RFID OsiSense® XG

Ethernet Smart Antenna

User Manual

Original instructions

YAGEO GROUP Brings you

Telemecanique Sensors

Legal Information

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither TMSS France nor any of its subsidiaries or other affiliated companies shall be responsible or liable for misuse of the information contained herein.
TelemecaniqueTM Sensors is a trademark of Schneider Electric Industries SAS used under license by TMSS France. Any other brands or trademarks referred to in this document are property of TMSS France or, as the case may be, of its subsidiaries or other affiliated companies. All other brands are trademarks of their respective owners.

Table of Contents

Important Information 5
About the Book 6
Cybersecurity 7
General Information 9
System Presentation 9
Exchange Principle 10
Overview of the OsiSense XG Range 11
System View 11
Information Related to Cyber Security 14
Specifications and Physical Description 15
Smart Antenna Characteristics 15
Tags Characteristics 17
Description of the Smart Antenna 20
Connecting the OsiSense XG Smart Antenna 21
Wiring Accessories 22
Smart Antennas Wiring Example 23
Installing the System 24
Installation Precautions 24
IP Address Configuration 28
Operating Principles 32
Read/Write Operating Mode 32
Memory Zones 34
Smart Antenna System Memory Zone 35
Smart Antenna Command/Instructions Memory Zone 36
EtherNet/IP Communications Support 43
Object Model 43
About the Object Model 43
Assembly Object (Class ID 4) 44
Modbus Object (Class ID 0x44) 45
Unity Pro: EtherNet/IP Application Example 46
Presentation 47
Creating a Project 47
Configuring the BMXNOC0401 EtherNet/IP Communication Module 48
Configuring the Ethernet Smart Antenna 49
Read Application Example 52
RSLogix: EtherNet/IP Application Example 53
Configuring a Smart Antenna on an EtherNet/IP Network with a ControlLogix PLC 54
Read the Assembly 102 (General Status) or 103 (Read Table) Using an Explicit Message 57
Reading/Writing Request with the Modbus Object 59
Modbus TCP/IP Communications Support 64
Modbus Commands Supported by the Smart Antenna 64
Modbus Requests Description 65
Modbus TCP/IP Application Example 67

Diagnostics 70
Smart Antenna Diagnostic LEDs 70
FAQs 72
FAQ 72
Glossary 77
Index 83

Important Information

NOTICE

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 TMSS France 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.

About the Book

Document Scope

This guide describes how to use OsiSense XG Smart Antenna and associated accessories.

Validity Note

This document is applicable to OsiSense XG Smart Antenna, XGCS850C201.

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

Step	Action
1	Go to the Telemecanique Sensors home page *www.tesensors.com*.
2	In the **Search** box, type the model number of a product or the name of a product range. • Do not include blank spaces in the model number/product range. • To get information on a grouping similar modules, use asterisks (*).
3	If you entered a model number, go to the **Product datasheets** search results and click the model number that interests you. If you entered the name of a product range, go to the **Product Ranges** search results and click the product range that interests you
4	If more than one model number appears in the **Products** search results, click the model number 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 XGCS850C201 product datasheet**.

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.

Product Related Information

⚠ CAUTION

UNINTENDED EQUIPMENT OPERATION

- The application of this product requires expertise in the design and programming of control systems. Only persons with such expertise must be allowed to program, install, alter, and apply this product.
- Follow all local and national safety codes and standards.
- Read recommendations related to Cyber Security detailed in Chapter Information Related to Cyber Security, page 14.

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

Related Documents

Title of documentation	Reference number
XGST2020 Terminal XG - Quick Start Guide	HRB34094
XGST2020 Handheld Terminal - Software Guide	EIO0000002166 (ENG), EIO0000002167 (FRE)

You can download these technical publications and other technical information from our website at *www.tesensors.com*.

QR Code

A QR code including the Telemecanique Sensors web address is present on the Ethernet Smart Antenna. Technical files and documents are available in this website.

http://www.qr.tesensors.com/XG0001

User Comments

We welcome your comments about this document. You can reach us by e-mail at customer-support@tesensors.com.

Cybersecurity

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

⚠ WARNING

UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS

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

Consult the Cybersecurity Best Practices (https://www.se.com/ww/en/download/document/CS-Best-Practices-2019-340/) for additional information.

General Information

Aim of this Chapter

This chapter presents the OsiSense XG Smart Antenna and the associated range of equipment.

System Presentation

Smart Antenna Presentation

The Smart Antenna is a compact RFID station offering the following advantages:

- 2 Ethernet ports
- Daisy chaining up to 32 Smart Antennas
- Compatible with most 13.56 MHz tags on the market.

Definition of RFID

RFID is the use of radio transmission to identify and locate objects.

An RFID system is based on 3 main components:

- A reader (read/write station)
- A radio antenna
- An electronic tag

Operation of an RFID System

The tag is attached on, or in, the object to be tracked or identified. There is no contact with the reader. This means that the tag can be placed inside objects (boxes, bags, and so on...) and that the reader can be positioned behind a protective screen, as long as the materials are not metallic.

When a tag enters the field generated by the reader, it detects the signal and exchanges the data (read or write) between its memory and the reader.

Presentation of the Offer OsiSense XG

OsiSense XG is an RFID system offering:

- Traceability and tracking of items
- Flexibility of production systems
- Various types of access control

An open system:

- System compatible with tags that comply with standards ISO 14443 and ISO 15693
- Modbus TCP/IP and EtherNet/IP protocols

A simple system:

- No station programming
- Data formatted in accordance with PLC standards (16-bit registers)
- Automatic configuration of communication parameters (speed, format, and so on...)

- Quick wiring using M12 connectors
- Extensive range of cables and mounting accessories
- Possibility of using metal supports

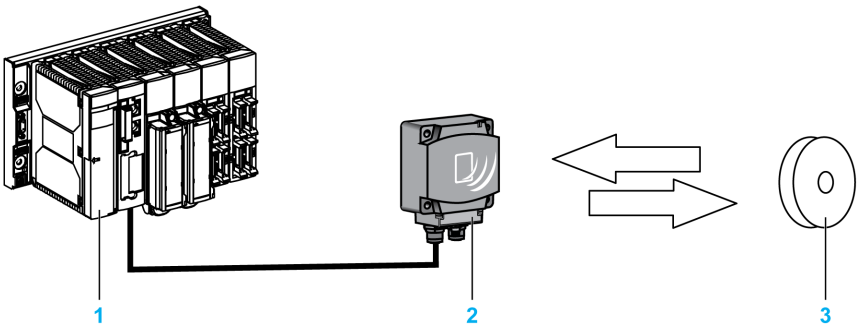
Integrated system:

- Reader, radio antenna, and network functionalities in one device
- The smallest industrial RFID reader

Exchange Principle

Presentation

The OsiSense XG Smart Antenna is used to send information from the tag to the PLC and vice versa, as described below:



1 PLC

2 Smart Antenna

3 Tag

Phases in the Process

The table shows the various exchange phases:

Phase	Exchanges	
	PLC **Smart Antenna**	**Smart Antenna** **Tag**
1		Look for a tag in the dialog zone →
2		Positive response ←
3	Send a read/write command →	
4		Execution of the command (with checks) ↔
5	Send back report ←	

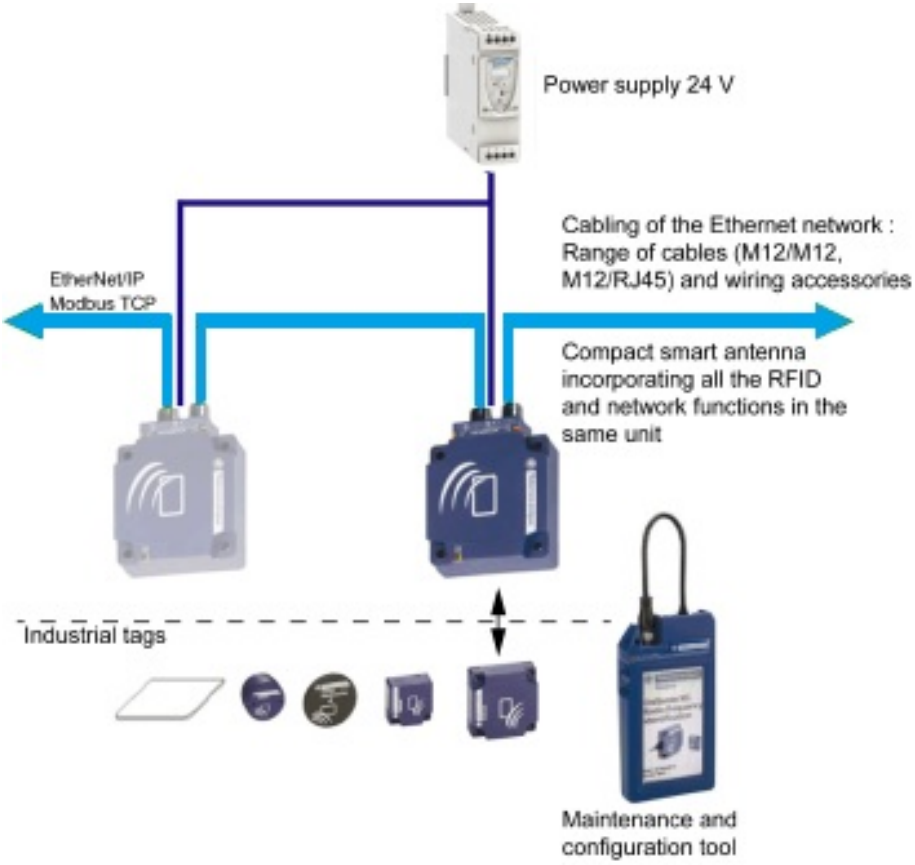
NOTE:

- If phase 3 is carried out with no tag present, a detected error message is sent back to the PLC.
- If a detected error occurs in phase 4, this phase is automatically restarted (up to 3 times). If a detected error is still detected at the end of phase 4, a detected error report is sent back in phase 5.

Overview of the OsiSense XG Range

Introduction

The figure illustrates the OsiSense XG range.



System View

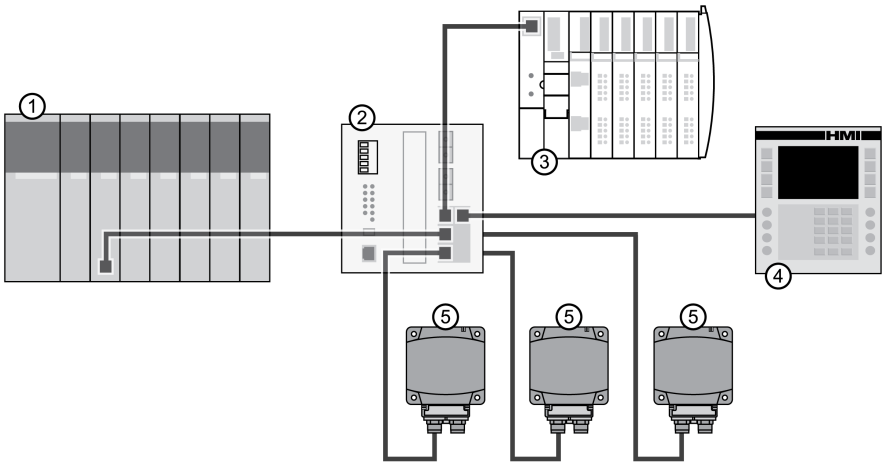
Description

OsiSense XG Smart Antenna can be used with a protocol compliant scanner as part of control system architecture. The built-in unmanaged 2-port Ethernet switch of the Smart Antenna allows you to use the network topology that meets your application needs. These topologies include the following:

- star
- daisy-chain
- ring (daisy-chain with loopback)
- combination of star and daisy-chain

Star

Star topology allows you to connect additional network equipment. Performing maintenance on one module—for example, by removing the network cable, or by cycling power to the module—does not affect other modules.



1 Quantum PLC

2 Ethernet switch

3 Advantys STB Island

4 Magelis HMI device

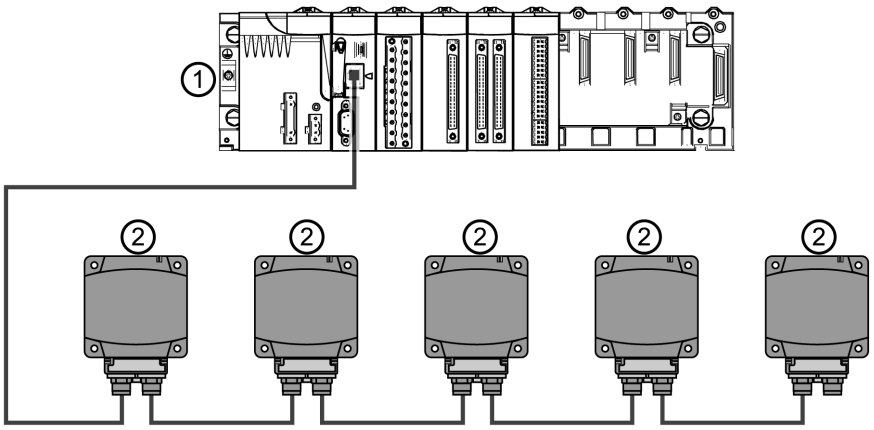
5 OsiSense XG Smart Antenna

Daisy-Chain

You can create a daisy-chain topology by using the embedded switch ports to connect a series of up to 32 OsiSense XG Smart Antennas.

NOTE: When considering the daisy chain topology, note that:

- Performing maintenance on any module not physically located at the end of the daisy chain—for example, by removing the network cable, or by cycling power to the module—affects any modules located down the chain from the maintained module.
- The embedded dual port Ethernet switch located in each module eliminates the need for additional Ethernet switches.



1 M340 PLC

2 OsiSense XG Smart Antenna

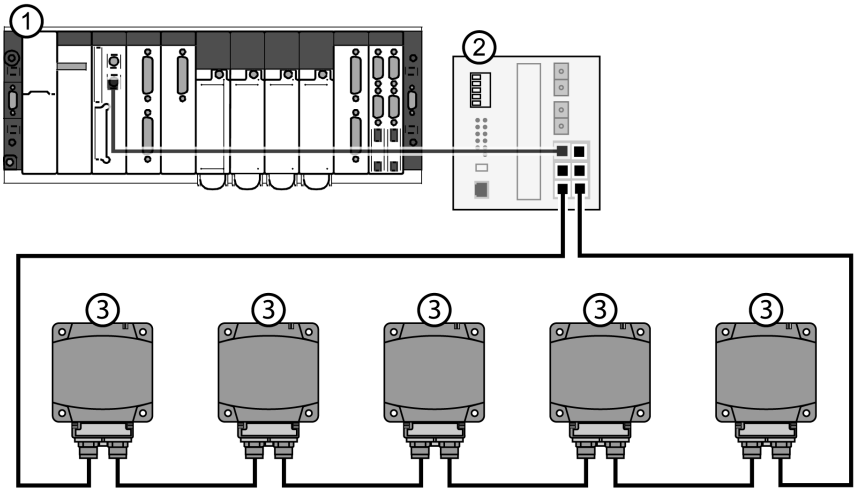
Ring

You can create a ring topology by using a switch with redundancy management protocol (for example ConneXium TCSESM043F23F0).

You can connect a series of up to 32 OsiSense XG Smart Antennas.

NOTE: When considering the ring topology, note that:

- If a network segment becomes inoperable or is cut, all Smart Antennas remain operational.



1 Premium PLC

2 Ethernet switch with loopback function

3 OsiSense XG Smart Antenna

The table shows the ConneXium switches with redundancy function compatible with Smart Antennas:

Reference	Description
TCSESB083F23F0	8 port basic managed switch 8TX
TCSESB083F2CU0	8 port basic managed switch 6TX – 2FX multi mode
TCSESB093F2CU0	9 port basic managed switch 6TX – 3FX multi mode
TCSESM043F1CS0	4 port managed switch 3TX – 1FX single mode
TCSESM043F1CU0	4 port managed switch 3TX – 1FX multi mode
TCSESM043F23F0	4 port managed switch 4TX
TCSESM043F2CS0	4 port managed switch 2TX – 2FX single mode
TCSESM043F2CU0	4 port managed switch 2TX – 2FX multi mode
TCSESM083F1CS0	8 port managed switch 7TX – 1FX single mode
TCSESM083F1CU0	8 port managed switch 7TX – 1FX multi mode
TCSESM083F23F0	8 port managed switch 8TX
TCSESM083F2CS0	8 port managed switch 6TX – 2FX single mode
TCSESM083F2CU0	8 port managed switch 6TX – 2FX multi mode
TCSESM103F23G0	10 port managed switch 8TX/2TX-GBIT
TCSESM103F2LG0	10 port managed switch 8TX/2SFP-GBIT
TCSESM163F23F0	16 port managed switch 16TX
TCSESM163F2CU0	16 port managed switch 14TX – 2FX multi mode
TCSESM163F2CS0	16 port managed switch 14TX – 2FX single mode

Reference	Description
TCSESM243F2CU0	24 port managed switch 22TX – 2FX multi mode
TCSESM083F23F1	8 port extended managed switch 8TX
TCSESM063F2CS1	8 port extended managed switch 6TX – 2FX single mode
TCSESM063F2CU1	8 port extended managed switch 6TX – 2FX multi mode

Information Related to Cyber Security

The XGCS850C201 RFID station shall be isolated from the network. The recommended network architecture is to place the station behind a PLC or an external device. For the different network topologies proposal, refer to chapter System View, page 11.

TMSS FRance also recommends a defense-in-depth approach to cybersecurity. No single approach is adequate. The defense-in-depth approach layers the network with security features, appliances, and processes.

For the XGCS850C201 product, TMSS FRance recommends the following best practices:

- Network Partitioning:

  Locate devices behind firewalls capable of deep packet inspection (for instance Tofino Firewall) with rulesets limiting access with only approved protocols and functions and to only those devices and endpoints requiring access. Please refer to the following document for further details with following link: https://www.se.com/ww/en/download/document/STN%20v2/
- Anomalous IP traffic:

  Block and detect anomalous IP traffic and malformed packets (use for instance Tofino Firewall).
- IP address setting:

  It is recommended to use a private IP address range that allows only communication between the concentrator and the PLC
- Access Controls:

  Install physical and logical controls so no unauthorized personnel or device can access your systems, components, peripheral equipment, and networks.

For more details and assistance on how to protect your installation, please contact your local TMSS FRance support.

Specifications and Physical Description

Aim of this Chapter

This chapter presents the specifications and the physical description of the OsiSense XG Smart Antenna.

Smart Antenna Characteristics

Characteristics

The table gives the technical characteristics of the Smart Antenna:

Characteristic		Description
Temperature	Operation	–25...+70 °C (–13...+158 °F)
	Storage	–40...+85 °C (–40...+185 °F)
Degree of protection		IP65 according to IEC60529
Vibration resistance EN 60068.2.27 EN 60068.2.6		2 mm (0.078 in) from 5 to 29.5 Hz / 7 g (7 gn) from 29.5 to 150 Hz 30 g (30 gn) / 11 ms
Resistance to mechanical shocks		IK02 according to EN 50102
Standards/Certifications		cULus, CE, UKCA, FCC, IC/ISED
Immunity to disturbances		Immunity to electrostatic discharges, radiated electromagnetic fields, fast transients, electrical surges, conducted and induced interference and power frequency magnetic field according to IEC61000/EN 55022
Unit dimensions		80x93x40 mm (3.15x3.66x1.57 in)
RFID frequency		13.56 MHz
Type of associated tag		Standardized ISO 15693 and ISO 14443 tags Automatic detection of the tag type
Nominal sensing distance		20...100 mm (0.78...3.94 in) depending on associated tag
Power supply		24 Vdc SELV/PELV Connection on M8 4 pins male socket
Power supply voltage limits		19.2...29 V including ripple
Power consumption		< 150 mA
Communication	Interface	Ethernet dual port 10 BASE-T/100 BASE-TX
	Connection	2 M12 D coded female sockets for chaining
Display		- 2 dual color LED for RFID communication - 4 dual color LED for Ethernet communication
Tightening torque for the mounting screws		< 3.6 Nm (31.9 lbf-in)

WARNING TO USERS IN THE UNITED STATES AND CANADA

WARNING TO USERS IN THE UNITED STATES

Federal Communication Commission Interference Statement

This equipment complies with FCC's radiation exposure limits set forth for an uncontrolled environment under the following conditions :

1. This equipment should be installed and operated such that a minimum separation distance of 20 cm is maintained between the radiator (antenna) and user's/nearby person's body at all times.
2. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

NO UNAUTHORIZED MODIFICATIONS

CAUTION: This equipment may not be modified, altered, or changed in any way without signed written permission from TMSS FRance Any changes or modifications to this equipment not expressly approved by TMSS France may cause harmful interference, will void the FCC authorization to operate this equipment and will void the TMSS France warranty.

WARNING TO USERS IN THE CANADA / *ATTENTION POUR LES UTILISATEURS AU CANADA*

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS (s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference received, including interference that may cause undesired operation of the device.

This equipment complies with RSS102's radiation exposure limits set forth for an uncontrolled environment under the following conditions :

1. This equipment should be installed and operated such that a minimum separation distance of 20 cm is maintained between the radiator (antenna) and user's/nearby person's body at all times.
2. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

L'émetteur/récepteur exempt de license contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement Economique Canada applicables aux appareils radio exempts de license. L'exploitation est autorisée aux deux conditions suivantes :

1. *il ne doit pas produire de brouillage, et*
2. *l'appareil doit accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible d'en compromettre le fonctionnement.*

Cet équipement est conforme aux limites d'expositions de la CNR102 applicables pour un environnement non contrôlé aux conditions suivantes :

1. *Cet équipement devra être installé et fonctionner de telle manière qu'une distance minimale de séparation de 20 cm soit maintenue entre la partie rayonnante (l'antenne) et l'utilisateur / les personnes à proximité à tout moment.*
2. *Cet émetteur ne doit pas être co-localisé ou opérer en conjonction avec tout autre antenne ou émetteur.*

References:

PMN	XGCS850C201
FCC ID	2BCVYXGCS85
IC info	31308-XGCS85

Tags Characteristics

Tag Characteristics

The table gives the technical characteristics of the tags with EEPROM memory:

Type of Tag	XGHB 123345	XGHB 444345	XGHB 320345	XGHB 221346	XGHB 211345	XGHB 520246	XGHB 90E340
Operation temperature	–25...+70 °C (–13...+158 °F)					–25...+85 °C (–13...+185°F)	–25...+50 °C (–13...+122°F)
Storage temperature	–40...+85 °C (–40...+185 °F)					–40...+90 °C (–40...+194 °F)	–40...+55 °C (–40...+131°F)
Degree of protection	IP68		IP65	IP68		IP68	IP65
Standards supported	ISO 15693	ISO 14443	ISO 15693				
Vibration resistance EN 60068.2.27 EN 60068.2.6	2 mm (0.078 in) from 5 to 29.5 Hz / 7 g (7 gn) from 29.5 to 150 Hz 30 g (30 gn) / 11 ms						
Resistance to mechanical shocks	IK02 according to EN 50102						
Dimensions	∅ 12x8 mm (0.47x0.31 in)	40x40x15 mm (1.57x1.57-x0.59 in)	∅ 30x3 mm (1.18x0.12 in)	26x26x13 mm (1.02x1.02-x0.51 in)	∅ 18 mm (0.70 in)	∅ 50x3 mm (1.97x0.12 in)	58x85.5x1 mm (2.28x3.34-x0.039 in)
Casing materials	PBT		PC	PBT		PPA	PVC
Mounting method	Glued	Screw or clip	Screw	Screw or clip	Threaded hole	Screw	-
Tightening torque for the mounting screws	-	< 1 Nm (8.85 lbf-in)					-
Memory capacity (bytes)	304	3 408	112	256	256	112	256
Type of memory	EEPROM						
Type of operation	Read/write						
Nominal sensing distance (read/write)	20 mm (0.78 in)	48 mm (1.89 in)	65 mm (2.56 in)	55 mm (2.16 in)	20 mm (0.78 in)	100 mm (3.94 in)	100 mm (3.94 in)
Number of read cycles	Unlimited						
Number of write cycles	100000 provided over the entire temperature range						
Number of write cycles at 30 °C *(86 °F)*	2.5 million typical cases						

Type of Tag	XGHB 123345	XGHB 444345	XGHB 320345	XGHB 221346	XGHB 211345	XGHB 520246	XGHB 90E340
Read/write time	Read/write time, page 19						
Retention period	10 years						

The table gives the technical characteristics of the tags with FeRAM memory:

Type of Tag	XGHB320246	XGH440245	XGH440845	XGHB441645	XGHB443245
Operation temperature	–25...+70 °C (–13...+158 °F)				
Storage temperature	–40...+85 °C (–40...+185 °F)				
Degree of protection	IP65	IP68			
Standards supported	ISO 15693		ISO 14443		
Vibration resistance EN 60068.2.27 EN 60068.2.6	 2 mm (0.078 in) from 5 to 29.5 Hz / 7 g (7 gn) from 29.5 to 150 Hz 30 g (30 gn) / 11 ms				
Resistance to mechanical shocks	IK02 according to EN 50102				
Dimensions	∅ 30x3 mm (1.18x0.12 in)	40x40x15 mm (1.57x1.57x0.59 in)			
Casing materials	PC	PBT			
Mounting method	Screw	Screw or clip			
Tightening torque for the mounting screws	< 1 Nm *(8.85 lbf-in)*				
Memory capacity (bytes)	2 000	2 000	8 192	16 384	32 768
Type of memory	FeRAM				
Type of operation	Read/write				
Nominal sensing distance (read/write)	65 mm (2.56 in)		39 mm (1.53 in)		
Number of read cycles	Unlimited				
Number of write cycles	10^{10} provided over the entire temperature range				
Read/write time	Read/Write time, page 19				
Retention period	10 years				

Tag Memory Zone

These tags are addressed according to the following table and are accessible in read/write mode.

The Smart Antenna can read any tag in the XGHB range (automatic detection of the tag type).

Tag reference	Memory Size (bytes)	Range Addresses	
		Dec	Hex
XGHB320345	112	0...55	0...37
XGHB520246	112	0...55	0...37
XGHB90E340	256	0...127	0...7F
XGHB211345	256	0...127	0...7F

Tag reference	Memory Size (bytes)	Range Addresses	
		Dec	Hex
XGHB221346	256	0...127	0...7F
XGHB123345	304	0...151	0...97
XGHB440245	2000	0...999	0...3E7
XGHB320246	2000	0...999	0...3E7
XGHB444345	3408	0...1703	0...6A7
XGHB440845	8192	0...4095	0...FFF
XGHB441645	16384	0...8191	0...1FFF
XGHB443245	32768	0...16383	0...3FFF

NOTE: If an address requested is out of the range address of the tag, a detected error code is generated.

Read/write Time and Tags Maximum Speed

The table shows the calculation of read/write time in static, and the tags maximum speed in dynamic:

Tag reference	Static		Dynamic		
	Access Time Calculation (ms)		Tag Maximum Speed (m/s)		
	Read Time	Write Time	Read a UID	Read a Register*	Read or Write 10 Register*
XGHB320345	12 + 0.825 x N	12 + 5.6 x N	5.8	2.7	0.9
XGHB520246	12 + 0.825 x N	12 + 5.6 x N	7.1	4.0	0.8
XGHB90E340	12 + 0.825 x N	20 + 11.8 x N	7.1	4.0	0.8
XGHB211345	12 + 0.825 x N	19 + 4.1 x N	3.2	1.1	0.6
XGHB221346	12 + 0.825 x N	20 + 11.8 x N	4.2	2.6	0.5
XGHB123345	12 + 0.825 x N	20 + 11.8 x N	3	0.9	0.4
XGHB440245	7 + 2 x N	7 + 2.4 x N	3.5	2.5	1
XGHB320246	7 + 2 x N	7 + 2.4 x N	3.5	2.5	1
XGHB444345	9.25 + 0.375 x N	13 + 0.8 x N	4.8	2.7	1.8
XGHB440845	6 + 0.25 x N	6 + 0.25 x N	3.8	3.0	2.6
XGHB441645	6 + 0.25 x N	6 + 0.25 x N	3.8	3.0	2.6
XGHB443245	6 + 0.25 x N	6 + 0.25 x N	3.8	3.0	2.6

N: Number of 16-bit registers

*: with use of the “Auto read/write” function

Description of the Smart Antenna

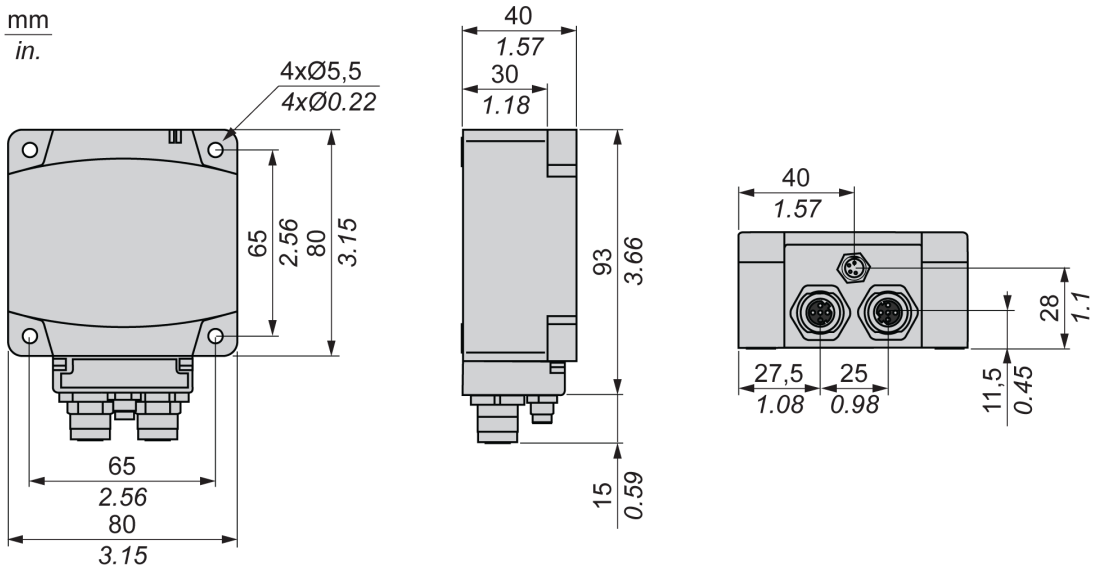
Presentation of the Smart Antenna

The figure presents the Smart Antenna:

No.	Description
1	TAG: Tag LED
2	COM: Communication LED
3	NS: Network Status LED
4	LK/SP: Ethernet communication port No. 1 LED
5	M12 socket, Ethernet port No. 1
6	M8 socket, 24 Vdc power supply
7	M12 socket, Ethernet port No. 2
8	LK/SP: Ethernet communication port No. 2 LED
9	MS : Ethernet Module Status LED

Dimensions

The figure shows the dimensions of the Smart Antenna:



Connecting the OsiSense XG Smart Antenna

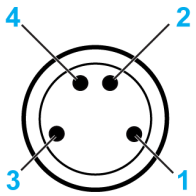
Introduction

The Smart Antenna is equipped with:

- a male M8 connector for the power supply,
- 2 female M12 D-coded connectors for Ethernet communication.

Power Supply Wiring

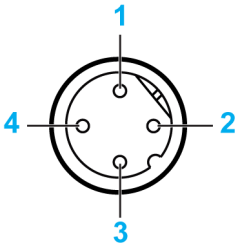
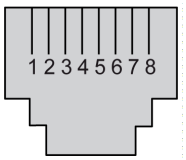
The table describes the M8 connector pinout:

M8 Connector	Pin No.	Signal	XZCP0941L• Wire Color
	1	+24 V ⎓	Brown
	2	Not connected	White
	3	0 V ⎓	Blue
	4	Not connected	Black

NOTE: Use a SELV or PELV power supply and fuse protection (1 A). The power supply used must be class II according to VDE 0106. The 0 V must be connected to the ground to increase EMC strength.

Communication Wiring

The table describes the M12 connectors pinout and the correspondence with the RJ45 connector of communication cables, page 22:

M12 Connector	M12 Pin	Signal	Description	RJ45 Pin	RJ45 Connector
	1	TD+	Transmit Data +	1	
	2	RD+	Received Data +	2	
	3	TD–	Transmit Data –	3	
	4	RD–	Received Data –	6	
	-	-	Not connected	4	
	-	-	Not connected	6	
	-	-	Not connected	7	
	-	-	Not connected	8	

Wiring Accessories

Introduction

The range of accessories is composed of power supply cables, communication cables, and Ethernet connection accessories.

Power Supply Cables

The table shows the range of power supply cables:

Description	Length	Reference
Pre-wired M8 connector	2 m *(6.56 ft)*	XZCP0941L2
	5 m *(16.4 ft)*	XZCP0941L5
	10 m *(32.8 ft)*	XZCP0941L10

Communication Cables

The table shows the range of communication cables:

Description	End Fittings	Length	Reference
Copper connecting cables, straight	1 x IP67 M12 4-pin connector and 1 x RJ45 connector	1 m *(3.28 ft)*	XGSZ12E4501
		3 m *(9.84 ft)*	XGSZ12E4503
		10 m *(32.8 ft)*	XGSZ12E4510
	2 x IP67 M12 4-pin connectors	1 m *(3.28 ft)*	XGSZ12E1201
		3 m *(9.84 ft)*	XGSZ12E1203
		10 m *(32.8 ft)*	XGSZ12E1210
		25 m *(82 ft)*	XGSZ12E1225
Copper connecting cables, elbowed	1 x IP67 M12 4-pin elbowed connector and 1 x RJ45 connector	3 m *(9.84 ft)*	XGSZ22E4503
		10 m *(32.8 ft)*	XGSZ22E4510
Ethernet copper cable (2 x 24 AWG shielded twisted pairs)	Connectors to install	300 m *(984.2 ft)**	TCSECN300R2
RJ45 connector	Conforms to EIA/TIA-568-D	-	TCSEK3MDS
M12 connector	Conforms to IEC 60176-2-101	-	TCSEK1MDRS

* The maximum length of Ethernet connecting cables made up in this way is 80 m *(262.5 ft)*.

Ethernet Connection Accessories

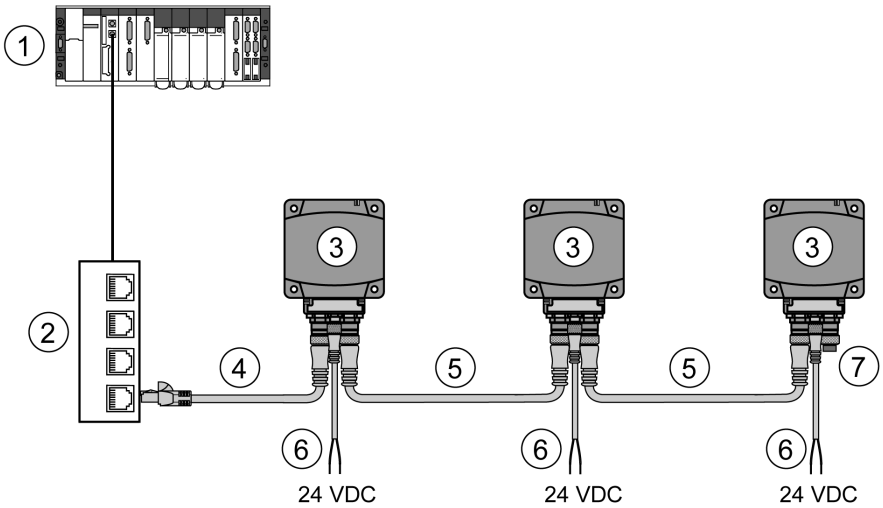
The table shows the range of Ethernet connection accessories:

Description	Reference
ConneXium M12 Ethernet switch IP67	TCSESU051F0
ConneXium Ethernet switch with loopback function	TCSESB•••••••• TCSESM••••••••
M12 female / RJ45 adaptor	TCSESAAF11F13F00
M12 connector cap for Smart Antenna	ASI67FACC1

Smart Antennas Wiring Example

Connection Diagram

Example of an Ethernet TCP/IP network setup with Smart Antennas:



1 PLC

2 Ethernet switch

3 Smart Antenna

4 Ethernet cable XGSZ12E45••

5 Ethernet cable XGSZ12E12••

6 Power supply cable XZCP0941L•

7 M12 connector cap ASI67FACC1 (2 caps are supplied with the Smart Antenna)

The maximum length of each segment is 80 m (262.5 ft).

In this example, the maximum bus length is 320 m (1050 ft):

- 80 m (262.5 ft) between the PLC and the Ethernet switch,
- 3 x 80 m (787.4 ft) between each Smart Antenna.

NOTE: It is possible to chain up to 32 Smart Antennas.

Installing the System

Aim of this Chapter

This chapter describes the procedure for installing the OsiSense XG Smart Antenna.

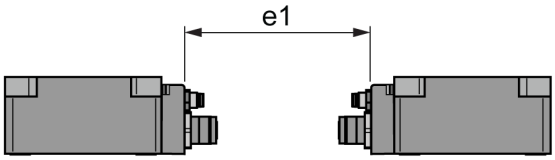
Installation Precautions

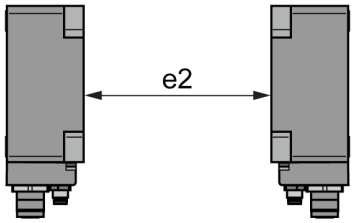
Distances Between Smart Antennas

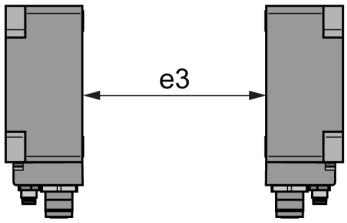
When 2 Smart Antennas are too close, there is a risk of mutual disturbance.

NOTICE
UNINTENDED OPERATION Follow the installation precautions given in this chapter on distances between 2 Smart Antennas. **Failure to follow these instructions can result in equipment damage.**

Distances between 2 identical Smart Antennas depend on the tag used:





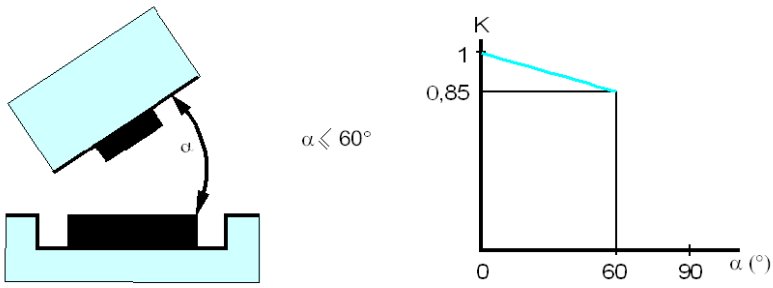


Minimum distances in mm (inches):

Tag reference	Minimum Distances in mm (inches)		
	e1	e2	e3
XGHB90E340 XGHB520246	430 (16.93)	750 (29.53)	280 (11.02)
XGHB221346	280 (11.02)	530 (20.86)	260 (10.24)
XGHB320•••	310 (12.20)	540 (21.25)	240 (9.45)
XGHB211345 XGHB123345	200 (7.87)	370 (14.57)	170 (6.69)
XGHB44••••	310 (12.20)	400 (15.75)	160 (6.29)

Angular Positioning

The angle between the Smart Antenna and the tag modifies the sensing distance according to the graph below:

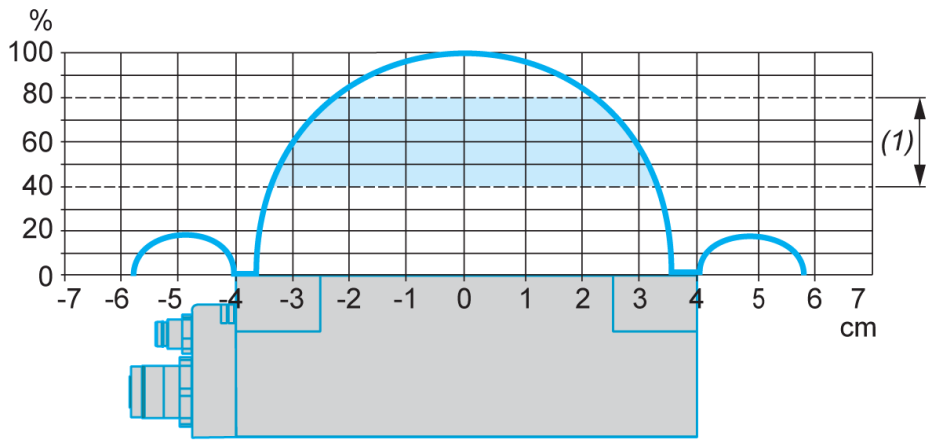


K = correction factor to be applied to the nominal sensing distance.

Sensing distance = nominal sensing distance x K.

Sensing Zones

The dialog zones of the Smart Antenna are circular. There is no recommended direction for the movement of the tag. The following diagram shows the dialog zones of the Smart Antenna:



(1) Movement zone consulted: between 0.4 and 0.8 of the nominal sensing distance.

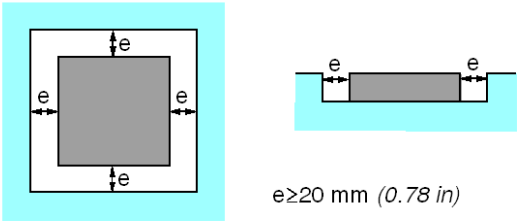
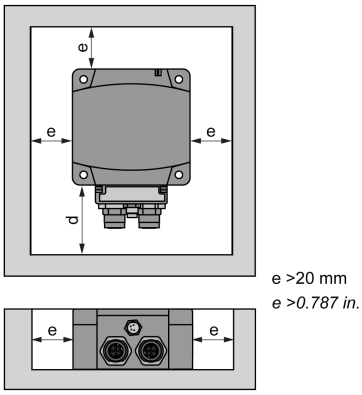
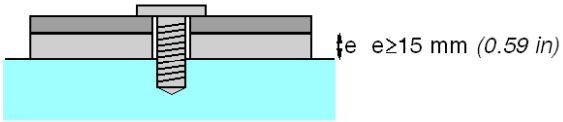
NOTE: Nominal sensing distance (Pn)

The conventional sensing distance does not take the dispersions (manufacturing, temperature, voltage, assembly in the metal) into account.

Mounting in the Metal

The presence of metal near the tags and the Smart Antenna affects the sensing distance (Reading/Writing distance).

The table shows the minimum assemblies allowed in a metal block:

References	Description
XGCS4901201 XGCS8901201 XGHB221346 XGHB44•••	The product is positioned in a steel block: 
XGCS850-C201	The Smart Antenna is positioned in a steel block:  **d** Depending on the connector size
XGHB90E340 XGHB123345 XGHB211345	No metallic piece is less than 25 mm (0.98 in.) from the tag.
XGHB32•••• XGHB52••••	The tag is fixed with an M4 steel screw (tightening torque = 1 Nm (8.85 lbf-in)). It is necessary to insert a non-metallic wedge between the tag and the metal tag: 

The table shows the effect on the nominal sensing distance when the Smart Antenna and the tag are assembled in metal according to the most unfavorable cases shown above:

Reference	Memory Size (bytes)	Dimensions	Reduced Sensing Distance with Presence of Metal	Nominal Sensing Distance
XGHB90E340	256	Badge of 85x58x0.8 mm (3.35x2.28x0.03 in.)	80 mm (3.15 in.)	100 mm (3.94 in.)
XGHB520246	112	∅ 50x3 mm (1.97x0.12 in.)		
XGHB221346	256	26x26x13 mm (1.02x1.02x0.51 in.)	33 mm (1.29 in.)	55 mm (2.16 in.)
XGHB320345	112	∅ 30x3 mm (1.18x0.12 in.)	56 mm (2.20 in.)	65 mm (2.56 in.)
XGHB320246	2000			
XGHB211345	256	∅ 18x12 mm	15 mm	20 mm

Reference	Memory Size (bytes)	Dimensions	Reduced Sensing Distance with Presence of Metal	Nominal Sensing Distance
		(0.70x0.47 in.)	(0.59 in.)	(0.78 in.)
XGHB123345	304	∅ 12x8 mm (0.47x0.31 in.)		
XGHB444345	3408	40x40x15 mm (1.57x1.57x0.59 in.)	34 mm (1.33 in.)	48 mm (1.89 in.)
XGHB440245	2000	40x40x15 mm (1.57x1.57x0.59 in.)	45 mm (1.77 in.)	65 mm (2.56 in.)
XGHB440845	8192	40x40x15 mm (1.57x1.57x0.59 in.)	28 mm (1.10 in.)	39 mm (1.53 in.)
XGHB441645	16384			
XGHB443245	32768			

Distances Between Tags

NOTICE

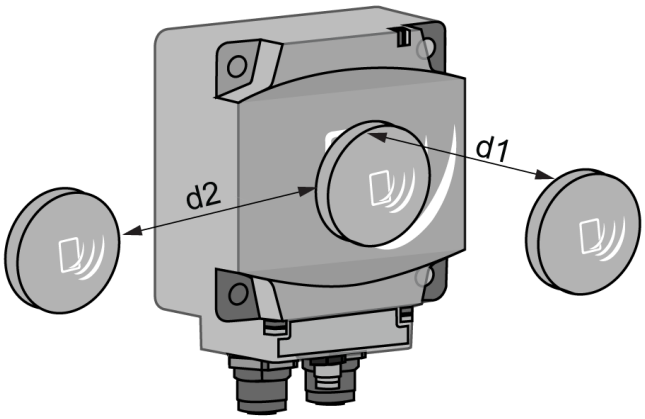
UNINTENDED OPERATION

Follow the installation precautions given in this chapter on distances between 2 tags.

Failure to follow these instructions can result in equipment damage.

NOTE: When 2 tags are too close, this may trigger dialog errors.

This figure illustrates the minimum distance between 2 identical tags:



Minimum distances between 2 identical tags according to their positioning:

Tag reference	Minimum Distances in mm (inches)	
	d1	d2
XGHB90E340 XGHB520246	140 (5.51)	110 (4.33)
XGHB221346	50 (1.97)	120 (4.72)
XGHB320345 XGHB440245 XGHB320246	60 (2.36)	190 (7.48)
XGHB211345 XGHB123345	20 (0.79)	120 (4.72)

Tag reference	Minimum Distances in mm (inches)	
	d1	d2
XGHB444345	40 (1.57)	70 (2.75)
XGHB440845 XGHB441645 XGHB443245	10 (0.39)	60 (2.36)

Electromagnetic Disturbances

NOTICE

UNINTENDED OPERATION

Do not install the Smart Antenna less than 300 mm (12 in) from a device generating electromagnetic disturbances (electric motor, solenoid valve...).

Failure to follow these instructions can result in equipment damage.

NOTE: Electromagnetic disturbances may block the dialog between the Smart Antenna and a tag.

IP Address Configuration

Introduction

IP address: Every item of equipment connected to an Ethernet network must have a unique IP address. This address makes it possible to refer to a specific unit.

Subnet mask: The subnet mask defines a range of IP addresses that can be accessed from an item of equipment.

The table describes the standard IP subnet masks:

Network Class	Host bits	Subnet mask
A	24	255.0.0.0
B	16	255.255.0.0
C	8	255.255.255.0

The table gives an example of accessible address ranges depending on the network class:

Network Class	Addresses	Accessible Addresses Ranges
B	IP: 192.168.0.1 Mask: 255.255.0.0	IP: 192.168.xxx.xxx
C	IP: 192.168.0.1 Mask: 255.255.255.0	IP: 192.168.0.xxx

NOTE: xxx represents a possible value from 0 to 255.

Address Configuration

The factory default address is 192.168.0.10.

The configuration of the IP address is made by setting parameters with:

- XGST2020 Handheld Terminal,

- IP Recovery Tool.

NOTICE
UNINTENDED EQUIPMENT DAMAGE • Do not use factory configured IP address for operation. • Assign a new IP address for operation. **Failure to follow these instructions can result in equipment damage.**

NOTE: Two or more Smart Antennas with identical IP address on the same network generate a duplicate IP condition (Smart Antenna Diagnostic LEDs, page 70).

Configuring IP Address with XGST2020 Handheld Terminal

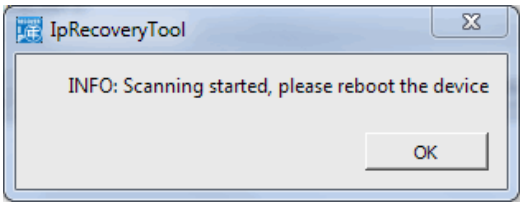
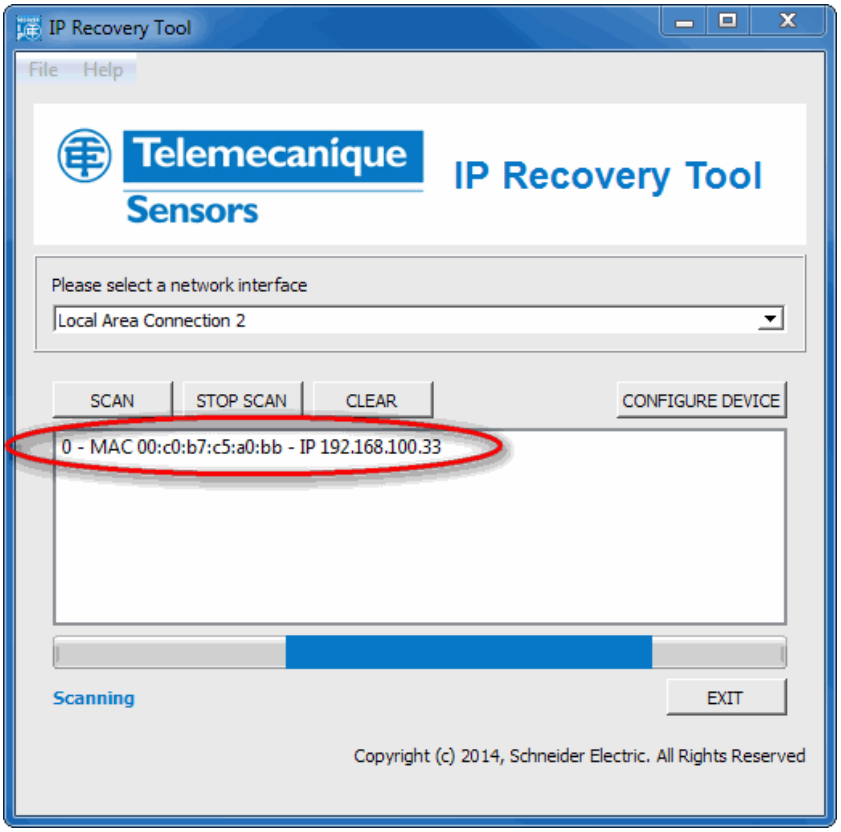
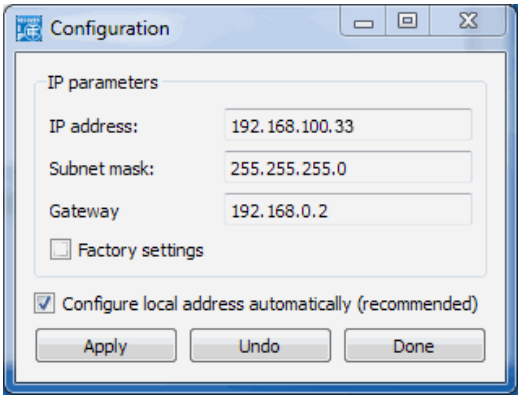
You can configure the IP parameters of the Smart Antenna with the XGST2020 Handheld Terminal. For more information, refer to documentation of the device, page 7.

NOTE: The IP address of the Smart Antenna must be known. If not, you must use the IP Recovery Tool (see below).

Configuring IP Address With IP Recovery Tool

Proceed as follow to retrieve and configure the IP address of a Smart Antenna:

Step	Action
1	Download and install on your PC the IP Recovery Tool software, page 7.
2	Connect a Smart Antenna to your PC with an Ethernet M12 / RJ45 cable (XGSZ12E4501).
3	Launch the IP Recovery Tool software.
4	Select in the list the network interface on which the Smart Antenna is connected to.
5	Click **SCAN**.

Step	Action
	Result: An information window is displayed: 
6	Reboot or power-up the Smart Antenna connected to the PC
7	Click **OK** to close the information window.
8	Wait until the MAC address and the IP address of the Smart Antenna is displayed in the scan result area. The scan can take 30 seconds to 2 minutes.  **NOTE:** If more than one Smart Antennas are connected to the PC, they are all displayed in the scan result area.
9	Click **STOP SCAN** after all Smart Antennas are detected.
10	Select in the scan result area the Smart Antenna to configure.
11	Click **CONFIGURE DEVICE**. **Result:** A configuration window is displayed: 

Step	Action
12	Set the new IP parameters of the Smart Antenna: • IP address • Subnet mask • Gateway
13	You can select the **Factory settings** check box to set the factory settings. **NOTE:** If you modify the values, the **Factory settings** check box becomes cleared.
14	If you clear the **Configure local address automatically (recommended)** check box, you must modify the network configuration of your PC to be compatible with the actual IP address range of the Smart Antenna.
15	Click **Apply** to validate the settings.
16	Click **Done** to close the configuration window.
17	Click **EXIT** to close the IP Recovery Tool software.
18	Reboot the Smart Antenna to apply the new IP parameters.

Operating Principles

Aim of this Chapter

This chapter describes the system operating principle based on memory zones.

Read/Write Operating Mode

Introduction

For read/write operations 2 operating modes are available:

- Static read/write: applications where the tag is stopped in front of the Smart Antenna.
- Dynamic read/write: applications where the tag does not stop in front of the Smart Antenna.

Static Read/Write

The controller must run cyclic scanning of the status of the Smart Antenna before sending read or write requests addressed to the internal memory of the tag.

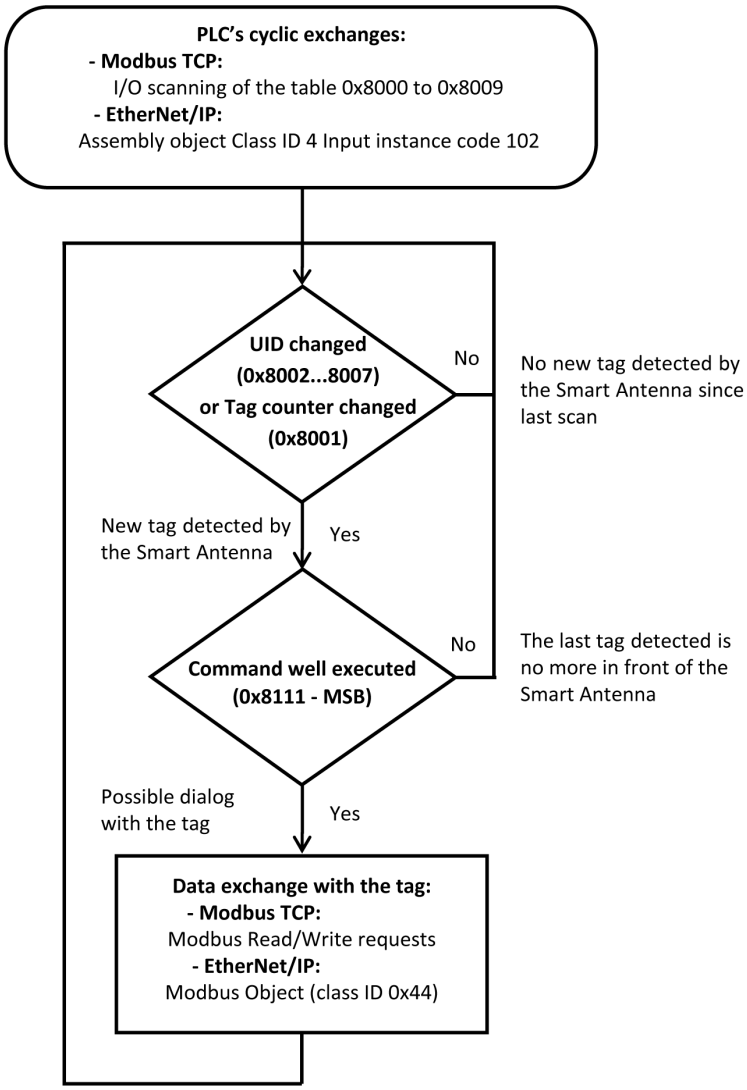
A table of holding registers in the system memory area of the Smart Antenna is dedicated to this function:

- Status register: a bit of this register is set to 1 when a tag is detected by the Smart Antenna.
- Tag counter: this register is incremented each time a new tag is detected by the Smart Antenna.
- UID: a group of 8 registers where the UID of the last tag detected by the Smart Antenna is stored.

The combination of these information gives the exact status of the system:

- Arrival of a tag in front of the Smart Antenna.
- New tag or same tag as previous one.
- Read/write operations in the tag possible or not.

This diagram illustrates static read/write operations:



Dynamic Read/Write

The Smart Antenna can be configured to run automatically read/write commands each time a new tag is detected. The results of the last commands are permanently accessible in the system memory of the Smart Antenna (Reading Table, page 39). Synchronization between PLC application program and tag presence is no more necessary.

First, the controller must send writing requests to the Smart Antenna to configure and activate the automatic R/W commands, page 36.

Then, the controller must run cyclic scanning of the reading table of the smart antenna:

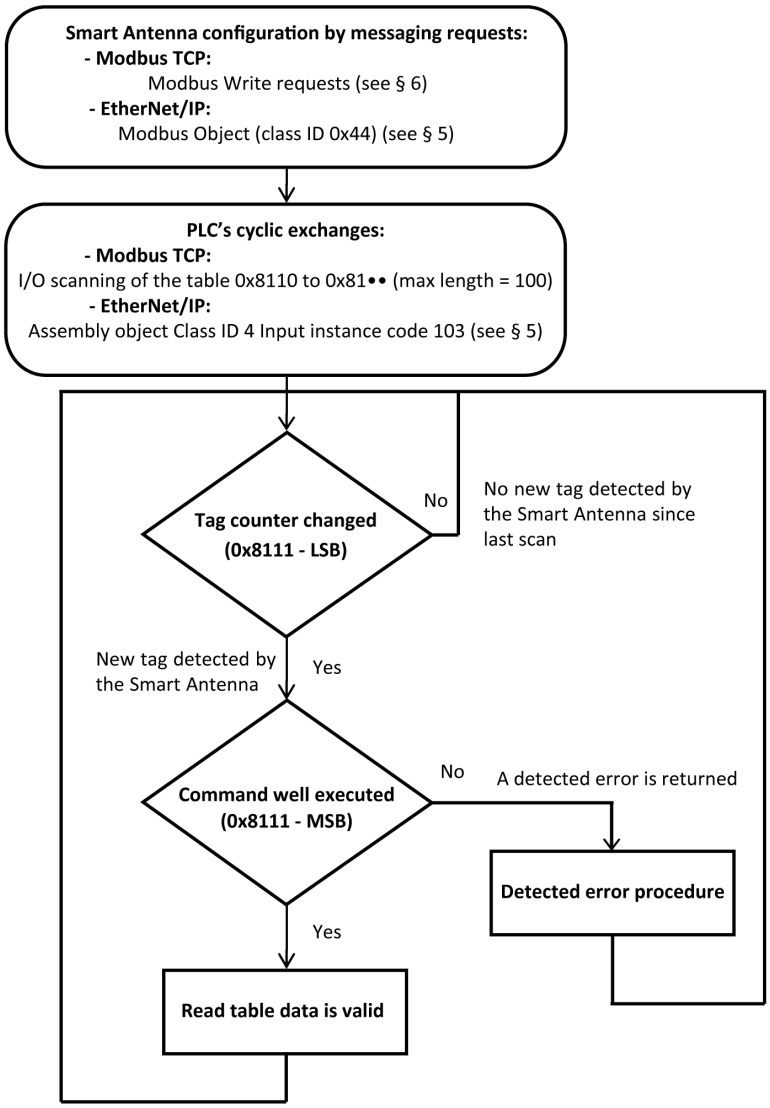
- First register: Status, a bit of this register is set to 1 when a tag is detected by the Smart Antenna.
- Second register: tag counter and detected error code.
- Third…X registers: results of read commands.

The combination of these information gives the exact status of the system:

- Arrival of a tag in front of the Smart Antenna.
- New tag or same tag as previous one.
- Data read from the last tag detected by the Smart Antenna.

All data will be overwritten by the arrival of the next tag.

This diagram illustrates dynamic read/write operations:



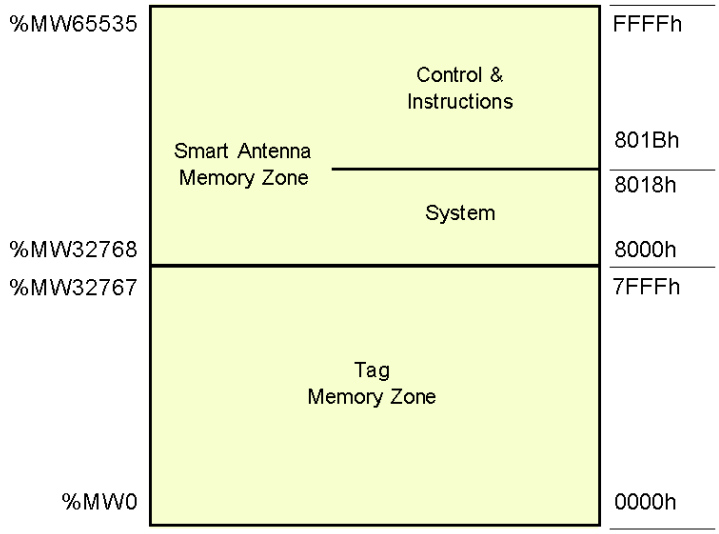
Memory Zones

Presentation

The addressing memory zone is divided into 2 zones:

- The tag Memory Zone, page 18
- The Smart Antenna memory zone:
  - System Zone, page 35,
  - Command/instructions zone, page 36.

Definition of the address zones of holding registers used:



Smart Antenna System Memory Zone

Description of the Zone

Composition of the system zone:

Register	Description	Access [1]	Protected
8000h	Tag family present / Tag system flags	R	No
8001h	Tag counter	R/W	No
8002...8009h	UID	R	No

[1]	R = Read, W = Write

Modifications to values in this zone are taken into account by the Smart Antenna immediately.

Register 8000h

Status:

MSB		LSB	
Tag family present Indicates the tag family while it is present. Reset when no longer present.		**Tag system flag** Real-time updating.	
Bit		Bit	
8	15693	0 (LSB)	Tag present
9	Icode	1	Initial parameter-setting phase following boot-up
A	14443A	2	Reserved
B	14443B	3	Reserved
C	Inside	4	Reserved
D	Reserved	5	Present configuration badge
E	Reserved	6	Reserved
F (MSB)	Reserved	7	Reserved

Register 8001h

Tag counter:

MSB	LSB
Incremented each time there is a new tag. RAZ at each power switch-on. Possible written access to predefine a value in the counter.	

Registers 8002h...8009h

UID:

MSB	LSB
Updated each time there is a new tag and valid if tag present.	

Each tag has a different single code (UID). This code is distributed in 16 bytes.

Smart Antenna Command/Instructions Memory Zone

General Description

The zone can activate the commands or operating modes and consists of:

Register	Table	Description	Access *	Protected
801Bh	Command	Activates operations such as initialization, automatic reading or writing, sleep mode, etc.	R/W	No
801C...80AFh	Reserved	Reserved	-	-
80B0...80FF	Instruction block	Sets parameters by up to 10 instructions, which are executed sequentially.	R/W	No
8100...810Fh	Reserved	Reserved	-	-
8110...817Fh	Reading table	Stores the results of the tag-reading operations and monitors the execution of the instructions.	R	No
8190...81E6h	Writing table	Stores the data which are to be written in the tags.	R/W	No
81E7...FFFFh	Reserved	Reserved	-	-

*: R = Read, W = Write

801Bh Register: Command

This register executes the following commands:

- **Reset:**
  - Reinitialization of the default factory adjustments
  - Launching the initialization sequence
  - The Command/instructions memory zone is reset to zero
  - The sleep mode is deactivated
- **Init:**
  - Smart Antenna reinitialization
  - Launching the initialization sequence
  - The Command/instructions memory zone is reset to zero
  - The sleep mode is deactivated
- **Sleep Mode:**
  - activation/deactivation of the Sleep Mode,

  - Emission of the electromagnetic field of the Smart Antenna is activated only when receiving a reading or writing request. This mode reduces the Smart Antenna consumption and frees it from interferences when the Smart Antenna is close to another one.
- **Execution of the instructions block:**
  - Defines the occurrence of executing the instructions block in the Smart Antenna
  - Unit execution command: the instruction block is executed once after detecting the first tag
  - Automatic execution command: the instruction block is executed at each tag detection up to the next reset or when the Smart Antenna is switched off

  NOTE: To be able to use the execution commands of the instructions block, the "Sleep" mode must be deactivated. Since this mode cannot detect the presence of a tag in the dialog zone.

Command	Register for Activa-tion	Register for Deactivat-ing the Command	Comment
Reset	4040h	-	After executing the command, the 801Bh register automatically retrieves its default value.
Init	2020h	-	
Sleep Mode	1010h	1000h	After restarting the Smart Antenna, the Sleep Mode is deactivated.
Execution of the instructions block	0101h	0100h	Single execution when a tag is present in front of the Smart Antenna.
	0202h	0200h	Execution performed each time a new tag is present in front of the Smart Antenna.

NOTE: After restarting the Smart Antenna, the 801Bh register automatically retrieves its default value.

80B0...80FFh Register: Instruction Block

The instructions block predefines up to 10 instructions. The instructions are executed (in the ascending order) when a tag is detected by the Smart Antenna.

Each instruction consists of 8 16-bit registers which define the parameters associated with it. The number of registers used to set the parameters of different instructions varies. The registers that are not used must be defined at 0000h.

The first register of each instruction is divided into 2 parts:

- The high-weight byte defines the type of instruction to be executed.
- The low-weight byte defines the number of registers processed by the instruction.

Data entry or instructions output is contained in the 2 tables:

- A writing table containing the data to be written in a writing instruction
- A reading table containing:
  - Diagnostic information associated with the execution of the instructions block
  - Data read in a reading instruction

Reading Instruction (C1)

Instruction structure:

Register		Instruction Field	Type	Value	Comment
1st	MSB	Instruction code	Byte	C1h	C1: **C**opy **I**n

Register		Instruction Field	Type	Value	Comment
	LSB	Number of registers	Byte	01...40h	Number of registers to be read
2nd		Address	Word	0000... FFFFh	Address of the first register to be read from the Smart Antenna or tag
Reserved			Word	0000h	-
Reserved			Word	0000h	-
Unused			Word	0000h	System registers to be defined at 0
			Word	0000h	
			Word	0000h	
			Word	0000h	

Writing Instruction (C0)

Instruction structure:

Register		Instruction Field	Type	Value	Comment
1st	MSB	Instruction code	Byte	C0h	C0: **C**opy **O**ut
	LSB	Number of registers	Byte	01...40h	Number of registers to be written
2nd		Address	Word	0000... FFFFh	Destination address of the first register to be written from the Smart Antenna or tag
Reserved			Word	0000h	-
Reserved			Word	0000h	-
Unused			Word	0000h	System registers to be defined at 0
			Word	0000h	
			Word	0000h	
			Word	0000h	

Copying instruction (CD)

Instruction structure:

Register		Instruction Field	Type	Value	Comment
1st	MSB	Instruction code	Byte	CDh	C0: **C**opy **D**ata
	LSB	Number of registers	Byte	01...FFh	Number of registers to be written
2nd		Data	Word	0000... FFFFh	Value to be copied
3rd		Address	Word	0000...7FF-Fh	First memory zone address to be written
4th		Iteration	Word	0001...1FF-Fh	Number of iterations to be executed
Unused			Word	0000h	System registers to be defined at 0
			Word	0000h	
			Word	0000h	
			Word	0000h	

8110...8174h Register: Reading Table

The reading table stores the consecutive result in a reading instruction (C1) as well as review the execution review of the instructions block (2 registers). Reading this review monitors progress of the instructions sequence.

Structure of the reading table:

Regis-ter	Description		
	MSB		LSB
	PF Quartet	Pf Quartet	
8110h	Smart Antenna status: image of the Register 8000h, page 35		
8111h	Instruction no.	Detected error code	Tag counter: image of the Register 8001h, page 36.
8112h	Data read as 1, 1st reading instruction		
8113h	Data read as 2, 1st reading instruction		
...	...		
...	Data read as N, 1st reading instruction		
...	Data read as 1, 2nd reading instruction		
...	Data read as 2, 2nd reading instruction		
...	...		
...	Data read as N, 2nd reading instruction		
...	Data read as 1, nth reading instruction		
...	Data read as 2, nth reading instruction		
...	...		
...	Data read as N, nth reading instruction		
...	...		
8174h	...		

NOTE: All reading instructions must not exceed the table capacity of 100 registers.

Description of the 8111h register:

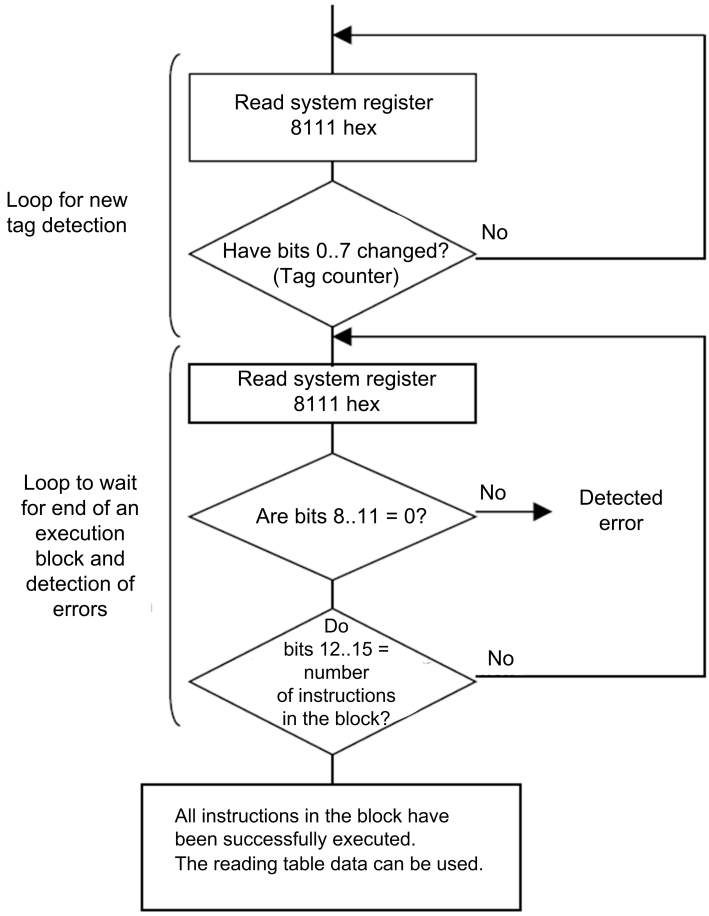
Bit	Signification	Description
15...12	Instruction no.	Number of the last instruction executed without detected error, such as "Detected error in the 3rd block instruction, therefore, the instruction no. = 2h"
11...8	Detected error codes	Modbus detected error codes: • 1h: unknown function code or incorrect request format • 2h: incorrect address, prohibited or protected zone or address not lying in the tag memory zone • 3h: incorrect data. Too much data in the frame or insufficient or quantity = 0 or incompatible data • 4h: execution fault detected (in reading, writing, or tag missing)
7...0	Tag counter	image of the Register 8001h, page 36.

NOTE: For example, if the 8111h register has the value 2409h, it means:

- 2h: Detected error in the 3rd block instruction.
- 4h: execution fault detected (in reading, writing, or tag missing)
- 09h: 09 tags have been detected (since the last RAZ of the counter).

Monitoring the Execution of the Instructions Block

Reading the 8111h system register of the Smart Antenna controls the execution of the instructions block:



8190...81E6h Register: Writing Table

The writing table stores the data to be written in a writing instruction.

Structure of the writing table:

Regis-ter	Description
8190h	Data to be written as 1, 1st written instruction
8191h	Data to be written as 2, 1st written instruction
...	...
...	Data to be written as N, 1st written instruction
...	Data to be written as 1, 2nd written instruction
...	Data to be written as 2, 2nd written instruction
...	...
...	Data to be written as N, 2nd written instruction
...	...

Regis-ter	Description
...	Data to be written as 1, nth written instruction
...	Data to be written as 2, nth written instruction
...	...
...	Data to be written as N, nth written instruction
...	...
81E6h	...

Application Example

In the following example, you define an instruction block containing 3 instructions:

- A reading instruction of 3 registers at the 0001h address
- A writing instruction of 2 registers at the 0010h address
- A reading instruction of 4 registers at the 0020h address

Definition of the instructions block:

Address	Value		Instruction no.
	MSB	LSB	
80B0h	C1h	03h	1
80B1h	0001h		
80B2...80B7h	0000h		
80B8h	C0h	02h	2
80B9h	0010h		
80BA...80BFh	0000h		
80C0h	C1h	04h	3
80C1h	0020h		
80C2...80C7h	0000h		

Definition of the writing table (data to be written in a writing instruction):

Address	Value	Instruction Associated
8190h	For example, FEFEh	2
8191h	For example, 0A0Bh	

Setting the parameters to activate the commands for each tag movement:

Address	Value	Instruction Associated
801Bh	0202h	Executing the instruction block at each new tag

Data received in the reading table after executing the instructions block:

Ad-dress	Value		Instruction Associated
	MSB	LSB	
8110h	Smart Antenna status		-
8111h	30h	01h	Composition: • 30h (MSB) = 3 instructions executed without detected error • 01h (LSB) = 1st tag detected by the Smart Antenna
8112h	0001h register content		Result of instruction number 1 (reading 3 registers)

Address	Value		Instruction Associated
	MSB	LSB	
8113h	0002h register content		
8114h	0003h register content		
8115h	0020h register content		Result of instruction number 3 (reading 4 registers)
8116h	0021h register content		
8117h	0022h register content		
8118h	0023h register content		

Example of data received in the reading table after executing the instructions block containing detected errors:

Address	Value		Instruction Associated
	MSB	LSB	
8110h	Smart Antenna status		-
8111h	14h	01h	Composition: • 14h (MSB) = execution of the instructions block was stopped due to a dialog detected error with the tag in instruction number 2 (instruction number 1 was executed correctly and instruction number 3 was not executed) • 01h (LSB) = 1st tag detected by the Smart Antenna
8112h	0001h register content		Result of instruction number 1 (reading 3 registers)
8113h	0002h register content		
8114h	0003h register content		

Definition of an instruction block that can delete the first 50 registers in each tag which is to be shown in front of the Smart Antenna:

Address	Value	Instruction Associated
80B0h	CD0Ah	CD: Copy Data / 0Ah = 10 registers deleted per iteration
80B1h	0000h	Filling with the 000h value
Address	0000h	First memory zone address to be written = 0000h
Iteration	0005h	Number of iterations to be executed = 5

EtherNet/IP Communications Support

Introduction

This chapter describes how a Smart Antenna can be accessed from other devices on an EtherNet/IP fieldbus network.

Object Model

Introduction

This section describes the object model for the EtherNet/IP NIM. For general information about the object model for a particular EtherNet/IP device, refer to ODVA specifications.

About the Object Model

Introduction

An EtherNet/IP node is modeled as a collection of objects. Each object provides an abstract representation of a particular component within a product.

An object model defines the device's:

- I/O data format
- Configurable parameters

The above information is made available to other vendors through the EDS of the device.

This chapter describes the implemented objects of the Smart Antenna in terms of:

- Supported class attributes
- Supported class services
- Supported instance attributes
- Supported instance services

Further details can be found in Chapter 5 of [28] The CIP Networks Library Volume 2 EtherNet/IP Adaptation of CIP.

Addressing Object Attributes

Objects: Objects provide services and implement behaviors.

Attributes: Attributes (object characteristics) for particular objects are addressed with integer values that correspond to this hierarchy:

- MAC ID (node ID)
- Class ID
- Instance ID
- Attribute ID

Supported Objects

This table lists the EtherNet/IP objects supported by the Smart Antenna:

Object Class	Class ID	Instance ID	Messages	Description
Identity Object	1	1	Explicit	This object returns the device type, vendor ID, serial number, and so on.
Message Router Object	2	1	Explicit	This object returns information about message router implementation.
Assembly Object, page 44	4	0x96, 0x66, 0x67 (150, 102, 103)	Implicit I/O or explicit	This object provides a collection of other attributes of object.
Connection Management Object	6	0x01(1)	Explicit	This object allows explicit messages to be conducted.
Port Object	0xF4 (244)	1	Explicit	This object returns information about the Ethernet port.
TCP/IP Interface Object	0xF5 (245)	1	Explicit	This object defines the number of IP address configuration options for the device.
Ethernet Link Object	0xF6 (246)	1	Explicit	This object tracks configuration and diagnostics information for the Ethernet port.
Modbus Object, page 45	0x44 (68)	1	Explicit	This object translates EtherNet/IP messages into Modbus requests (code function 0x3 and 0x10).

Assembly Object (Class ID 4)

Introduction

The assembly object groups different attributes (data) from a variety of application objects into a single attribute that can be moved with a single message. This message provides the I/O data and status of the Smart Antenna. Assembly objects can be used to bind input data or output data, as defined from the network's perspective. (That is, an *input* produces data on the network and an *output* consumes data from the network.) For the Smart Antenna assembly object:

- The class ID is 4.
- The instance codes are 150 for the output instance, 102 and 103 for the input instances.

Class Attributes (Instance 0)

The assembly object supports these class attributes:

Attribute ID	Name	Access	Description
0x01	Revision	R	This attribute returns the revision of the CIP object (0x02).
0x02	Max Instance	R	This attribute returns the maximum value of the instance number (102).
0x03	Num Instances	R	This attribute returns the number of class instances. The value is 2.
0x06	Max. Class Attribute	R	This attribute returns the numeric value of the highest class attribute (7).
0x07	Max. Instance Attribute	R	This attribute returns the numeric value of the highest instance attribute (4).

Class Services

The assembly object supports these class services:

Service Code	Name	Description
0x0E	Get Attribute Single	This service returns the value of the specified attribute.

Instance Codes

The Smart Antenna provides 3 instances of the assembly object class:

Instance ID	Access	Size (Bytes)	Description
150	R/W	2	Tag counter (Register 8001h, page 36)
102	R	20	General status (Registers 8000...8009h, Smart Antenna System Memory Zone, page 35)
103	R	200	Read table of 100 registers (8110...814Fh Register: Reading Table, page 39)

NOTE: Only one Input Assembly (102 or 103) can be used at a time.

Instance Attributes

The assembly object supports these instance attributes:

Attribute ID	Name	Access	Description
1	Number of members	R	This attribute returns a register value of the number of members in the instance.
2	Member list	R	This attribute is an array of structures in which each structure represents one member and consists of: • *Member data size*: a word containing the member data size (in bits) • *Member path size*: a word containing the byte size of the subsequent EPATH: ◦ 0: unused space between members ◦ 0x09: actual members • *Member path*: the EPATH representing the member (For example, "20 04 24 65 30 28 01" is member 1 of instance 101.)
3	Instance data	R/W	This attribute returns instance data as an array of bytes. Access is: • *Read (only)*: input data assemblies • *Read/write*: output data assemblies
4	Instance data size	R	This attribute returns a register representing the instance data size in bytes. (The size depends on the particular I/O modules configured on the bus.)

Instance Services

The assembly object supports these instance services:

Service Code	Name	Description
0x0E	Get Attribute Single	This service returns the value of the specified attribute.
0x010	Set Attribute Single	This service modifies an assembly object instance attribute value.
0x018	Get Member	This service reads a member of an assembly object instance.
0x019	Set Member	This service modifies a member of an assembly object instance.

Modbus Object (Class ID 0x44)

Introduction

The Modbus object is assigned a vendor-specific class ID of 68 (0x44). The Modbus object is an application object that provides the read/write requests of the Smart Antenna memory zones. For the Smart Antenna Modbus object:

- The class code is 0x44 (68).
- The single supported instance is 1.

Instance Services

The Modbus object supports these instance services:

Service Code	Name	Description
0x4E	Read holding registers	This service sends a read request of the specified registers (123 words maximum).
0x50	Write holding registers	This service sends a write requests of the specified registers (123 words maximum).

Service Code 0x4E Description

The table describes the service parameters of the read holding registers request:

Name	Data Type	Description	Semantics of Values
Starting address	UINT	Offset in table to begin reading from[1]	Zero based
Quantity of holding registers	UINT	Number of holding registers to read[1] (Max number = 123)	-

[1]The request parameter is little endian. The Modbus protocol is big endian. You may have to swap bytes depending on the Modbus subsystem implementation.

The table describes the service parameters of the read holding registers response:

Name	Data Type	Description	Semantics of Values
Holding register values	Array of 16-bit word[1]	Holding register values read[2]	-

[1]The data is returned as 16-bit entities for each register. The actual data type of the values is unknown.

[2]The response data is little endian. The Modbus protocol is big endian. You may have to swap bytes depending on the Modbus subsystem implementation.

Service Code 0x50 Description

The table describes the service parameters of the write holding registers request:

Name	Data Type	Description	Semantics of Values
Starting address	UINT	Offset in table to begin writing to[1]	Zero based
Quantity of outputs	UINT	Number of output registers to write[1] (123 maximum)	-
Output values	Array of 16-bit word	Output register values	-

[1]The request parameter is little endian. The Modbus protocol is big endian. You may have to swap bytes depending on the Modbus subsystem implementation.

The table describes the service parameters of the write holding registers response:

Name	Data Type	Description	Semantics of Values
Starting address	UINT	Offset in table where writing began[1]	Zero based
Quantity of outputs	UINT	Number of outputs forced[1]	-

[1]The response parameters are little endian. The Modbus protocol is big endian. You may have to swap bytes depending on the Modbus subsystem implementation.

Unity Pro: EtherNet/IP Application Example

Introduction

This example illustrates the configuration of a Smart Antenna on an EtherNet/IP network to communicate with a Modicon M340 PLC on Unity Pro.

Presentation

Overview

This example illustrates the Smart Antenna on an EtherNet/IP network to communicate with a Modicon M340 controller on Unity Pro.

It is a walkthrough for the configuration of the Smart Antenna with the following steps:

- Create the required Modicon M340 automation platform on Unity Pro
- Configure the Smart Antenna
- 1 command examples

NOTE: This example will not provide explanations on how to install the hardware, refer to the document of the controller for this purpose.

Hardware Requirement

The hardware required to set up this example is the following:

- A Modicon M340 automation platform
- A BMXNOC0401 Ethernet module
- Smart Antenna

Software Requirement

The software required to set up this example is the following:

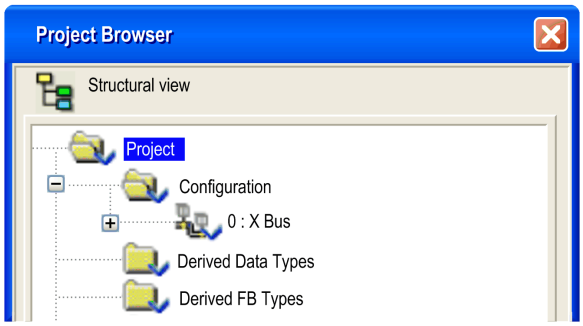
- Unity Pro (version 7.0 or better)

EDS file (XGCS850_V21.eds) can be downloaded from www.tesensors.com or from the USB memory key delivered with the Smart Antenna.

Creating a Project

Procedure

Use Unity Pro to create a new project:

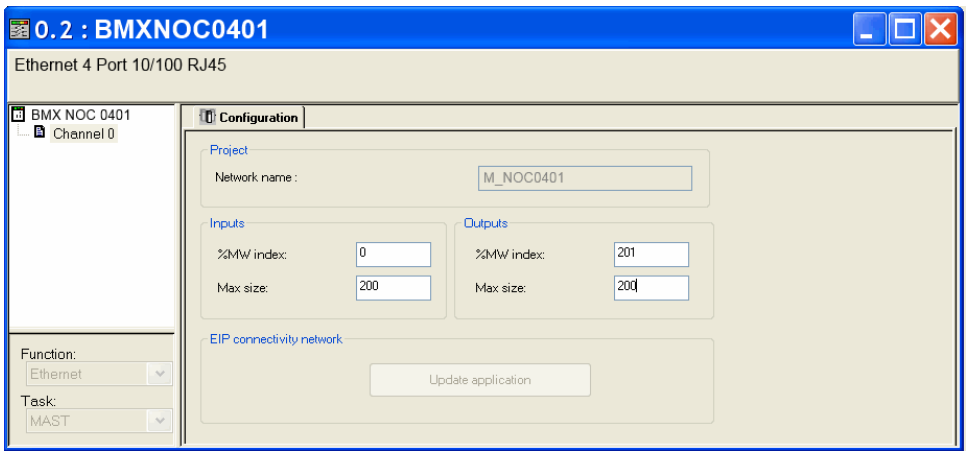
Step	Action
1	Launch Unity Pro.
2	In the Unity Pro main menu, select **File > New...**. The **New Project** window opens displaying a list of controller types.
3	In the **New Project** window, open the Modicon M340 sub-list and select the controller BMXP342020.
4	Click **OK**. The **Project Browser** opens: 
5	In the **Project Browser**, double-click **PLC Bus**. Unity Pro displays: • The **Hardware catalog**, and

Step	Action
	• A **PLC Bus** window with the selected CPU in the second position (slot 0) and a BMXCPS2000 power supply in the first position
6	In the **Hardware catalog**, use your mouse to drag a BMXNOC0401 EtherNet/IP communication module from the **Communication** section to a position in the backplane. In this example, the module is placed in the third position (slot 1). Result: A windows appears. You can modify the proposed module name **M_NOC0401**. **Note:** After the module name is entered, the module name cannot be edited.
7	To open the configuration window for the BMXNOC0401, do one of the following: • double-click the left mouse button on the BMXNOC0401 module in the **PLC Bus** window above, or • Click the right mouse button on the module, then select **Open Module...** in the popup menu The module configuration window opens, where you can configure the properties for the BMXNOC0401.

Configuring the BMXNOC0401 EtherNet/IP Communication Module

Setting Input and Output Memory Addresses and Naming the Module

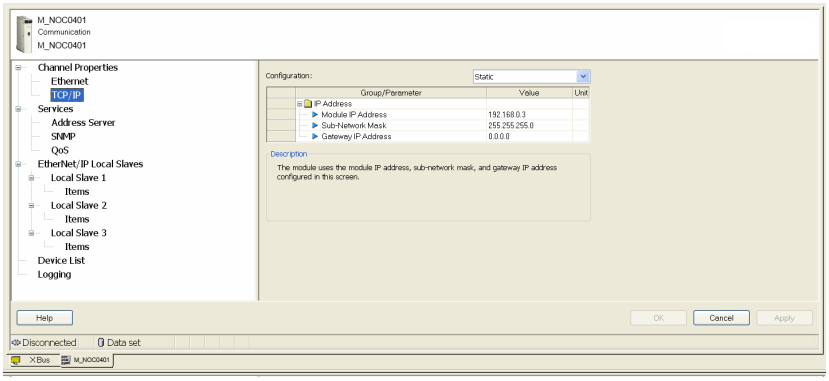
The **Configuration** page looks like this:



In the **Configuration** page, perform the following steps to set addresses and sizes for both inputs and outputs:

Step	Action
1	In the **Input area** and **Output area**, type in the size and starting position of both the inputs and outputs. These values can be edited later. For this example, the following values are entered: In the **Input area**: • In the **%MW index** field, type in a starting address for inputs - in this example: **0**. • In the **Max size** field, type in the maximum number of 16-bit words dedicated to inputs -in this example: **110**. In the **Output area**: • In the **%MW index** field, type in a starting address for outputs - in this example: **110**. • In the **Max size** field, type in the maximum number of 16-bit words dedicated to outputs - in this example: **20**. **Notes**: • The inputs and outputs can be located at any available address, and do not need to be located in adjacent areas. It is important only that the space allocated to inputs and outputs do not overlap • The specified %MW range for both inputs and outputs must be available in the CPU. For more information, refer to the Unity Pro help file topic *Processor Configuration Screen*.
2	In Unity Pro, select **Edit > Validate** (or click the **Validate** button) to save the address and size settings for inputs and outputs.
3	In the **EIP connectivity network** area, click the **Update application** button:

Configuring the BMXNOC0401 Module Address

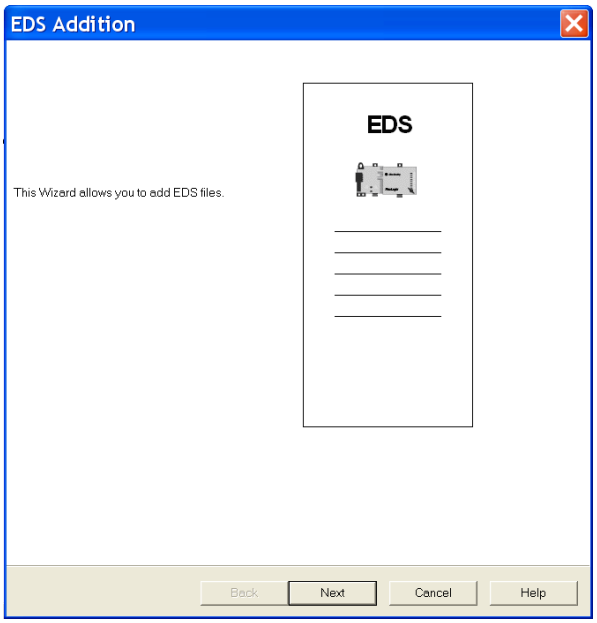
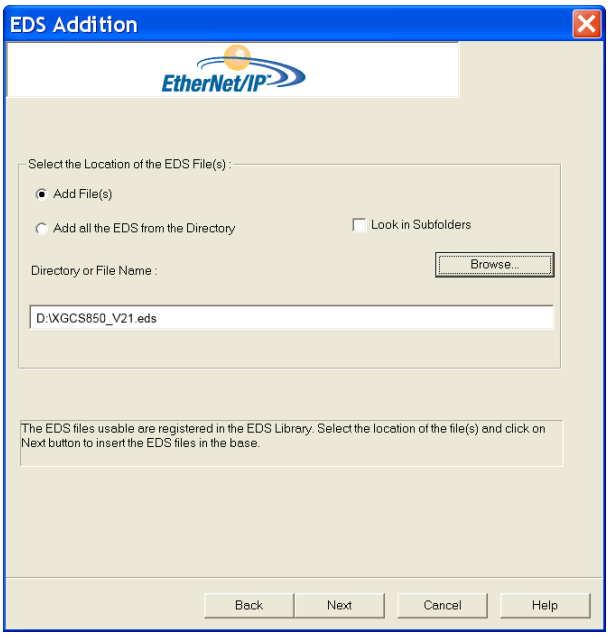
Step	Action
1	Select **Tools > DTM Browser**.
2	Double-click the **M_NOC0401** Ethernet module.
3	In the **Channel Properties** entry, click the **TCP/IP** subentry. 
4	Double-click the **Module IP Address** and set the IP address to `192.168.0.3` (master address) then press `Enter`.
5	Click **Apply**.

Configuring the Ethernet Smart Antenna

Adding the Ethernet Smart Antenna EDS File

Follow this step if you have not added the Smart Antenna EDS file before:

Step	Action
1	Click **Tools > DTM Browser**.
2	In the **DTM Browser**, right-click the **M_NOC0401** Ethernet module. Click **Device menu > Additional functions > Add EDS to library**.

Step	Action
	The **EDS Addition** window appears: 
3	Click **Next**.
4	Click **Browse** and browse your computer folders to the location of the file `XGCS850_V21.eds` select the file and click **Select**. 
5	Click **Next**.
6	Click **Next**.
7	Click **Finish**.
8	Click **Tools** > **Hardware Catalog**.
9	In the **Hardware Catalog** window, select the **DTM Catalog** tab and click **Update**.

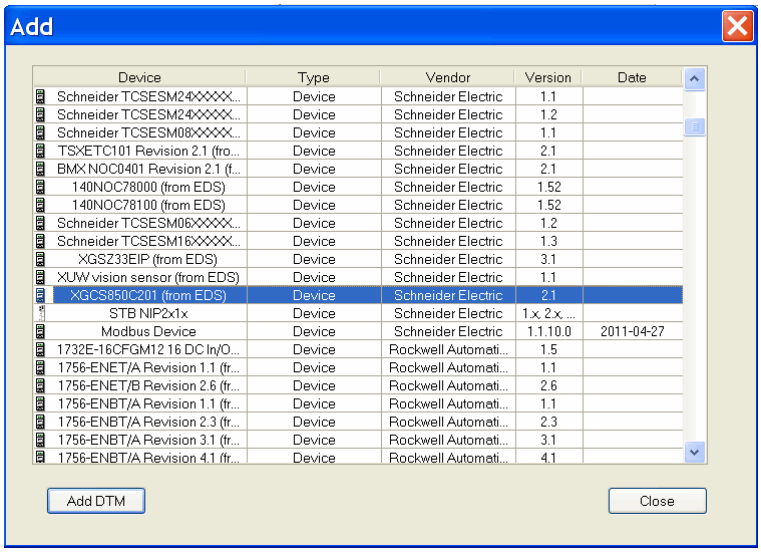
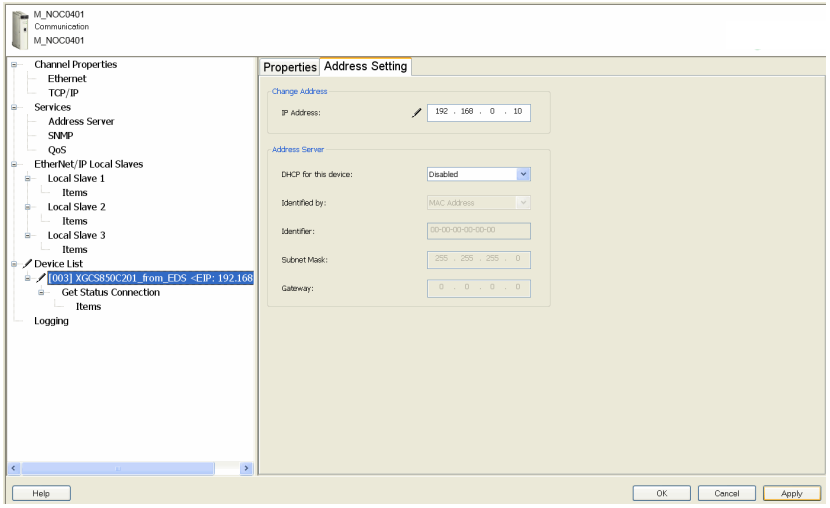
Adding and Configuring the Ethernet Smart Antenna Devices

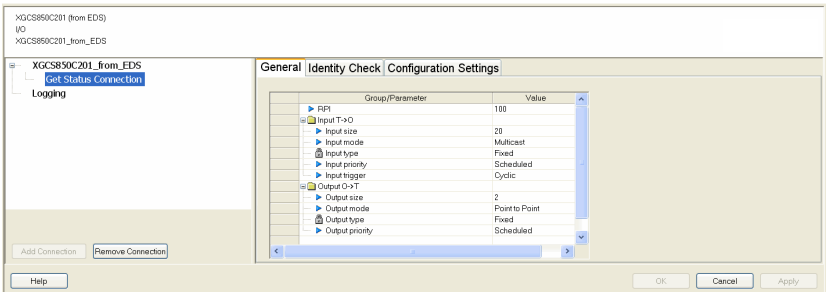
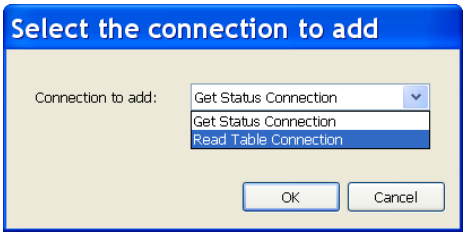
To communicate on EtherNet/IP network, the Smart Antenna uses one of the 2 following connections:

- the **Get Status Connection** (created automatically)

- the **Read Table Connection**

Follow this step to add and configure a Smart Antenna:

Step	Action
1	In the **DTM Browser** window, right-click the **M_NOC0401** Ethernet module and click **Add...**.
2	Select the **XGCS850C201** device in the list and click **Add DTM**: 
3	Click **Ok**.
4	In the **M_NOC0401** Ethernet module configuration window, click the Smart Antenna and select the **Address Setting** tab: 
5	Click **IP Address** and set the IP address of the Smart Antenna. (factory default IP address is 192.168.0.10). Press `Enter`.
6	Click **Apply**.

Step	Action
7	In the **DTM Browser** window, double-click the new device. This window appears: 
8	Select the **Get Status Connection** entry.
9	Click **Remove Connection**.
10	Click **Add Connection**.
11	Select **Read Table Connection** in the list and click **Ok**: 
12	Click **Apply**.
13	Click **Build > Rebuild All Project**. Result: The Smart Antenna is now configured to communicate on EtherNet/IP network.

Read Application Example

Introduction

This example describes the implementation of the Modbus object, page 45 for reading 123 registers in the tag memory area using the **DATA_EXCH** function. Refer to the Unity Pro online help for more information about explicit message.

Example

```
(* EtherNET/IP Explicit Message Example : Read Modbus Object *)

IF START and not TableGest[0].0 THEN


        (*TableRecep:=0;*)
        MOVE_INT_ARINT(0,TableRecep);    (* RAZ Reception table *)
        TableGest[2]:= 5;                (* TIMEOUT BASE 100ms *)
        TableGest[3]:= 10;               (* Length of data ToSend parameter, in Bytes *)

        DataToSend[0]:= 16#024E;         (* CIP request service information *)
        DataToSend[1]:= 16#4420;         (* CIP request class information *)
        DataToSend[2]:= 16#0124;         (* CIP request instance information *)
        DataToSend[3]:= 16#0001;         (* address of the first word to be read*)
        DataToSend[4]:= 16#007B;         (* Number of word to be read*)


        DATA_EXCH (ADR := ADDM('0.1.0{192.168.0.10}UNC.CIP'),
             TYP := 16#01,
             EMIS := DataToSend,
             GEST := TableGest,
             RECP => TableRecep);

End_IF;
```

START is a boolean variable to launch the read command.

CIP Request Description

The **DataToSend** variable identifies the type of explicit message and the CIP request:

Variable	Description	Value (hex)
`DataToSend [0]`	CIP request service information: • High byte = request size in registers: 16#02 (2 decimal) • Low byte = service code: 16#4E (78 decimal)	16#024E
`DataToSend [1]`	CIP request class information: • High byte = class: 16#44 (68 decimal) • Low byte = class segment: 16#20 (32 decimal)	16#4420
`DataToSend [2]`	CIP request instance information: • High byte = instance: 16#01 (1 decimal) • Low byte = instance segment: 16#24 (36 decimal)	16#0124
`DataToSend [3]`	Starting register (for example, %MW01): • High byte = 16#00 (0 decimal) • Low byte = 16#01 (1 decimal)	16#0001
`DataToSend [4]`	Number of registers to read: • High byte = 16#00 (0 decimal) • Low byte = 16#7B (123 decimal)	16#007B

The **TableGest** variable identifies the communication management table:

Variable	Description	Value (hex)
`TableGest [0]`	Data managed by the system: • High byte = exchange number • Low byte = activity bit)	-
`TableGest [1]`	Data managed by the system: • High byte = operation report • Low byte = communication report	-
`TableGest [2]`	Timeout (100 ms base)	16#0005
`TableGest [3]`	Length of data to send (in bytes)	16#000A

The **TableRecep** variable is the reception table:

Variable	Description
`TableRecep[0]`	Received data (value of the 123 registers read)
...	
`TableRecep [122]`	

RSLogix: EtherNet/IP Application Example

Introduction

This example describes the configuration of a Smart Antenna on an EtherNet/IP network to communicate with an Allen Bradley PLC.

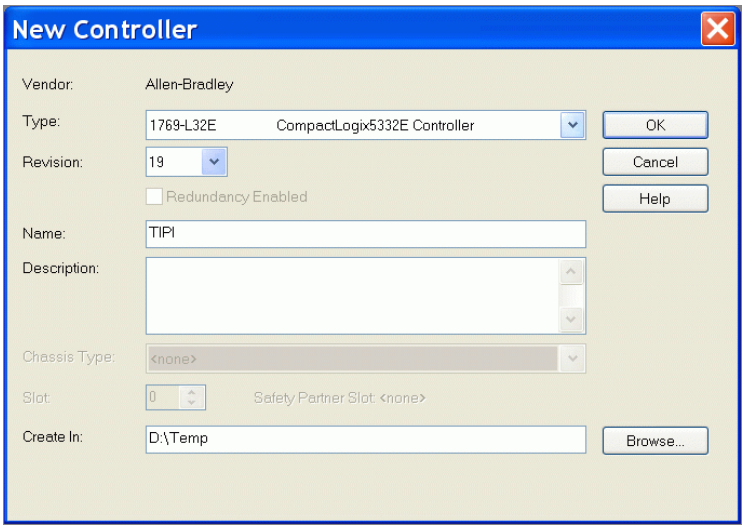
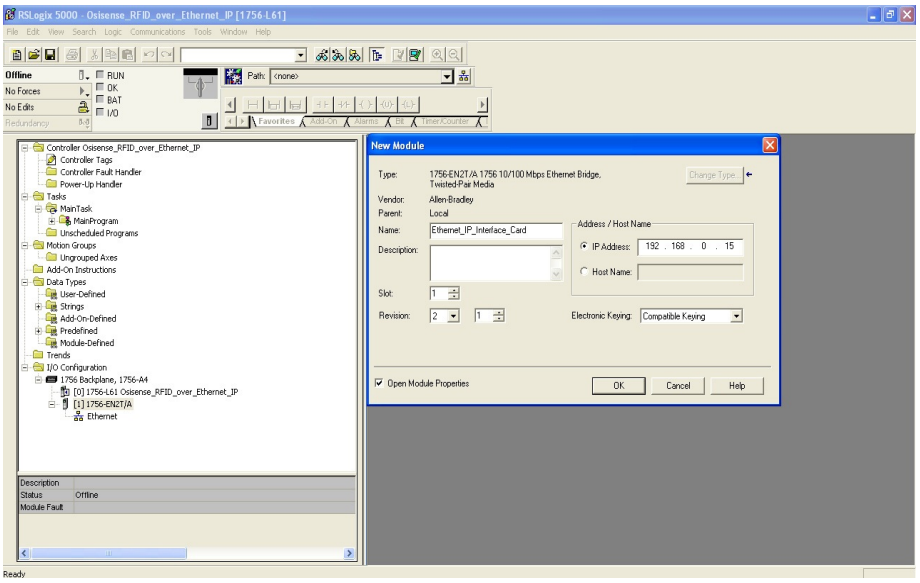
Configuring a Smart Antenna on an EtherNet/IP Network with a ControlLogix PLC

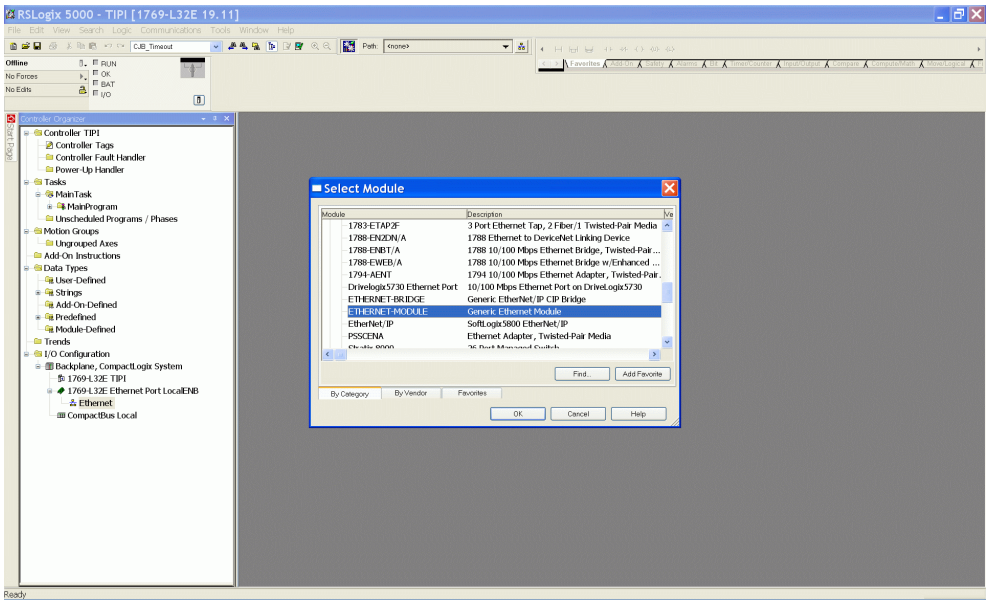
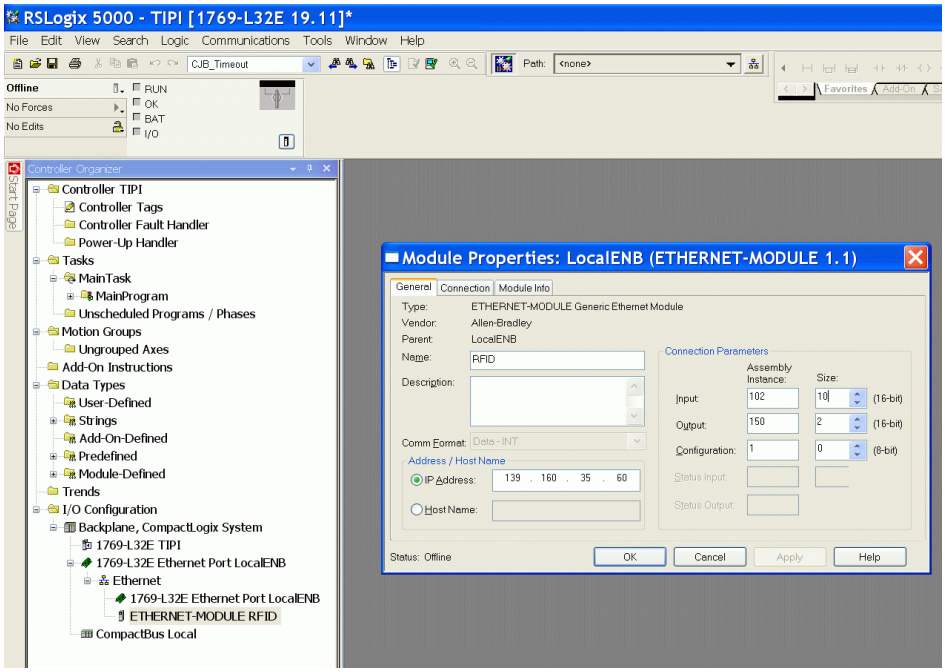
Introduction

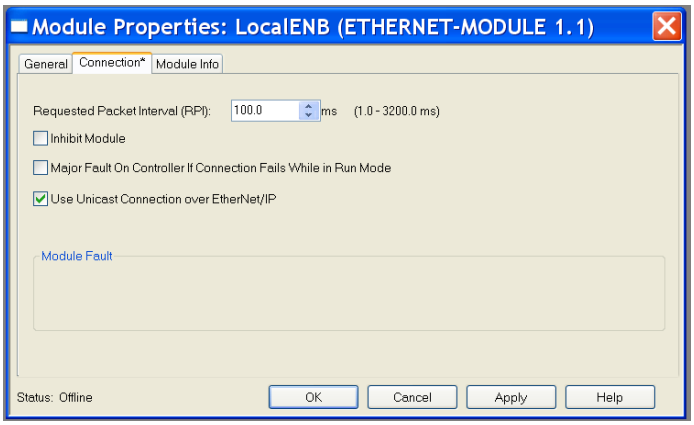
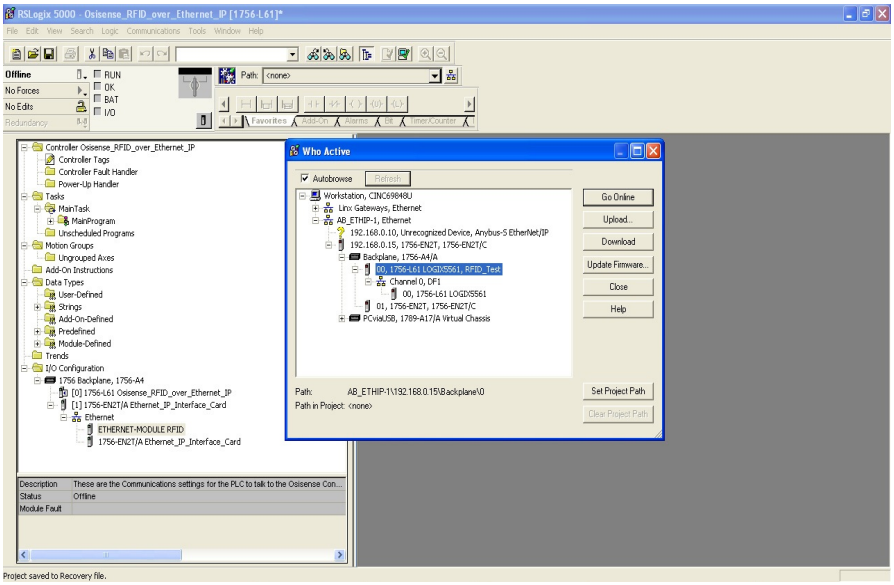
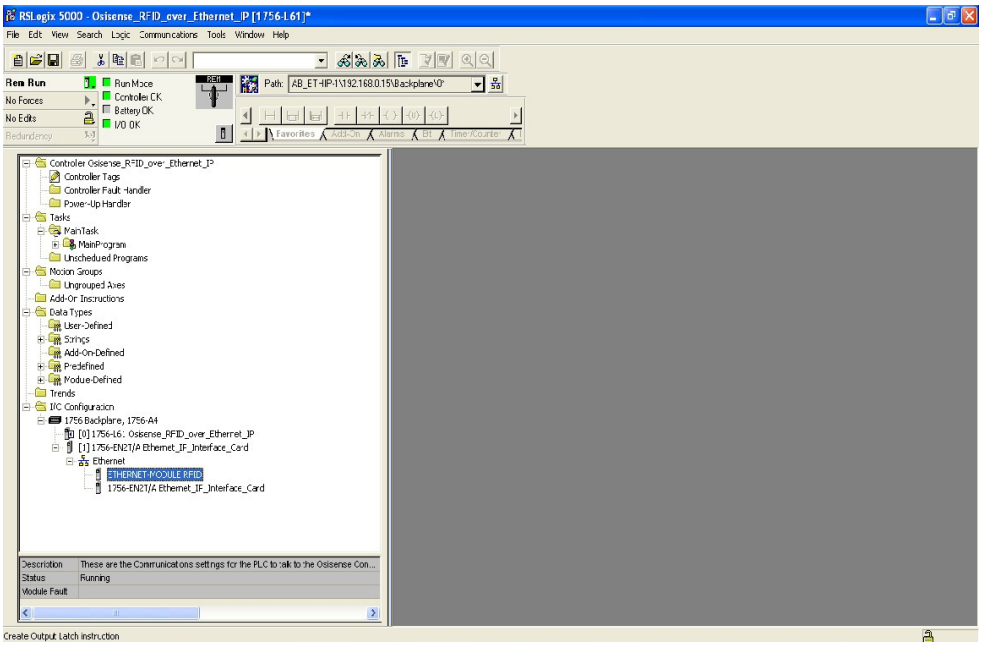
This topic illustrates how to configure a Smart Antenna on an EtherNet/IP network to communicate with an Allen Bradley ControlLogix PLC through an Ethernet cable.

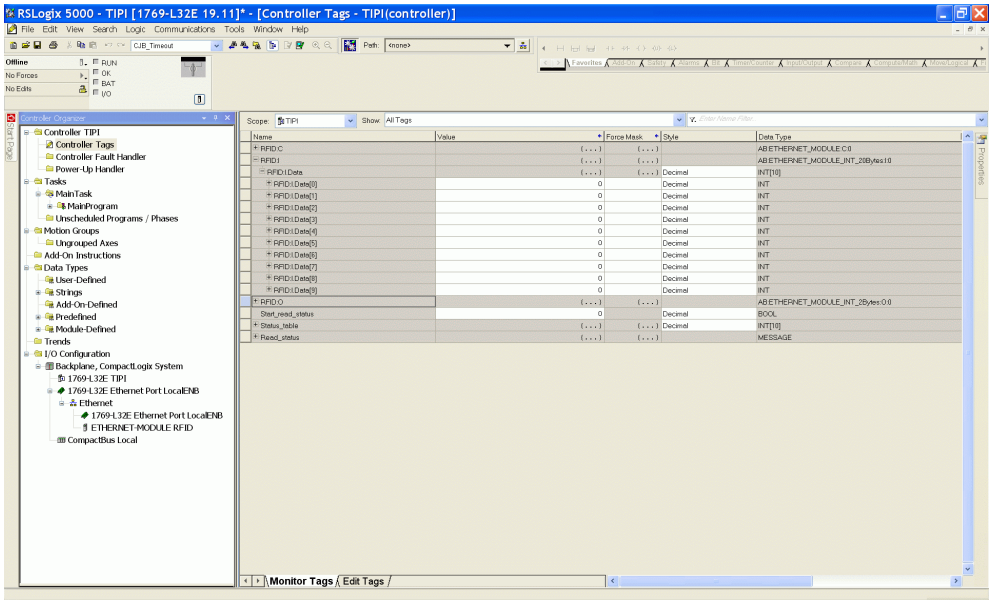
ControlLogix PLC Setup

This table covers the steps necessary to program the ControlLogix PLC using RSLogix 5000 software:

Step	Action
1	Start the RSLogix 5000 software.
2	Select **File** > **New**. The **New Controller** dialog box opens. 
3	Configure the controller by completing the required information.
4	Click **OK**.
5	Configure the EtherNet/IP card by completing the appropriate fields. 
6	Click **OK**.
7	Configure the communication module to communicate with the Smart Antenna: • From the **Select Module** dialog box, select **ETHERNET-MODULE**.

Step	Action
	• Click **OK**. 
8	Configure the Ethernet parameters to communicate with theSmart Antenna:  For the input parameters use: • **Assembly Instance** 102 (size 10) for the General status, page 44, • or **Assembly Instance** 103 (size 100) for the Read table, page 44. For the output parameters, use the **Assembly Instance** 150 (size 2).
9	Select the **Communication** tab.

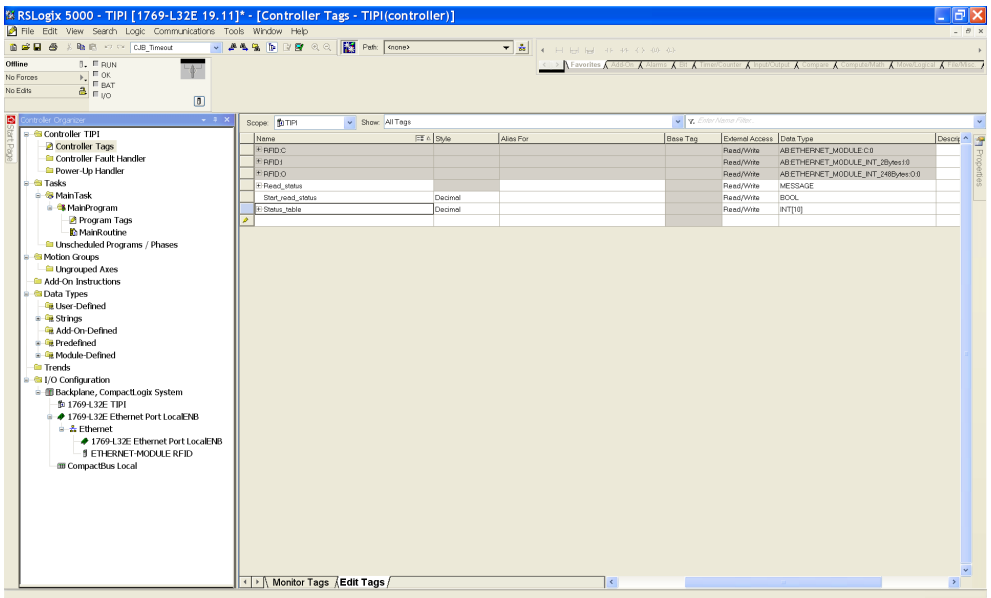
Step	Action
10	Change the **Requested Packet Interval (RPI)** value to 50...100 ms. 
11	Click **OK**.
12	Save and download the configuration to your ControlLogix PLC by selecting the module and clicking the buttons on the **Who Active** dialog box to perform the various functions as necessary. 
13	When the download is complete, a prompt displays to place the ControlLogix PLC in Run Mode. 

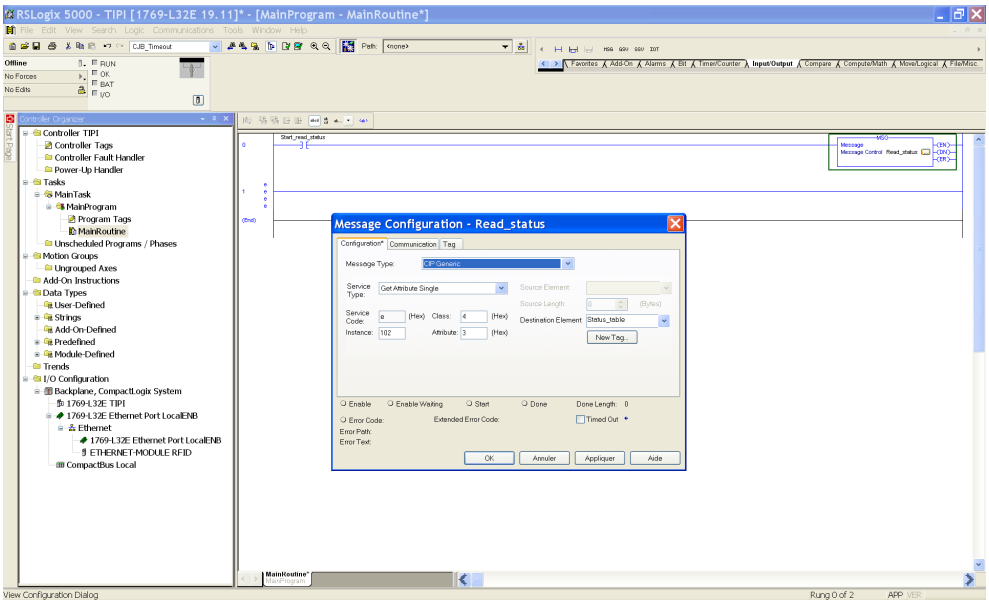
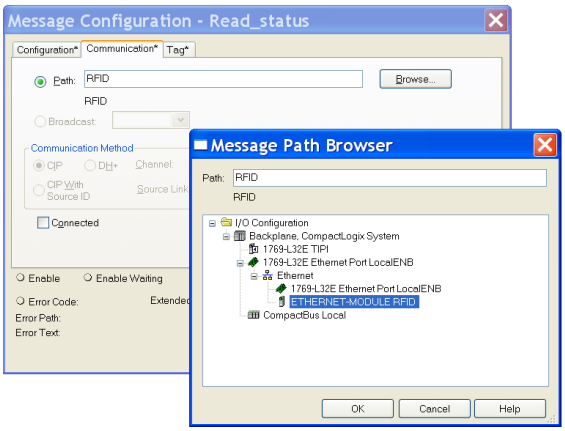
Step	Action
14	Select **Controller Tags** from the navigation panel located on the left side of the window. The controller tags that are used to communicate with the Smart Antenna appear on the right side of the window. 
15	The configuration of the communication from a ControlLogix PLC to a Smart Antenna system using the EtherNet/IP protocol is complete.

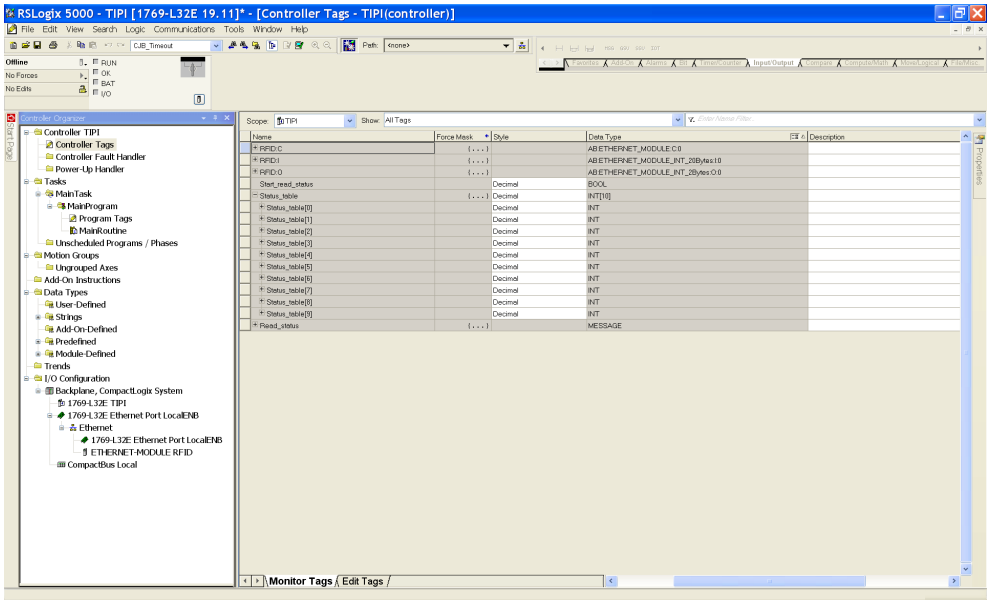
Read the Assembly 102 (General Status) or 103 (Read Table) Using an Explicit Message

Procedure

This table covers the steps necessary to read the assembly 102 or 103 with an explicit message:

Step	Action
1	In the **Controller Organizer**, open the **Controller Tags** and select the **Edit Tags** tab.
2	Create the following tags: • `Read_status` (type: MESSAGE) • `Start_read_status` (type: BOOL) in order to manage the message block • `Status_table` (type: array of INT), the length depends on the assembly (10 for the assembly 102, 100 for the assembly 103) 
3	In the **Controller Organizer** > **MainRoutine**, create a new rung.

Step	Action
4	Insert a message block **MSG** (available in the **Input/Output** tab):  Configure the message element: • **Message Type**: CIP Generic • **Service Type**: Get Attribute Single • **Service Code**: e • **Class**: 4 • **Instance**: 102 or 103 • **Attribute**: 3 • **Destination Element**: `Status_table`
5	Select the **Communication** tab and configure the communication path using the browser: 
6	Click **OK**.
7	Save and download the application to the PLC.
8	When the download is complete, a prompt displays to place the PLC in Run Mode.

Step	Action
9	Click **Controller Organizer** > **Controller Tags** and select the **Monitor Tags** tab: 
10	Use the `Start_read_status` bit to manage the message block. **Result:** The assembly data are returned in the `Status_table array`.

Reading/Writing Request with the Modbus Object

Introduction

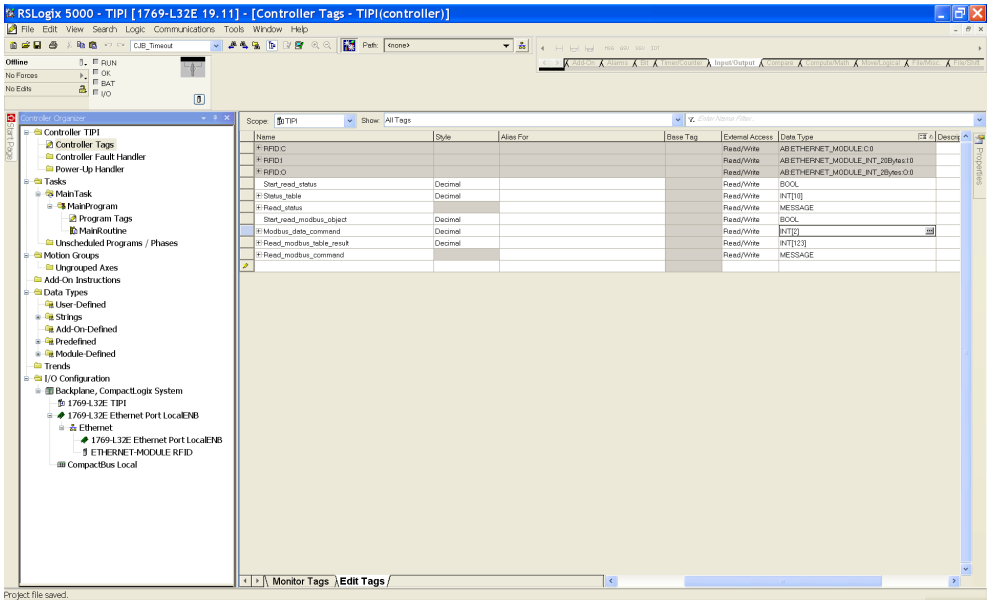
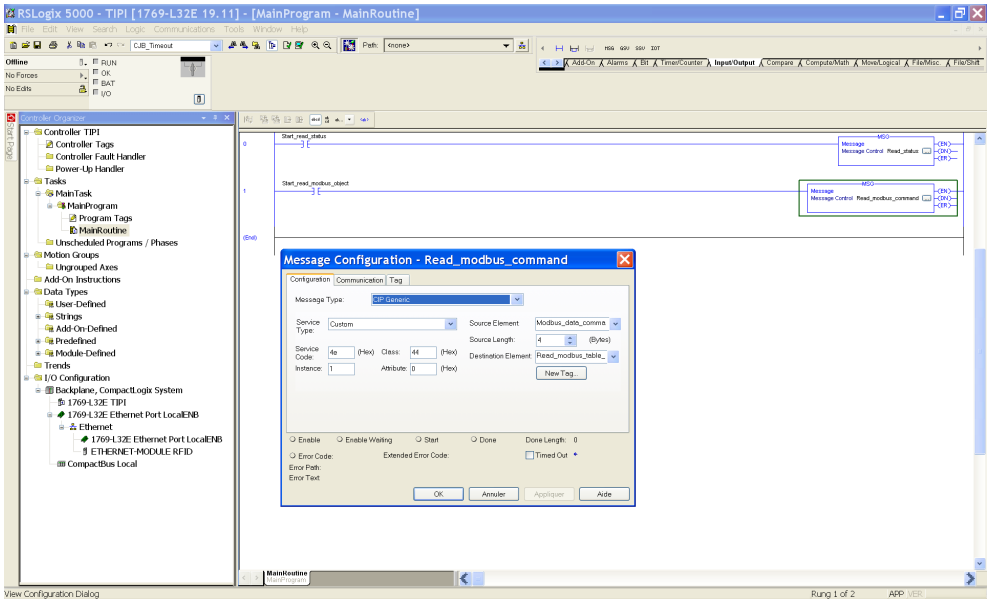
These Modbus explicit commands must be used to manage the tag and the Smart Antenna memory zones, page 34.

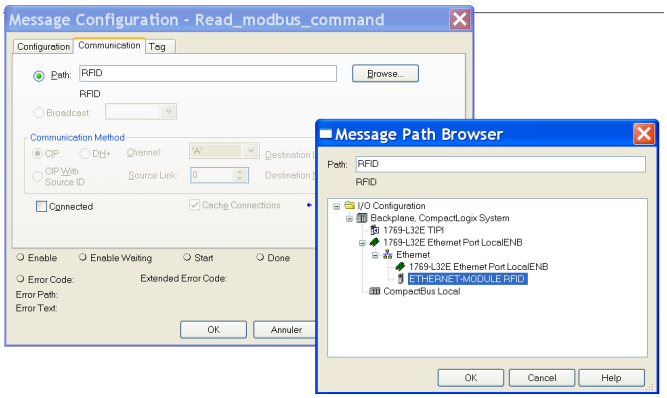
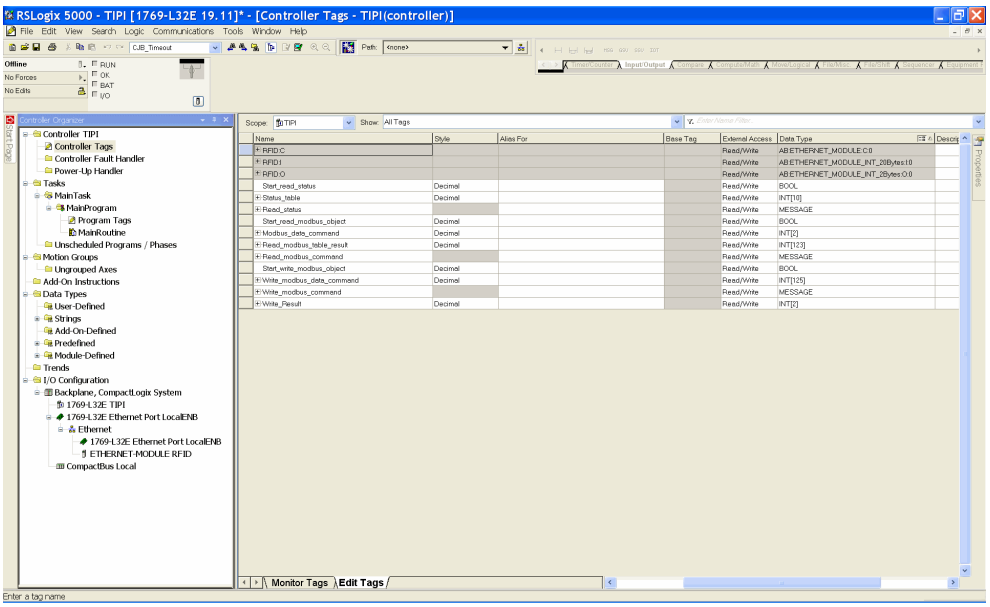
Reading Request with the Modbus Object and an Explicit Message

This table explains how to use the Modbus object, page 45 for reading with an explicit message:

Step	Action
1	In the **Controller Organizer**, open the **Controller Tags** and select the **Edit Tags** tab.

2	Create the needed tags:
	• `Read_modbus_command` (type: MESSAGE)
	• `Start_read_modbus_object` (type: BOOL) in order to manage the message block
	• `Modbus_data_command` (type: array of 2 INT), data of the read Modbus command:
	  ◦ First register: starting address
	  ◦ Second register: quantity of registers to read
	• `Read_modbus_table_result` (type: array of INT), the length depends on the quantity of the register to read (123 registers maximum)

Step	Action
	
3	In the **Controller Organizer > MainRoutine**, create a new rung.
4	Insert a message block **MSG** (available in the **Input/Output** tab):  Configure the message element: • **Message Type**: CIP Generic • **Service Type**: Custom • **Service Code**: 4e • **Class**: 44 • **Instance**: 1 • **Attribute**: 0 • **Source Element**: `Modbus_data_command` • **Source Length**: 4 • **Destination Element**: `Read_modbus_table_result`

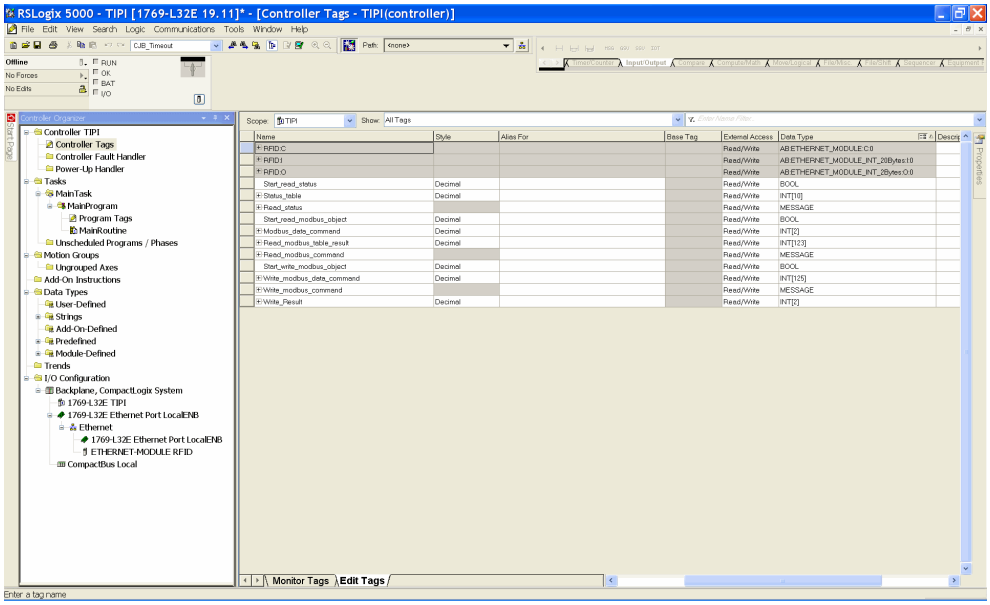
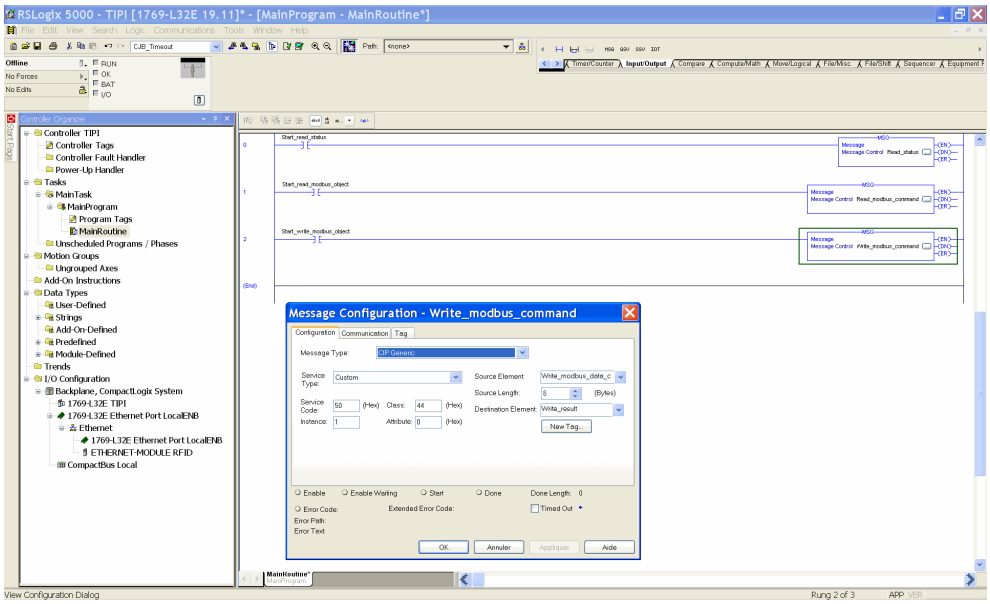
Step	Action
5	Select the **Communication** tab and configure the communication path using the browser: 
6	Click **OK**.
7	Save and download the application to the PLC.
8	When the download is complete, a prompt displays to place the PLC in Run Mode.
9	Click **Controller Organizer** > **Controller Tags** and select the **Monitor Tags** tab: 
10	Use the `Start_read_status` bit to manage the message block. **Result:** The result of the reading request is retuned in the `Read_modbus_table_result` array.

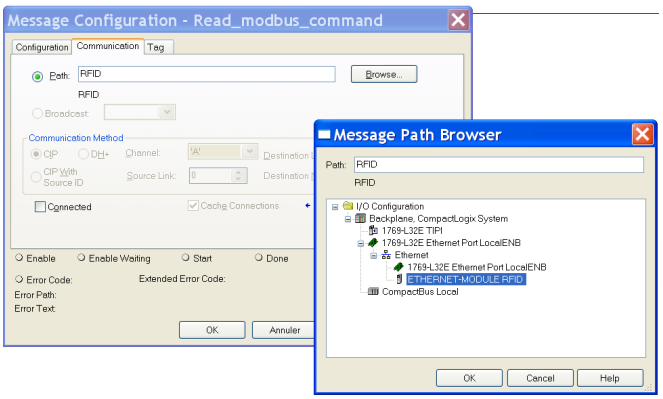
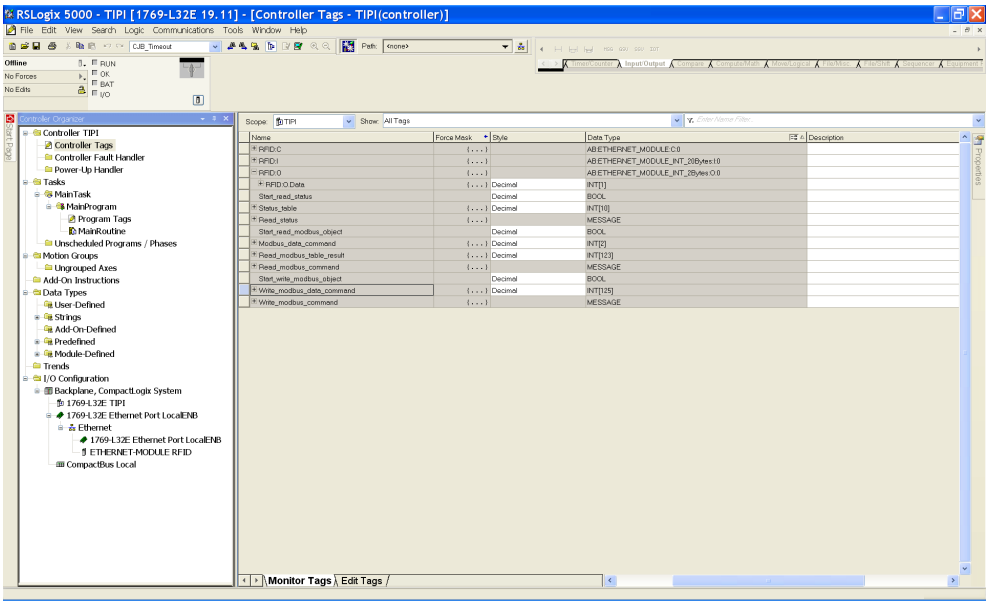
Writing Request with the Modbus Object and an Explicit Message

This table explains how to use the Modbus object, page 45 for writing with an explicit message:

Step	Action
1	In the **Controller Organizer**, open the **Controller Tags** and select the **Edit Tags** tab.

2	Create the needed tags:
	• `Write_modbus_command` (type: MESSAGE)
	• `Start_write_modbus_object` (type: BOOL) in order to manage the message block
	• `Write_Modbus_data_command` (type: array of N INT), data of the write Modbus command (the length depends on the quantity of the register to write):
	  ◦ First register: starting address
	  ◦ Second register: quantity of registers to write

Step	Action
	◦ Third...N register: data to write • `Write_Result` (type: array of 2 INT), status of the write command. 
3	In the **Controller Organizer > MainRoutine**, create a new rung.
4	Insert a message block **MSG** (available in the **Input/Output** tab):  Configure the message element: • **Message Type**: CIP Generic • **Service Type**: Custom • **Service Code**: 50 • **Class**: 44 • **Instance**: 1 • **Attribute**: 0 • **Source Element**: `Write_modbus_command` • **Source Length**: 4 bytes + N bytes (to write N/2 registers). For example: 6 to write 1 register • **Destination Element**: `Write_Result`

Step	Action
5	Select the **Communication** tab and configure the communication path using the browser: 
6	Click **OK**.
7	Save and download the application to the PLC.
8	When the download is complete, a prompt displays to place the PLC in Run Mode.
9	Click **Controller Organizer > Controller Tags** and select the **Monitor Tags** tab: 
10	Place the data to write in the `Write_modbus_data_command` array. Use the `Start_write_modbus_object` bit to manage the message block.

Modbus TCP/IP Communications Support

Introduction

This chapter describes how a Smart Antenna can be accessed from other devices on a Modbus TCP/IP fieldbus network.

Modbus Commands Supported by the Smart Antenna

Introduction

Modbus is the protocol used by Modicon PLCs. Modbus defines the message structure that the PLCs understand and use, regardless of network type. The Modbus protocol describes the process that a controller uses to access another device, how that device responds, and how detected errors are reported.

The Smart Antenna is a server on a Modbus TCP system.

It can be connected to any system with Modbus TCP clients, including these:

- PLC (function blocks or I/O scanner)
- HMI
- SCADA
- Computer

The Unit ID of the Smart Antenna on Modbus TCP is fixed to 1, the Smart Antenna is addressed by its IP address.

Modbus Message Data Frame

Modbus messages are embedded within the frame or packet structure of the network in use. A Modbus over TCP/IP network uses both the Ethernet II and IEEE 802.3 data formats. For communications with the Smart Antenna, Modbus messages can be embedded in either frame type. Ethernet II is the default data format.

Modbus Message Structure

The Modbus protocol uses 16-bit words (holding registers). A Modbus message begins with a header. A Modbus message uses a Modbus function code, page 64 as the first byte.

Following is a description of the structure of a Modbus message header:

Invoke Identifier	Protocol Type	Command Length	Destination ID	Modbus Message
Two-byte field that associates a request with a response	Two-byte field Value for Modbus is always 0	Two-byte field Value is the size of the rest of the message	One-byte	N-byte field First byte is the Modbus function code

List of Supported Commands

The table lists the Modbus commands that the Smart Antenna supports:

Modbus Function Code	Subfunction or Subindex	Command
03h	-	Read n holding registers (1 ≤ n ≤ 123)
06h	-	Write one register
08h	16h	Get/clear Ethernet statistics

Modbus Function Code	Subfunction or Subindex	Command
0Bh	-	Read event counters
10h	-	Write n registers (1 ≤ n ≤ 123)
2Bh	0Eh	ID

Modbus Requests Description

Read N Registers

This function is used to read tables of registers.

Read request:

Slave no.	Function code	Address of 1st register		Number of registers		Check
01h	3h	Hi	Lo	Hi	Lo	
1 byte	1 byte	2 bytes		2 bytes		2 bytes (RTU mode)

- Slave no.: 01h
- Function code: 3h
- Address of first register: Corresponds to the address of the first register to be read in the tag or the Smart Antenna (depending on the address)
- Number of registers: 1 ≤ N ≤ 123

Response:

Slave no.	Function code	Number of bytes read	Value of 1st register			Value of last register		Check
01h	3h or 4h		Hi	Lo		Hi	Lo	
1 byte	1 byte	1 byte	2 bytes			2 bytes		2 bytes (RTU mode)

- Slave no.: 01h
- Function code: Same as read request
- Number of bytes read: 2 to 246
- Value of the registers read: 0000h to FFFFh
- If there is no tag present, the Smart Antenna sends a detected error report (Error messages, page 67).

Write One Register

Write request:

Slave no.	Function code	Address of register		Register Value		Check
01h	6h	Hi	Lo	Hi	Lo	
1 byte	1 byte	2 bytes		2 bytes		2 bytes (RTU mode)

- Slave no.: 01h
- Function code: 6h

- Address of register: Same addressing field as for the read request
- Register values: 0000h to FFFFh

Response:

Slave no.	Function code	Address of register		Register Value		Check
01h	6h	Hi	Lo	Hi	Lo	
1 byte	1 byte	2 bytes		2 bytes		2 bytes (RTU mode)

The response is an echo of the request, indicating that the value contained in the request has been taken into account by the Smart Antenna.

Write N Registers

Write request:

Slave no.	Function code	Address of 1st register		Number of registers		Number of bytes	Value of 1st register			Value of last register		Check
01h	10h	Hi	Lo	Hi	Lo		Hi	Lo		Hi	Lo	
1 byte	1 byte	2 bytes		2 bytes		1 byte	2 bytes			2 bytes		2 bytes (RTU mode)

- Slave no.: 01h
- Function code: 10h
- Number of registers: 1 ≤ N ≤ 123
- Number of bytes: Twice the number of registers
- Register values: 0000h to FFFFh

Response:

Slave no.	Function code	Address of 1st register written		Number of registers written		Check
01h	10h	Hi	Lo	Hi	Lo	
1 byte	1 byte	2 bytes		2 bytes		2 bytes (RTU mode)

- Slave no.: 01h
- Function code: Same as request
- Address of first register written: Same as request
- Number of registers written: Same as request

Identification Request

Function 2Bh: This function is used to identify the Smart Antenna.

Read request:

Slave no.	Function code	MEI *	Read Device ID code	Object ID
01h	2Bh	0Eh	01h, 02h, 03h	00h

*: MEI = Modbus Encapsulated Interface

Response:

Index	Object Name & Description	Description	Data Type
0 (0000h)	Manufacturer name	TELEMECANIQUE	ASCII string

Index	Object Name & Description	Description	Data Type
1 (0001h)	Product code		
2 (0002h)	Version number	Vx.y (for example: V3.6)	

Detected Error Messages

When an anomaly in the message (or during its execution) is detected by the Smart Antenna to which it is addressed, the Smart Antenna sends back a detected error message to the master system.

Syntax:

Slave no.	Function code	Detected error code	Check
1 byte	1 byte	1 byte	2 bytes (RTU mode)

- Slave no.: 01h
- Function code: Same as the function code and most significant bit of the byte set at 1

Examples:

- Function code of the detected error message after a read request:

  83h = (80 + 03) or 84h = (80 + 04)
- Function code of the detected error message after a write request:

  90h = (80 + 10)

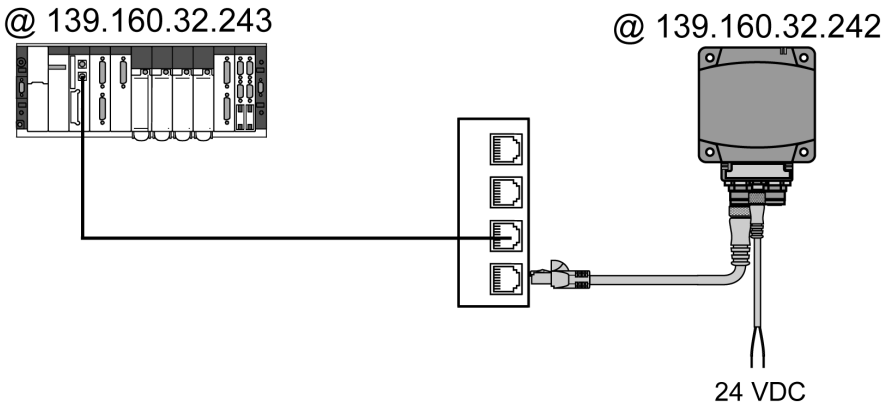
Detected error code:

- 1h: Unknown function code or incorrect request format
- 2h: Incorrect address or prohibited zone or protected zone or address outside the tag memory zone
- 3h: Incorrect data too much or not enough data in the frame, or quantity = 0, or data incompatible
- 4h: Execution detected error (in read or write mode, or tag missing)

Modbus TCP/IP Application Example

Application Example

A Smart Antenna and a Premium PLC are connected to a Modbus TCP/IP network.

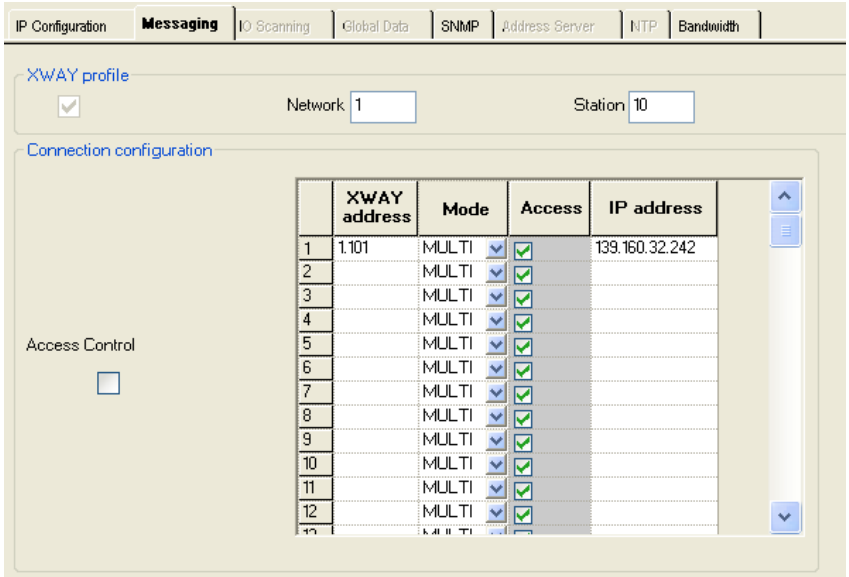


PLC Configuration with Unity Pro XL

To enable communication between these 2 devices, the PLC hardware configuration must be entered, giving:

- An XWAY address for the Smart Antenna
- The IP address of the Smart Antenna

The figure illustrates the configuration in Unity Pro:

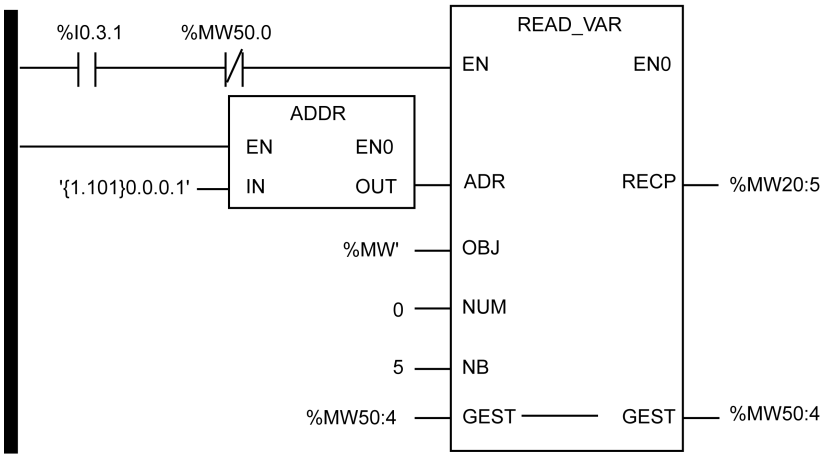


Example of Program in Unity Pro

Program example: Read 5 registers in the tag starting at register %MW0 of the tag.

NOTE: The Modbus address of the Smart Antenna is 1 (fixed address).

LADDER programming



Structured Text programming

```
if % I0.3.1 and not Management_buffer[0].0 then
     READ_VAR (adr := ADDR('(1.101)0.0.0.1)'),
           OBJ := '%MW',
           NUM := 0,
           NB := 5,
           GEST := Management_buffer,
           RECP => Reception_buffer);
end_if;
```

Reception_buffer	ARRAY[0..4] OF INT
Reception_buffer[0]	INT
Reception_buffer[1]	INT
Reception_buffer[2]	INT
Reception_buffer[3]	INT
Reception_buffer[4]	INT

Management_buffer	ARRAY[0..3] OF INT
Management_buffer[0]	INT
Management_buffer[1]	INT
Management_buffer[2]	INT
Management_buffer[3]	INT

NOTE: The ADDR function is structured: **'(***XWAY address***)***Rack***.***Module***.***Channel***.***Modbus address***)'**.

Diagnostics

Aim of This Chapter

This chapter describes how to diagnose a detected issue using the LEDs on the Smart Antenna.

Smart Antenna Diagnostic LEDs

Introduction

The 6 bicolor LEDs display all the operating states of the Smart Antenna:

LEDs Description

The table describes the LEDs state:

LED	Name	LED State	Description	Smart Antenna State
1	TAG	Solid green	Tag presence	A tag is detected, dialog ok
		1 flash	No tag detected	Waiting for a tag
		Red flashes	RFID detected error	Errors detected in the dialog with the tag
2	COM	Green flashes	Requests received from a client	Ok
		Red flashes	Detected error in requests received from a client	Detected error code returned to the client (no tag / bad parameters,...)
3	NS (Network Status)	Steady off	Not powered or no IP address	Waiting for IP address setting (fixed or DHCP).
		Flashing green	No connections	No CIP connection established, and an exclusive owner connection with a client has not timed out.
		Solid green	Connected	At least one CIP connection is established, and an exclusive owner connection with client has not timed out.
		Flashing red	Connection timeout	An exclusive owner connection with client has timed out.
		Solid red	Duplicate IP	The Smart Antenna has detected that its IP address is already in use.
		Flashing green/red	Self-test	The Smart Antenna is performing its power-on self test.
4	Link Activity (port 1 and 2)	Solid green	Ethernet link present at 100 Mbit/s	Ok

LED	Name	LED State	Description	Smart Antenna State
5		Flashing green	Traffic at 100 Mbit/s	Ok
		Solid yellow	Ethernet link present at 10 Mbit/s	Ok
		Flashing yellow	Traffic at 10 Mbit/s	Ok
6	MS (Ethernet module status)	Solid green	The Ethernet module of the Smart Antenna is operational	Ok
		Flashing green	Standby	The Smart Antenna is waiting for network configuration.
		Flashing red	Minor detected fault	The Smart Antenna has detected a recoverable minor fault. **NOTE:** An incorrect or inconsistent configuration is considered as a minor detected fault.
		Steady red	Major detected fault	The Smart Antenna has detected a non-recoverable major fault on its Ethernet module.
		Flashing green/red	Self-test	The Smart Antenna is performing its power-on self test.

FAQs

Aim of This Chapter

This chapter contains FAQs for the Smart Antenna.

FAQ

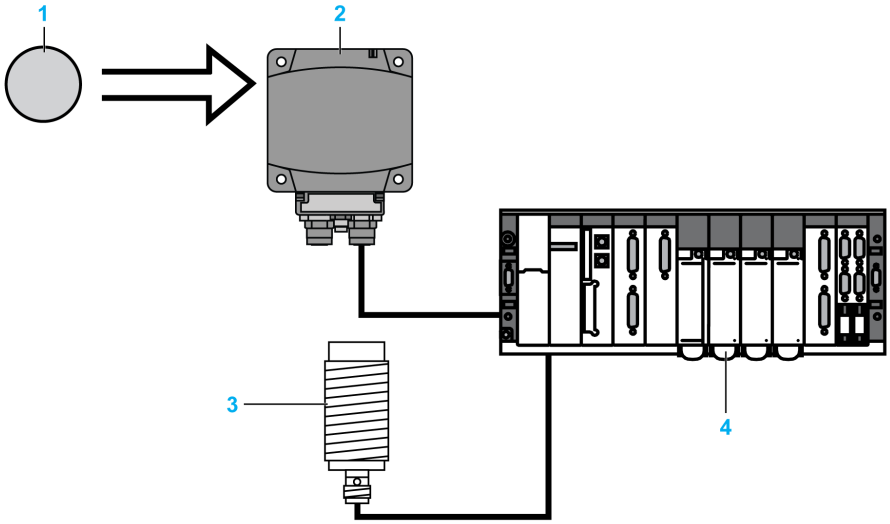
Detected Errors During Tag Reading/Writing

How to avoid making errors in reading/writing a tag?

To avoid making errors in reading/writing a tag, it is necessary to check the tag presence between making the request.

1: Use a sensor:

Synchronize the read/write requests with a sensor that indicates the presence of the tag to the control system:



1 Tag

2 Smart Antenna

3 Tag presence sensor

4 PLC

In case of processing detected errors (such as incorrect positioning of the tag or a transmission detected error), provide for repetition of the request before switching to the "Fallback" mode (abandoning of the request and generation of an alarm).

2: Read the STATUS register of the Smart Antenna:

Before initiating a tag read/write request, ensure that the tag is present using a request to read the Smart Antenna STATUS register (bit 0 of the register STATUS = 1 if the tag is present).

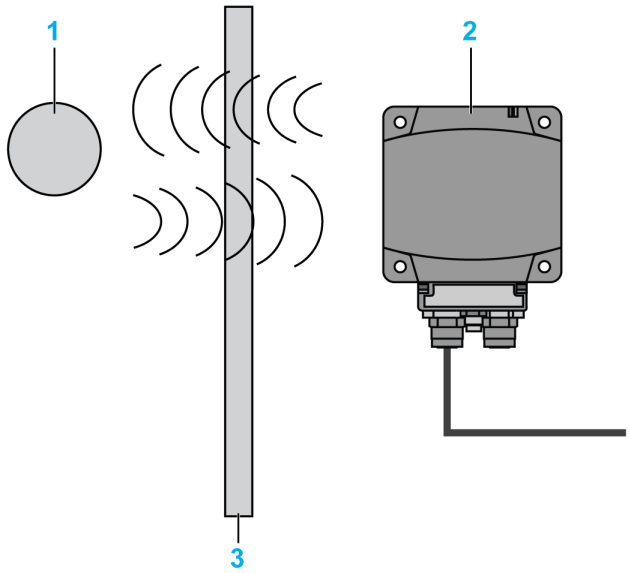
Protecting the Smart Antenna

How to protect the Smart Antenna against shock?

To protect the system against shock, you can:

- Embed the Smart Antenna in metal, page 25
- Embed the tag in metal, page 25

- Protect the Smart Antenna by making use of its capability to work through non-metallic materials according to the diagram shown below:



1 Tag

2 Smart Antenna

3 Non-metallic screen

NOTE: Thermal protection

Avoid exposing the tags to radiating heat sources, such as infrared dryers.

Maximum Cable Length

What is the maximum connection cable length of the Smart Antenna?

80 m (262.5 ft) between each Smart Antenna.

Line Terminator

How to insert the line terminator?

A line terminator is not necessary on Ethernet network.

COM Detected Error

How to process the communication interruptions between the PLC and the Smart Antenna?

There is a permanent risk of communication detected error in the reading or writing of a tag (disturbances, EMC/EMI, tag in the dialog zone limit...).

It is necessary to integrate the risk management into the PLC program:

- Process the detected error codes of the Smart Antenna (request for reading / writing is rejected since no tag is detected in front of the Smart Antenna,...)
- Process the "Time-Out" when the Smart Antenna does not respond, such as "the message is not included following a disturbance".
- In the case of detected error, repeat the request (up to 3 times) before exiting and issuing a PLC alarm.

Tag Writing Cycle Limitation

How many times can it be written in the XGHB tags?

The maximum number of writing depends on the tag storage temperature: the higher the temperature is, the more this limit decreases.

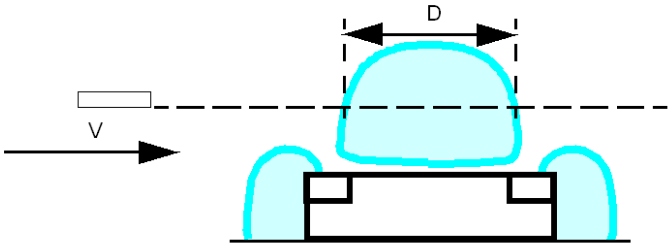
If the tag is permanently at the defined storage temperature range, the minimum number of writing in the tag is 100,000.

If the tag is permanently at a temperature less than 30°C (86°F) (the most frequent case), the maximum number of typical writings is **2.5 million**.

NOTE: For application where frequent writing is required, select a tag with a Feram memory (10^{10} write cycles).

Readable Data of a Moving Tag

What amount of data can be exchanged in a moving tag?



When the tag is not stopped during its movement in front of the Smart Antenna, it is necessary to:

Step	Action
1	Determine the speed **V** of the tag.
2	Determine the number of registers to exchange.
4	Refer to the maximum speed in the tag characteristics, page 19.

NOTICE

UNINTENDED EQUIPMENT OPERATION

Do not make a writing request when the tag exits the detection zone of the Smart Antenna (Sensing Zone, page 25).

Failure to follow these instructions can result in equipment damage.

NOTE: This may generate a tag-writing error or incorrect data writing.

Using Third-party Tags

What is the dialog distance between a Smart Antenna and a tag purchased at a third-party supplier?

There is no normalization of the reading distances. Each tag with its own characteristics cannot allow a dialog distance.

It is imperative to test a sample to determine the proper dialog distance.

Compatibility of Smart Antenna with Other 13.56 MHz Tags

Is my 13.56 MHz tag compatible with the Smart Antenna?

Send a sample to your TMSS France agency to verify its

compatibility.

Precautions Against EMC/EMI Perturbations

What are the precautions to be taken regarding EMC/EMI?

To avoid EMC/EMI perturbations, it is necessary:

- Make sure that the Smart Antenna is at least 30 cm (11.81 in) from an EMC/EMI source (motor, solenoid valve, and so on).
- Use the intended cables (conceived to protect against EMC/EMI perturbations).

Metal Influence

What is the influence of metal on the Smart Antenna/tag reading distances?

The presence of metal near an RFID tag affects the reading distances.

Some tags in the Smart Antenna range are designed to attenuate this phenomenon (XGHB44•••• and XGHB221346). Other references cannot be attached directly on a metallic support.

Glossary

100Base-TX:

An adaptation of the IEEE 802.3u (Ethernet) standard, the 100Base-T standard uses 2 twisted-pair wiring with a maximum segment length of 100 m (328 ft) and terminates with an RJ45 connector. A 100Base-T network is a baseband network capable of transmitting data at a maximum speed of 100 Mbit/s. "Fast Ethernet" is another name for 100Base-T because it is 10 times faster than 10Base-T.

10Base-T:

An adaptation of the IEEE 802.3 (Ethernet) standard, the 10Base-T standard uses twisted-pair wiring with a maximum segment length of 100 m (328 ft) and terminates with an RJ45 connector. A 10Base-T network is a baseband network capable of transmitting data at a maximum speed of 10 Mbit/s.

802.3 frame:

A frame format, specified in the IEEE 802.3 (Ethernet) standard, in which the header specifies the data packet length.

A

ARRAY:

An ARRAY is a table containing elements of a single type. The syntax is as follows: `ARRAY [<limits>] OF <Type>`

Example 1: `ARRAY [1..2] OF BOOL` is a 1-dimensional table with 2 elements of type `BOOL`.

Example 2: `ARRAY [1..10, 1..20] OF INT` is a 2-dimensional table with 10x20 elements of type `INT`.

ASCII:

The american standard code for information interchange is a communication protocol for representing alphanumeric characters (letters, numbers, and certain graphic and control characters).

B

BOOL:

A *Boolean* type is the basic data type in computing. A `BOOL` variable can have one of these values: 0 (`FALSE`), 1 (`TRUE`). A bit that is extracted from a word is of type `BOOL`, for example: `%MW10.4` is the fifth bit of a memory word number 10.

BootP:

BootP (bootstrap protocol) is an UDP/IP protocol that allows an Internet node to obtain its IP parameters based on its MAC address.

BYTE:

When 8 bits are grouped together, they are called a `BYTE`. You can enter a `BYTE` either in binary mode or in base 8. The `BYTE` type is encoded in an 8-bit format that ranges from `16#00` to `16#FF` (in hexadecimal format).

C

configuration:

The arrangement and interconnection of hardware components within a system and the hardware and software selections that determine the operating characteristics of the system.

CRC:

cyclic redundancy check. Messages that implement this detected error checking mechanism have a CRC field that is calculated by the transmitter according to the message content. Receiving nodes recalculate the field. Disagreement in the 2 codes indicates a difference between the transmitted message and the one received.

D

DHCP:

dynamic host configuration protocol. A TCP/IP protocol that allows a server to assign an IP address based on a device name (host name) to a network node.

E

EDS:

electronic data sheet. The EDS is a standardized ASCII file that contains information about a network device communications functionality and the contents of its object dictionary. The EDS also defines device-specific and manufacturer-specific objects.

EEPROM:

Electrically Erasable Programmable Read-Only Memory. EEPROM is a nonvolatile memory.

EMC:

electromagnetic compatibility. Devices that meet EMC requirements can operate within a system expected electromagnetic limits without interruption.

Ethernet II:

A frame format in which the header specifies the packet type, Ethernet II is the default frame format for NIM communications.

EtherNet/IP:

EtherNet/IP (the Ethernet Industrial Protocol) is especially suited to factory applications in which there is a need to control, configure, and monitor events within an industrial system. The ODVA-specified protocol runs CIP (the Common Industrial Protocol) on top of standard Internet protocols, like TCP/IP and UDP. It is an open local (communications) network that enables the interconnectivity of all levels of manufacturing operations from the office plant to the sensors and actuators on its floor.

Ethernet:

A LAN wiring and signaling specification used to connect devices within a defined area, for example, a building. Ethernet uses a bus or a star topology to connect different nodes on a network.

F

FeRAM:

Ferroelectric Random Access Memory. FeRAM is a nonvolatile memory offering faster write performance and greater number of writing cycles.

flash memory:

Flash memory is nonvolatile memory that can be overwritten. It is stored on a special EEPROM that can be erased and reprogrammed.

function block:

A function block performs a specific automation function, such as speed control. A function block comprises configuration data and a set of operating parameters.

function code:

A function code is an instruction set commanding 1 or more slave devices at specified addresses to perform a type of action, for example, read a set of data registers and respond with the content.

H

HMI:

human-machine interface. An operator interface, usually graphical, for industrial equipment.

HTTP:

hypertext transfer protocol. The protocol that a web server and a client browser use to communicate with one another.

I

IEC:

International Electrotechnical Commission Carrier. Founded in 1884 to focus on advancing the theory and practice of electrical, electronics, and computer engineering, and computer science. EN 61131-2 is the specification that deals with industrial automation equipment.

IEEE:

Institute of Electrical and Electronics Engineers, Inc. The international standards and conformity assessment body for all fields of electrotechnology, including electricity and electronics.

IP rating:

Ingress Protection rating according to IEC 60529.

IP:

Internet Protocol. That part of the TCP/IP protocol family that tracks the Internet addresses of nodes, routes outgoing messages, and recognizes incoming messages.

L

LAN:

local area network. A short-distance data communications network.

LSB:

least significant bit, least significant byte. The part of a number, address, or field that is written as the rightmost single value in conventional hexadecimal or binary notation.

M

MAC address:

media access control address. A 48-bit number, unique on a network, that is programmed into each network card or device when it is manufactured.

master/slave model:

The direction of control in a network that implements the master/slave model is from the master to the slave devices.

Modbus:

Modbus is an application layer messaging protocol. Modbus provides client and server communications between devices connected on different types of buses or networks. Modbus offers many services specified by function codes.

MSB:

most significant bit, most significant byte. The part of a number, address, or field that is written as the leftmost single value in conventional hexadecimal or binary notation.

%MW:

According to the IEC standard, %MW represents a memory word register (for example a language object of type memory word).

P

PELV:

protective extra low voltage.

PLC:

programmable logic controller. The PLC is the brain of an industrial manufacturing process. It automates a process as opposed to relay control systems. PLCs are computers suited to survive the harsh conditions of the industrial environment.

R

Register:

Set of data encoded in a 16-bit format (WORD type).

RFID:

radio frequency identification. RFID is a term used for radio frequency identification systems. These frequencies range between 50 kHz and 2.5 GHz. The most widely used is 13.56 MHz.

Rx:

reception.

S

SCADA:

supervisory control and data acquisition. Typically accomplished in industrial settings with microcomputers.

Smart Antenna:

RFID reader incorporating all the RFID and network functions in the same device.

Structured Text:

A program written in the structured text (ST) language includes complex statements and nested instructions (such as iteration loops, conditional executions, or functions). ST is compliant with IEC 61131-3.

subnet:

A part of a network that shares a network address with the other parts of a network. A subnet may be physically and/or logically independent of the rest of the network. A part of an Internet address called a subnet number, which is ignored in IP routing, distinguishes the subnet.

T

TCP:

transmission control protocol. A connection-oriented transport layer protocol that provides full-duplex data transmission. TCP is part of the TCP/IP suite of protocols.

Tx:

transmission.

U

UDP:

user datagram protocol. A connectionless mode protocol in which messages are delivered in a datagram to a destination computer. The UDP protocol is typically bundled with the Internet protocol (UPD/IP).

UID:

Unique ID. Identification number of the tag. Each tag has a different UID.

W

WORD:

The WORD type is encoded in a 16-bit format

Index

F

frame type
  Ethernet II 64
  IEEE 802.3 64

I

IP address configuration 28

M

Modbus function codes 64
Modbus over TCP/IP
  data formats 64
Modbus protocol 64

N

network topology 11

P

PLC 64

T

topology 11

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

TMSS France SAS
share capital: 366 931 214 €
Tour Eqho, 2 avenue Gambetta,
92400 Courbevoie – France
908 125 255 RCS Nanterre

©2024, TMSS France, All Rights Reserved

EIO0000001601.02
09/2024