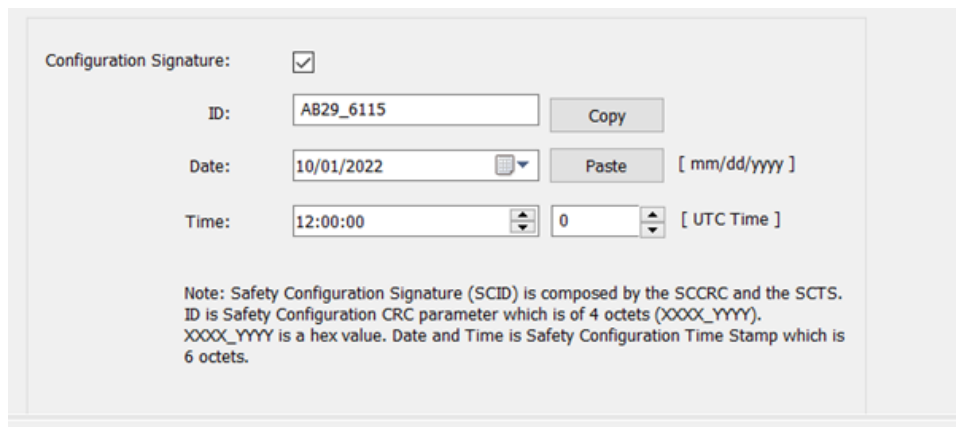
- Time-Based: Generate a hexadecimal value based on the month, day, year, hour, minute, second, and millisecond at the time of generation.
- Manual: Generate a value based on a decimal value from 1 to 9999, which is appended to two hexadecimal values, as follows:
 - word 1: 0004 (fixed)
 - word 2: 0000 (fixed)
 - word 3: 0001...270F (the hexadecimal value of the 1...9999 input value)
- Vendor Specific: The vendor-specific identifier is based on three input hexadecimal words:
 - word 1: 05B5...2DA7 (from vendor)
 - word 2: 0000 (fixed)
 - word 3: 0001...270F (from vendor)
- A directly entered hex value (typed or pasted) consists of:
 - word 1: 2DA8...FFFE
 - words 2 & 3: 0000_0000...0526_5BFF

Configuration Signature (SCID)

The SCID (Safety Configuration Identifier) is unique to the safety system. The use of SCID is a method to improve the communication constancy to sustain a matching correspondence between the M580 Safety PLC and the safety configuration of the Safety Drive.

The SCID is composed by:

- ID is safety configuration CRC parameter.
- Date and Time is safety configuration Time Stamp.



The SCID has a fixed value as shown in the table below:

Parameter	Definition	Value
Configuration date	October 1st 2022	0x4868
Configuration time	12:00:00:000 UTC	0x02932E00
Configuration CRC	-	0xAB296115

Selecting this function is optional. If selected, set the given value and validate by clicking OK.

CIP Safety communications operate only when there is no mismatch between the SCID that is configured and the SCID in the CIP Safety drive.

Request Packet Interval (RPI)

RPI (Requested Packet Interval): This value represents the period at which data updates over a connection. It is defined by the vendor in the EDS file or set by default to:

Safety Input

Default Value	Setting	Description
40ms	20...1000 ms	Setting range. Safety output for connection Target to Originator.

NOTE: RPI Safety Input is defined on ECE as Safety Input = SafeTaskPeriod/ 2 (ms).

Safety Output

Default Value	Setting	Description
20ms	20...1000 ms	Setting range. Safety output for connection Originator to Target.

NOTE: RPI Safety output is defined on ECE as Safety Output= SafeTaskPeriod (ms).

CIP Safety Timeout

Network Time Expectation: Usually called a Timeout, this is one of the most important communication parameters.

By default, the NTE is calculated with this formula:

Network Time Expectation (ms) = 1.5 * Minimum_Network_Time_Expectation (ms)

(with Minimum_Network_Time_Expectation (ms) = RPI (ms) * Timeout_multiplier + Network_Transmission_max (ms)).

⚠ WARNING

LOSS OF CONTROL

Verify that the setting of this parameter is suitable for the application by performing comprehensive commissioning tests for all potential error conditions.

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

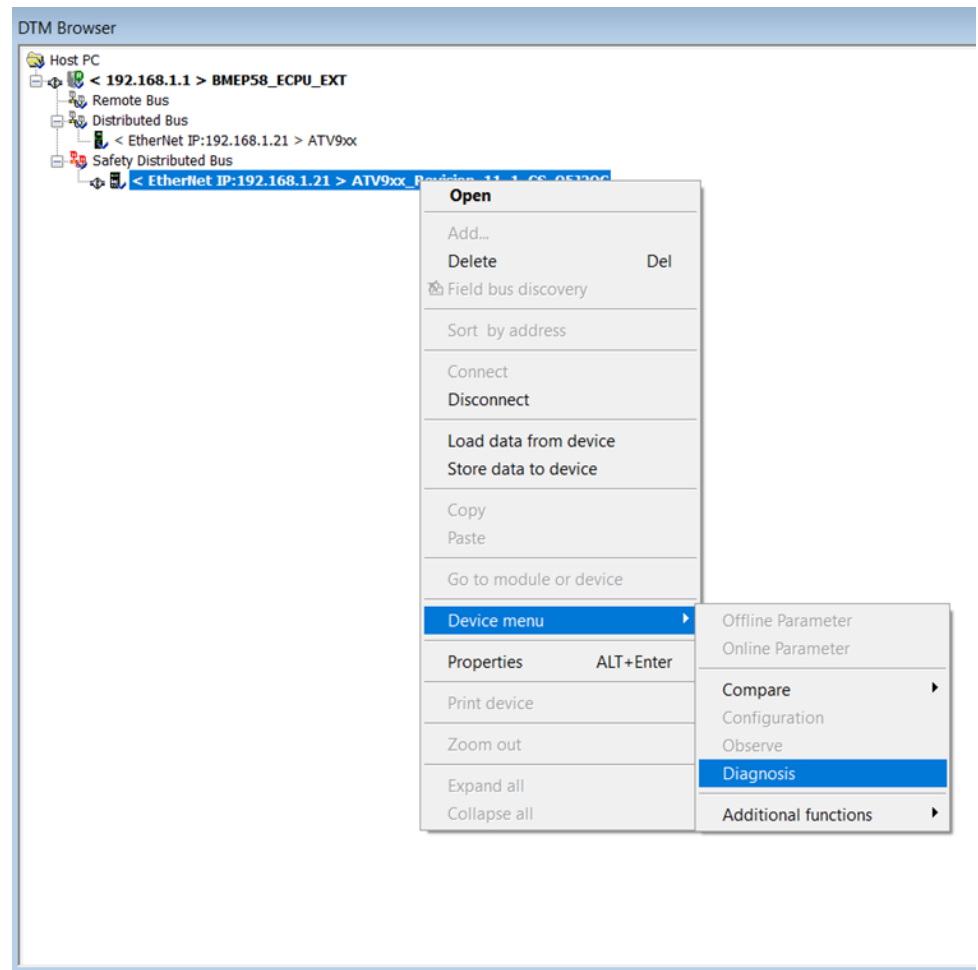
Network Transmission Max: This value is the maximum network communication time between the Safety controller and the CIP Safety drive. Default value = 40 (ms) + Tsafe (ms).

Timeout Multiplier: CIP Safety protocol processing uses the value of the "Timeout_Multiplier" parameter to define the number of messages that can be lost before a connection error is detected and declared.

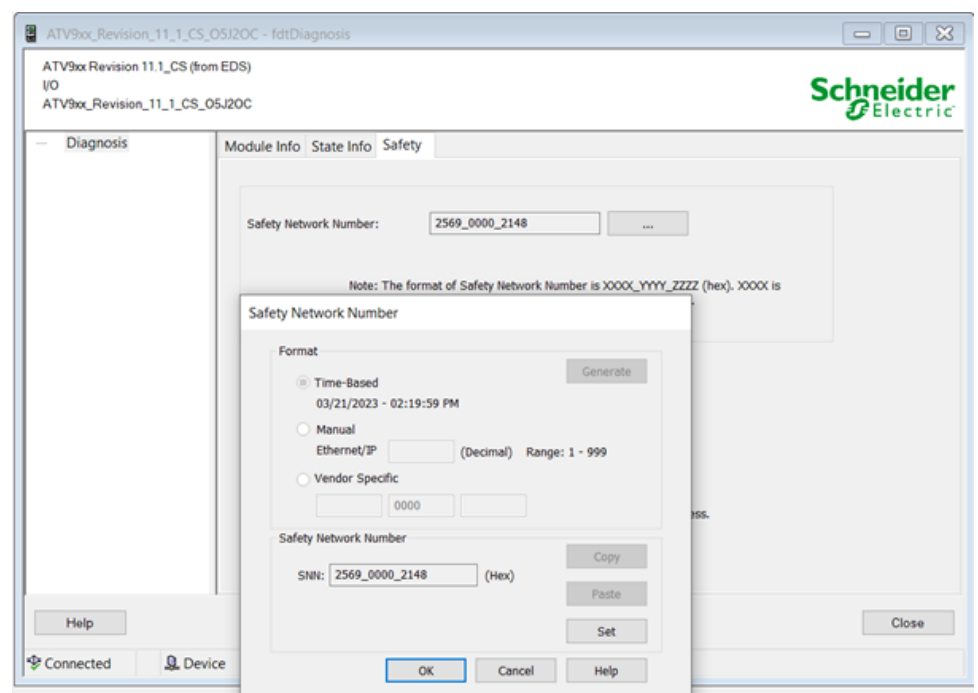
- Timeout Multiplier = 1 :no message can be lost, the Safety controller does not accept frames loss.
- Timeout Multiplier = 2 : one message can be lost, the Safety controller accepts 1 frame loss.
- Timeout Multiplier = 3 : two messages can be lost, the Safety controller accepts 2 frames loss.
- Timeout Multiplier = 4 : three messages can be lost the Safety accepts 3 frames loss.

Set the Safety Network Number

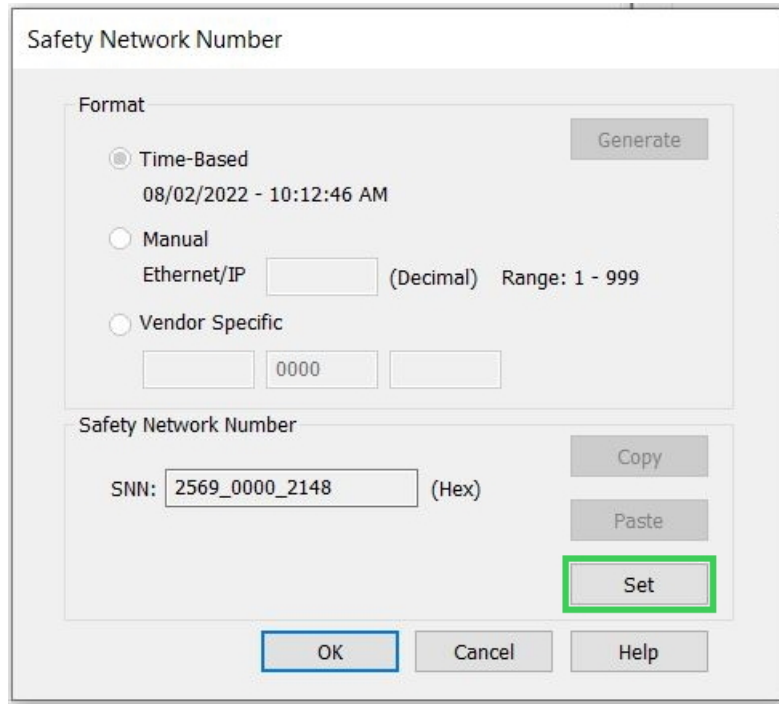
After configuring all parameters for the originator and target, connect the DTM to the safety drive, go to the Diagnosis tab:



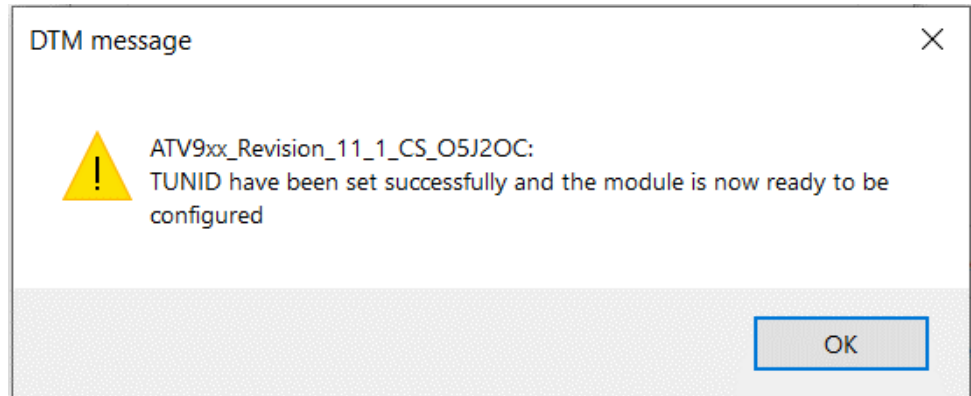
In Safety tab, click on "...":



Click on "Set" to send the TUNID to the safety drive :

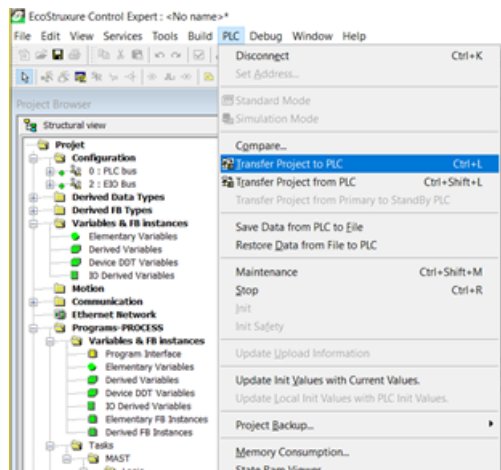


Confirm the following notification pop-up by clicking on OK:



Establishment of the CIP Safety connection

After setting the TUNID, Connect and transfer the project to the PLC, start it in RUN to establish the connection:



When the connection is established, verify in the state info window of the Diagnosis tab the state of the CIP Safety set to executing:

Module Info State Info Safety			
	Parameter	Value	Unit
	▶ CIP Safety State	Executing	
	▶ Exception Status	N/A	
	▶ Major Fault	No Fault	
	▶ Minor Fault	No Fault	
	▶ IP Address	192.168.1.21	
	▶ TUNID (IP,SNN)	192.168.1.21, 2569_0000_2148	
	▶ OUNID (IP,SNN)	192.168.1.1, 4722_0212_2AA8	
	▶ Lock State	###	
	▶ Configuration Signature (ID , TimeStamp)	AB29_6115, 10/01/2022, 12:00:00:000	

Refresh

When the connection is successful, the CIP Safety state is in Executing and both of the OUNID and TUNID have the previously set values. The **[Drive State]** HMI S state is STO by default.

Acceptance Test

Overview

The system integrator/machine manufacturer performs a configuration test of the CIP safety module to verify and document the correct selection of the parameter values. The system integrator/machine manufacturer hereby certifies to have tested the effectiveness of the safety functions used. The configuration test must be performed on the basis of the risk analysis. All applicable standards and regulations must be adhered to.

▲ WARNING

LOSS OF SAFETY FUNCTION

Incorrect usage may cause a hazard due to the loss of the safety function.

- Verify that the engineering prerequisites still apply.
- Carefully perform each individual step.
- Document each individual step.

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

The purpose of the test is to verify proper configuration of the defined safety functions and test mechanisms and to examine the response of dedicated monitoring functions to explicit input of values outside the tolerance limits.

The test must cover all drive-specific Safety configured monitoring functions and global Safety functionality of the drive with the safety module.

A configuration test of the safety module must be performed at the following points in time:

- After the configuration for each machine,
- After changes to parameter values,
- After changes to the machine (as per applicable standards and regulations).

Condition Prior to Acceptance Test

- The machine is wired up correctly.
- All safety-related devices such as protective door monitoring devices, light barriers, and emergency stop switches are connected and ready for operation.
- All motor parameters and command parameters must be correctly set on the drive.
- The connection has been established between the safety controller and the safety drive.

Acceptance Test Process

Verify the effectiveness of all safety functions used.

Document each individual step of the test.

Do not release the system unless the system has successfully passed all individual steps of the test.

The following steps can be executed for the system test:

Communication test: by verifying the Inputs and outputs of the safety controller to confirm that the communication is properly established.

Application test:

- Verify that the STO is active and the CIP Input. TorqueDisabled is set to 1.
- Deactivate STO and verify that the CIP Input. TorqueDisabled is set to 0 and the safety drive state is in RDY/NST..
- Start the motor. Verify that the CIP Input. TorqueDisabled is set to 0 and the safety drive state is in RUN (running).
- Activate STO function. Verify that the CIP Input. TorqueDisabled is set to 1 and the safety drive is in STO state.

Safety validation of the application test: Consists on validating the application following the Safety Test Procedure defined by the system integrator/machine manufacturer.

Operating and maintenance

What's in This Part

Operation with CIP Safety configuration	63
Reset Ownership	65

Operation with CIP Safety configuration

After configuring the Safety drive, the drive displays a STO state, and the CIP Safety state (SSO) is in Idle.

The safety drive is in STO state by default. To deactivate the STO and allow the torque to run the motor, a safety controller must be connected and configured to open the connection between the Originator (safety controller) and Target (safety drive).

⚠ WARNING

UNANTICIPATED EQUIPMENT OPERATION

Verify that having a control command active on level cannot result in unsafe condition after having disabled STO.

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

NOTE: for the applications that require it, a manual acknowledgment of the control command activation on level can only be programmed in the safety controller.

For each CIP Safety device, a data structure (DDDT) collects the input data that is received by the safety controller and the output data that is sent to the safety drive.

Name	Type	Value	Comment	Alias
ATV9xx_Revision_11_1_CS_05/20C	T_ATV9xx_Revision_11_1HW69M			
Health	BOOL		= Global Health= Health_In & Health_Out	
CTRL_IN	BOOL	1	= Enable/Disable Input connection	
CTRL_OUT	BOOL	1	= Enable/Disable Output connection	
Status_IN	S_CIP_SAFETY_STATUS		= Input Status	
Status_OUT	S_CIP_SAFETY_STATUS		= Output Status	
Conf_IN	S_CIP_SAFETY_CONF		= CIP signatures and parameters for Input connection	
Conf_OUT	S_CIP_SAFETY_CONF		= CIP signatures and parameters for Output connection	
Input	T_ATV9xx_Revision_11_1HW69M_IN		Input Variables	
Free0	BYTE		Unused Variable	
Torque_Disabled	BOOL			
Safety_Fault	BOOL			
Restart_required	BOOL			
Free1	ARRAY[0..2] OF BYTE		Unused Variable	
Output	T_ATV9xx_Revision_11_1HW69M_OUT		Output Variables	
Free2	BYTE		Unused Variable	
Safe_Torque_Off	BOOL			
Safety_Reset	BOOL			
Free3	ARRAY[0..2] OF BYTE		Unused Variable	

NOTE: Before establishing the CIP safety connection, verify that the Ethernet IP standard connection is established and the ATV●●●_Freshness value is 1.

The communication between the PLC and the safety drive can be enabled through the setting of CTRL_IN & CTRL_OUT bits to 1 in the corresponding CIP Safety device DDDT.

Parameter	Attribute (bit)	Data Type	Description
Health	–	BOOL	Input or Output health: For input: <ul style="list-style-type: none"> • 1= input communication is open and operational. • 0= error detected for input communication by server safety validator. For output: <ul style="list-style-type: none"> • 1= output communication is open and operational. • 0= error detected for output communication by client safety validator.
CTRL_IN	–	BOOL	Enable/Disable Input connection.
CTRL_OUT	–	BOOL	Enable/Disable Output connection.
Status_IN	–	T_CIP_SAFETY_STATUS	The status of the input connection (Safety drive to PLC).

Parameter	Attribute (bit)	Data Type	Description
Status_OUT	–	T_CIP_SAFETY_STATUS	The status of the output connection (PLC to Safety drive).
Conf_In	–	T_CIP_SAFETY_CONF	CIP signatures and parameters for Input connection.
Conf_Out	–	T_CIP_SAFETY_CONF	CIP signatures and parameters for Output connection.
Input			
Input.Torque_Disabled	[0]	BOOL	1= Torque disabled 0= Torque permitted
Input.Safety_Fault ⁽¹⁾	[6]	BOOL	1= CIP Safety error is present
Input.Restart_Required	[7]	BOOL	1= Restart is required
Output			
OUTPUT.Safe_Torque_off ⁽¹⁾	[0]	BOOL	1= Permit Torque 0= Disable Torque
OUTPUT.Safety_Reset ⁽¹⁾	[7]	BOOL	0 → 1 = Reset CIP Safety error
(1): Only this data is safety data with SIL 3 integrity.			

The safety controller is responsible for managing the safety aspect (activate/deactivate the STO function) of the drive when the connection is opened through the safety output assembly. When no safety output assembly has been exchanged between the Originator and Target, the safety drive activates the STO function by default.

The function can be activated/deactivated through the CIP Safety OUTPUT.Safe_Torque_off.

The safety drive STO function reaction time is 36 ms. Reaction time for the drive is the delay between the time the STO function of the CIP Safety module receives the STO request and the time when the torque is disabled from the motor.

NOTE: this reaction time does not include the network reaction time dependent of the parameters stored in the safety controller. For more details, refer to Modicon M580 Safety Manual

The timeout error is triggered when the time between cyclic exchanges have exceeded the CIP Safety timeout or the drive timeout. The first triggered timeout is the one taking effect but generally the CIP safety timeout is set to a value lower than the drive timeout.

If the CIP Safety timeout is exceeded, the safety drive triggers a **SIOF** error, and if the drive timeout is exceeded, **[Eth Error Response] ETHF** error is triggered. For more information, refer to the Ethernet manual, page 12.

Reset Ownership

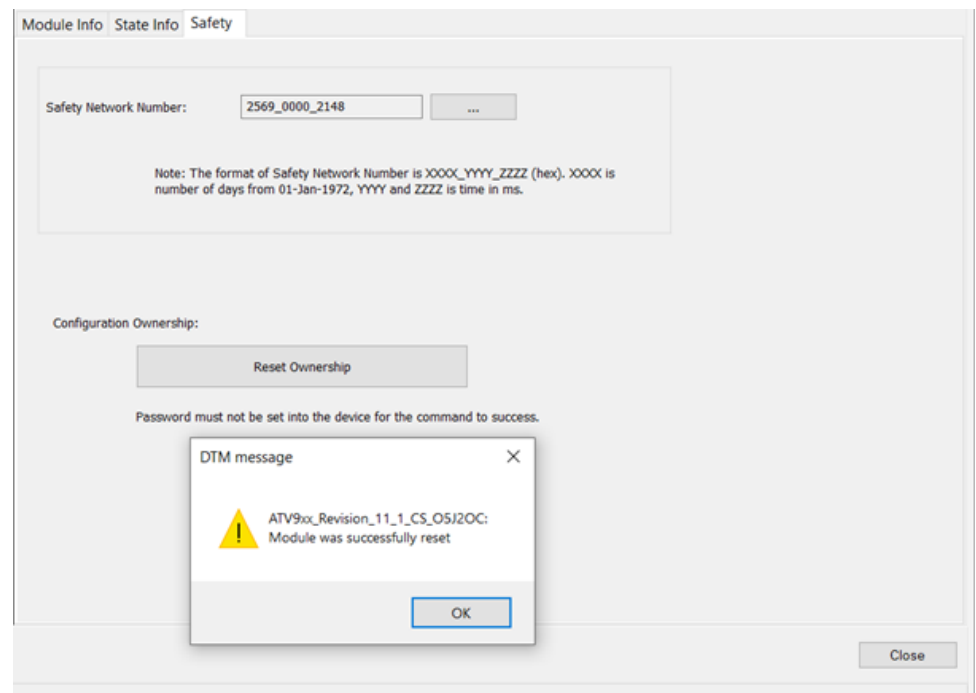
The RESET Ownership command allows to reset the CIP Safety drive configuration settings to the factory default values.

The safety connection must be inhibited before the reset by reset CTRL_IN and CTRL_OUT bits from SAFETY DRIVE DDDT.

Reset ownership is not possible when the safety drive is in **[Ready] RDY** state (SSO-executing), verify that the input and output connections are disabled

After the reset, the safety drive performs a restart. It is now not owned and can be configured by another originator.

The reset Ownership functionality can be accessed in the **[Diagnosis] → [Safety tab]**.



Diagnostics and Troubleshooting

What's in This Part

Operating states.....	67
Detected Errors.....	68

Operating states

The table provides the different operating states for the CIP safety module:

Name	Description
[Starting]	Initialization ongoing but not completed.
[Not Rdy to Switch On]	CIP Safety module initialization is completed.
[Switch On Disabled]	Safety module and drive initialization are completed but CIP safety controller has not opened the CIP Safety connection with the Safety drive.
[Ready to Switch On]	Configuration of CIP safety module is completed.
[Operation Enabled]	CIP Safety drive is in operational mode. STO is deactivated and safety drive state is in RDY.
[Fault]	Safety error triggered.
[STO Active]	Safety function STO is active.

NOTE: The CIP safety module operating state machine is different from the drive operating state machine.

Detected Errors

Overview

The safety-related errors are classified as follows

- **SIOF**: Safety-related IO errors
- **SAVF**: Safety function violation error
- **SCFF**: Safety-related configuration error

When an error is detected by the CIP safety module, the drive displays one of the previous errors depending on the cause(s).

This detected error is completed with one or several error codes in order to provide more information on the probable causes and remedies (refer to the table related to each error for more information on the main error codes).

The error codes can be accessed by scrolling at the bottom of the window displayed on the Display Terminal when an error is triggered. They can also be accessed in the menu **[Complete Settings] → [Safety Module] → [Safety Module Error]** or via the Safety Display tab of the commissioning software.

NOTE: If several errors are detected simultaneously, the first detected error defines which safety related error code will be triggered.

Error Class

The CIP safety module triggers errors. The errors can be grouped by classes as following:

Error Class	Stop category (as per IEC 60204)	Description
0	–	Warning: an event has been detected. No interruption of the movement.
2	0	An error has been detected by the CIP safety module. Error class 2 are resettable.
3	0	An error has been detected. The safety function STO is triggered and the power stage is immediately disabled. Errors class 3 are resettable.
4	0	An error has been detected. The safety function STO is triggered and the power stage is immediately disabled. Errors class 4 are non-resettable.

CIP Safety Error Reset

Resettable error: After the cause has been removed, this detected error can be cleared via:

- The Safety Output assembly OUTPUT.Safety_Reset or a power cycle of the safety drive when the safety connection between the safety drive and the safety controller is established.

Note: The Safety output assembly does not clear the drive resettable errors not linked to the CIP safety module.

- Digital input or control bit set to the **[Fault reset] RST** function or Ethernet IP standard assembly Bit7 Fault Reset of **[Command Register] CMD** or a power cycle when the safety connection between the safety drive and the safety controller is not in executing state.

NOTE: When using **[Product Restart] RP** or **[Prod Restart Assign] RPA** to clear the safety error, the safety drive takes longer time to be in RDY state mode than a standard drive (with no CIP Safety module).

Non-resettable error: After removing the cause, this detected error requires a power cycle of the drive to be cleared.

Note:



- If a resettable error and a non-resettable error are detected at the same time, the non-resettable error cannot be reset manually. After removing the causes, these detected errors require a power cycle of the drive to be cleared.
- When an error is triggered by the CIP safety module, it is communicated to the drive. Similarly, the drive can also trigger an error.



If both the drive and the CIP safety module detect an error, and the safety error is cleared via the OUTPUT.Safety_Reset,, it is necessary to clear the drive error separately by performing a power cycle or using **[Fault reset] RST**.



It is possible that the same cause triggers errors in both the drive and the CIP safety module.



SIOF Errors

The table provides the list SIOF detected errors

Error Code	Probable Cause 	Remedy 	Error Class
[CIP Incorrect Length] SME128	<ul style="list-style-type: none"> CIP Safety message has incorrect length Standard CIP assembly received instead of CIP Safety assembly Defective network equipment swapping messages 	<ul style="list-style-type: none"> Verify and replace network equipment if needed Contact your local Schneider Electric representative. 	2
[TCoo Msg Timeout] SME122	<p>Time coordination message timeout reached</p> <ul style="list-style-type: none"> Network cable unplugged Defective network equipment Time coordination message requested by drive not generated by PLC 	<ul style="list-style-type: none"> Verify and replace network equipment if needed Verify PLC Verify that the Ethernet IP standard connection is established before the CIP Safety connection. Contact your local Schneider Electric representative. 	2
[TCoo Parity Error] SME124	<p>Time coordination message parity error</p> <ul style="list-style-type: none"> Defective network equipment sending old messages 	<ul style="list-style-type: none"> Verify and replace network equipment if needed Contact your local Schneider Electric representative 	2
[TCoo 5 Sec Timeout] SME125	<p>Time coordination message 5 sec timeout reached</p> <ul style="list-style-type: none"> Network cable unplugged Network overload Defective network equipment causing delay 	<ul style="list-style-type: none"> Verify and adapt network load Verify and replace network equipment if needed Contact your local Schneider Electric representative 	2
[TCoo Ping Timeout] SME126	<p>Time coordination message ping interval timeout reached</p> <ul style="list-style-type: none"> Network cable unplugged Network overload Defective network equipment causing delay 	<ul style="list-style-type: none"> Verify and adapt network load Verify and replace network equipment if needed Contact your local Schneider Electric representative 	2
[TCoo CRC Error] SME127	<p>Time coordination message CRC error</p>	<ul style="list-style-type: none"> Verify and adapt network load 	2



Error Code	Probable Cause 	Remedy 	Error Class
	<ul style="list-style-type: none"> • Network cable unplugged • Network overload • Defective network equipment causing delay 	<ul style="list-style-type: none"> • Verify and replace network equipment if needed • Contact your local Schneider Electric representative 	
[CIP Msg Tstamp Error] SME12A	CIP Safety message with same timestamp received <ul style="list-style-type: none"> • Defective network equipment sending previous messages • Timestamp not incremented by PLC 	<ul style="list-style-type: none"> • Verify and replace network equipment if needed • Verify PLC • Contact your local Schneider Electric representative. 	2
[CIP Msg Tstamp>NTE] SME12B	CIP Safety message timestamp greater than Network Time Expectation <ul style="list-style-type: none"> • Transfer time of message from PLC to device is greater than maximum allowed limit • Network overload • Defective network equipment causing delay or inverted message 	<ul style="list-style-type: none"> • Verify and adapt network load • Verify and replace network equipment if needed • Contact your local Schneider Electric representative. 	2
[Inval Msg Age>NTE] SME12C	Invalid message age greater than Network Time Expectation <ul style="list-style-type: none"> • Transfer time of message from PLC to device is greater than maximum allowed limit • Network overload • Defective network equipment causing delay or inverted message 	<ul style="list-style-type: none"> • Verify and adapt network load • Verify and replace network equipment if needed • Contact your local Schneider Electric representative. 	2
[Valid Msg Age>NTE] SME12D	Valid message age greater than Network Time Expectation <ul style="list-style-type: none"> • Transfer time of message from PLC to device is greater than maximum allowed limit • Network overload • Defective network equipment causing delay or inverted message 	<ul style="list-style-type: none"> • Verify and adapt network load • Verify and replace network equipment if needed • Contact your local Schneider Electric representative. 	2

Error Code	Probable Cause 	Remedy 	Error Class
[CIP Msg CRC Error] SME12E	CIP Safety message CRC error <ul style="list-style-type: none"> • Electromagnetic disturbances on network • Defective network equipment corrupting messages 	<ul style="list-style-type: none"> • Verify the environment (electromagnetic compatibility) • Verify and replace network equipment if needed • Contact your local Schneider Electric representative 	2
[CIP Msg Mode Error] SME12F	CIP Safety message redundant bits error <ul style="list-style-type: none"> • Electromagnetic disturbances on network • Defective network equipment corrupting messages • Bits not duplicated correctly in safety message by PLC 	<ul style="list-style-type: none"> • Verify the environment (electromagnetic compatibility) • Verify and replace network equipment if needed • Contact your local Schneider Electric representative 	2
[CIP Msg CRC Error] SME130-	CIP Safety message CRC error <ul style="list-style-type: none"> • Electromagnetic disturbances on network • Defective network equipment corrupting messages 	<ul style="list-style-type: none"> • Verify the environment (electromagnetic compatibility) • Verify and replace network equipment if needed • Contact your local Schneider Electric representative 	2
[CIP Msg CRC Error] SME131 [CIP Msg Mode Error] SME132 [CIP Msg Mismatch] SME133	CIP Safety message CRC error <ul style="list-style-type: none"> • Electromagnetic disturbances on network • Defective network equipment corrupting messages 	<ul style="list-style-type: none"> • Verify the environment (electromagnetic compatibility) • Verify and replace network equipment if needed • Contact your local Schneider Electric representative 	2
[CIP Msg Timeout] SME134	CIP Safety message timeout reached <ul style="list-style-type: none"> • Network cable unplugged • Network overload • Defective network equipment causing delay • Interruption of CIP Safety due to error detection by PLC 	<ul style="list-style-type: none"> • Verify and adapt network load • Verify and replace network equipment if needed • Verify devices on the network • Contact your local Schneider Electric representative 	2

Error Code	Probable Cause 	Remedy 	Error Class
[Internal 24V OverV] SME060	Internal 24VDC overvoltage.	Contact your Schneider Electric Customer Care Center (CCC).	2
[Internal 24V UnderV] SME06D	Internal 24VDC undervoltage.	Contact your Schneider Electric Customer Care Center (CCC).	2
[Unexpected STO] SME0D4	<ul style="list-style-type: none"> • STO is requested from Drive terminal. • The safety module has detected an error on STO circuitry. 	<ul style="list-style-type: none"> • Verify that drive STO_A and STO_B are wired to 24V. • Contact your local Schneider Electric representative. 	3

SAVF Errors



The table provides the list **SAVF** detected errors

Error Code	Dec. ⁽¹⁾ value	Probable Cause 	Remedy 	Error Class
[Low Temp Warn] SME01C	28	Temperature exceeds lower limit (warning).	Verify environment temperature	0
[High Temp Warn] SME01D	29	Temperature exceeds upper limit (warning).	Verify environment temperature	0
[Low Temp Error] SME05F	95	Temperature exceeds lower limit.	Verify environment temperature.	4
[High Temp Error] SME061	97	Temperature exceeds upper limit.	Verify environment temperature.	4

(1) Dec. = Decimal



SCFF Errors

The table provides the list SCFF detected errors

Error Code	Dec. ⁽¹⁾ value	Probable Cause 	Remedy 	Error Class
[Corrupted Config] SME032	50	Corrupted configuration.	Contact your Schneider Electric Customer Care Center (CCC).	4
[Board Compatibility] SME0F4	244	Drive control board is incompatible with CIP safety module.	Contact your Schneider Electric Customer Care Center (CCC).	4
[TUNID Mismatch] SME113	275	Mismatch between TUNID and IP address <ul style="list-style-type: none"> IP address of the device has been modified 	<ul style="list-style-type: none"> Use the same IP address used when saving TUNID Perform a CIP Safety reset type 1 	3

(1) Dec. = Decimal

[Internal Error 6] InF6 Error

Error Code	Probable Cause 	Remedy 
[Internal Error 6] InF6	<ul style="list-style-type: none"> The option module installed in the drive is not recognized. The drive firmware version is not compatible with the CIP safety module 	<ul style="list-style-type: none"> Verify the catalog number and compatibility of the option module. Contact your local Schneider Electric representative.

For more details about detected errors, contact your local Schneider representative.

To access the Probable causes and remedies for the errors triggered by the CIP Safety module on the Graphic Display Terminal, navigate to **[Safety Module Error x] SMEx** (for more information, refer to *Dedicated Safety Function* menu in the Display Terminal, page 42) using the Graphic Display Terminal and then press the "i" button. A Cause & Remedy message is displayed.

Maintenance and decommissioning

What's in This Part

Remove or replace the safety drive	76
Remove or replace the safety controller	78
Clone the safety drive	79
Reset safety configuration of the safety drive	80
Decommission the safety drive	81

Safety instructions

▲ WARNING

UNANTICIPATED EQUIPMENT OPERATION

- Carefully follow the instructions given in this chapter.
- Do not operate the Safety drive with unknown or unsuitable settings or data.
- Perform a comprehensive commissioning test to verify that modification of the hardware has been done properly.

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

Remove or replace the safety drive

To replace the safety drive while keeping the same CIP safety module (configured):

- The safety drive configuration must be saved during the commissioning part into FDR server or using Somove/DTM (for more information refer to DTM online help) or using Graphic Display Terminal.
- Power off the safety drive.
- Unplug the CIP safety module from the safety drive.
- Mount the new safety drive onto the safety system and plug the CIP safety module.
- Power on the safety drive.
- If the configuration has been saved using SoMove:
 - Select Edit Connection/ Scan → Modbus IPv6 → Scan to discover the safety drive through the IPv6.
 - Select the discovered safety drive and restore the configuration previously saved to the safety drive.
- If the configuration has been saved into FDR server:
 - Set the IPmode to DHCP and enter the DeviceName used in the previous safety drive.
- Restart the safety drive by activating this function through the parameter **[Product Restart]_{RP}** (set **[Product Restart]_{RP}** to **[Yes]** Yes, or perform a power cycle)(for more information refer to the ATV900 Programming manual, page 12).
 - The safety drive configuration is restored from FDR server, and the safety drive state SSO is in Waiting for TUNID state.
- Set SNN to the new safety drive to reestablish the connection with the M580 safety PLC using the EcoStruxure Control Expert.

To replace the CIP safety module while keeping the same drive:

- Power off the safety drive.
- Unplug the CIP safety module from the safety drive.
- Plug the new CIP Safety module.
- Power On the safety drive (Safety drive state is on Waiting for TUNID).
- Set SNN to reestablish the connection with the M580 safety PLC.

To replace the safety drive (drive+ CIP Safety module):

- Power off the safety drive.
- Uninstall the safety drive.
- Mount the new safety drive and plug the new CIP Safety module.
- Power on the safety drive.
- If the configuration has been saved into FDR server:
 - Set the IPmode to DHCP and enter the DeviceName used in the previous safety drive.
- If the configuration has been saved using SoMove:
 - Select Edit Connection/ Scan ➡ Modbus IPv6 ➡ Scan to discover the safety drive through the IPv6.
 - Select the discovered safety drive and restore the configuration previously saved to the safety drive.
 - Restart the safety drive by activating this function through the parameter **[Product Restart]_{RP}** (set **[Product Restart]_{RP}** to **[Yes]** Yes, or perform a power cycle).

The safety drive configuration is restored from FDR server and the safety drive state SSO is in Waiting for TUNID state.
- Set SNN to reestablish the connection with the M580 safety PLC.

Remove or replace the safety controller

To replace the safety controller:

- Power off the safety controller.
- Uninstall the safety controller.
- Mount the new safety controller.
- Power on the safety controller.
- Restore the safety controller configuration through EcoStructure Control Expert (previously saved on the computer):
 - If the configuration is completely restored, the safety drive requires a power cycle to establish a CIP Safety connection with the new safety controller.
 - If the configuration is not completely restored (modification of safety PLC IP address, safety PLC SNN not restored → configuration not identical to the configuration of the previous safety PLC):
 - A Reset Ownership is required.
 - Set The SNN to the safety drive to establish a CIP Safety connection with the new Safety controller.

Clone the safety drive

Verify that the firmware version of the safety drive is compatible with CIP safety module (**V2.1IE82**), otherwise a firmware update is required. Contact your local Schneider Electric Services.

To clone the safety drive (Only the drive configuration is restored, the safety configuration needs to be configured):

- If the safety drive configuration is previously saved on:
 - Display terminal:
 - Restore the safety drive configuration.
 - Restart the safety drive.
 - SoMove or webserver:
 - Restore the safety drive configuration using IPv6 connection, see ATV900 DTM online help for more details on how to restore a drive configuration.
 - Connect to the safety drive using IPv6. Restart the safety drive.
- Open the archived project on Ecostructure Control Expert.
- Select the vendor DTM to clone the safety drive configuration.
- The safety configuration need to be reconfigured, refer to Configuration with the commissioning software, page 46.

Reset safety configuration of the safety drive

The safety configuration can be reset by setting the **[Safety Config Reset] SFRS** to **YES** (see **[Safety Config Reset] SFRS**, page 42).

The safety connection must be inhibited before the reset by reset CTRL_IN and CTRL_OUT bits from SAFETY DRIVE DDDT.

A warning pop-up on the Display terminal should be confirmed. Once confirmed, the safety drive will perform a restart.

The safety configuration, including the TUNID, is then reset. The safety drive is in SSO-Waiting for TUNID.

NOTE: During the safety configuration reset, the displayed status of the safety drive may be incoherent.

Note: The drive configuration remains the same and is not impacted by the safety configuration reset.

Decommission the safety drive

Consider performing decommissioning at the end of the device's lifecycle as a recommended practice.

The process of decommissioning the safety drive involves resetting the safety and non-safety configuration.

▲ WARNING

UNANTICIPATED EQUIPMENT OPERATION

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.

First the safety configuration must be reset. Refer to *Reset safety configuration of the safety drive*, page 80.

After this step is completed, the drive configuration can be reset by selecting the **[Go to Factory Settings]** GFS in the **[File management]** → **[Factory settings]** menu on the Display Terminal several screens to consider are displayed.

Glossary

C

CIP:

CIP: Common Industrial Protocol

D

DDDT:

Device Derived Data Type

A DDT predefined by the manufacturer and not modifiable by user. It contains the I/O language elements of an I/O module.

DTM:

Device Type Manager

A DTM is a device driver running on the host PC. It provides a unified structure for accessing device parameters, configuring, and operating the devices, and troubleshooting devices. DTMs can range from a simple graphical user interface (GUI) for setting device parameters to a highly sophisticated application capable of performing complex real-time calculations for diagnosis and maintenance purposes. In the context of a DTM, a device can be a communications module or a remote device on the network.

E

ECE: EcoStruxure Control Expert

EDS:

Electronic Data Sheet

EDS are simple text files that describe the configuration capabilities of a device. EDS files are generated and maintained by the manufacturer of the device.

O

OUNID:

Originator Unique Network Identifier

A value that uniquely identifies the connection originating device (typically a CPU) on a CIP safety network.

The OUNID consists of:

- a safety network number (SNN)
- a node address (for EtherNet/IP networks, the IP address).

P

PLC:

Programmable logic controller.

S

SCID:

Safety Configuration Identifier

SNN:

SNN: Safety Network Number

T**TUNID:**

Target Unique Network IDentifier

A value that uniquely identifies the connection target device on a CIP safety network.

The TUNID consists of:

- a safety network number (SNN)
- a node address (for EtherNet/IP networks, the IP address).

Schneider Electric
35 rue Joseph Monier
92500 Rueil-Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

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

© 2023 Schneider Electric. All rights reserved.

JYT89146.01