



User Manual
Nexto Series CPU
NX3008

MU214620 Rev. N

March 4, 2026

No part of this document may be copied or reproduced in any form without the prior written consent of Altus Sistemas de Automação S.A. who reserves the right to carry out alterations without prior advice.

According to current legislation in Brazil, the Consumer Defense Code, we are giving the following information to clients who use our products, regarding personal safety and premises.

The industrial automation equipment, manufactured by Altus, is strong and reliable due to the stringent quality control it is subjected to. However, any electronic industrial control equipment (programmable controllers, numerical commands, etc.) can damage machines or processes controlled by them when there are defective components and/or when a programming or installation error occurs. This can even put human lives at risk. The user should consider the possible consequences of the defects and should provide additional external installations for safety reasons. This concern is higher when in initial commissioning and testing.

The equipment manufactured by Altus does not directly expose the environment to hazards, since they do not issue any kind of pollutant during their use. However, concerning the disposal of equipment, it is important to point out that built-in electronics may contain materials which are harmful to nature when improperly discarded. Therefore, it is recommended that whenever discarding this type of product, it should be forwarded to recycling plants, which guarantee proper waste management.

It is essential to read and understand the product documentation, such as manuals and technical characteristics before its installation or use. The examples and figures presented in this document are solely for illustrative purposes. Due to possible upgrades and improvements that the products may present, Altus assumes no responsibility for the use of these examples and figures in real applications. They should only be used to assist user trainings and improve experience with the products and their features.

Altus warrants its equipment as described in General Conditions of Supply, attached to the commercial proposals.

Altus guarantees that their equipment works in accordance with the clear instructions contained in their manuals and/or technical characteristics, not guaranteeing the success of any particular type of application of the equipment.

Altus does not acknowledge any other guarantee, directly or implied, mainly when end customers are dealing with third-party suppliers. The requests for additional information about the supply, equipment features and/or any other Altus services must be made in writing form. Altus is not responsible for supplying information about its equipment without formal request. These products can use EtherCAT® technology (www.ethercat.org).

COPYRIGHTS

Nexto, MasterTool, Grano and WebPLC are the registered trademarks of Altus Sistemas de Automação S.A.

Windows, Windows NT and Windows Vista are registered trademarks of Microsoft Corporation.

OPEN SOURCE SOFTWARE NOTICE

To obtain the source code under GPL, LGPL, MPL and other open source licenses, that is contained in this product, please contact opensource@altus.com.br. In addition to the source code, all referred license terms, warranty disclaimers and copyright notices may be disclosed under request.

Contents

1.	Introduction	1
1.1.	Nexto Series	1
1.2.	Innovative Features	2
1.3.	Documents Related to this Manual	3
1.4.	Visual Inspection	5
1.5.	Technical Support	5
1.6.	Warning Messages Used in this Manual	5
2.	Technical Description	6
2.1.	Panels and Connections	6
2.2.	Product Features	7
2.2.1.	General Features	7
2.2.2.	Standards and Certifications	9
2.2.3.	Memory	10
2.2.4.	Protocols	11
2.2.5.	Serial Interfaces	12
2.2.5.1.	COM 1	12
2.2.6.	CAN Interface	13
2.2.7.	USB Interface	13
2.2.8.	Ethernet Interfaces	14
2.2.8.1.	NET 1	14
2.2.8.2.	NET 2	15
2.2.8.3.	NET 3	15
2.2.9.	Memory Card Interface	16
2.2.10.	Power Supply	16
2.2.11.	Environmental Characteristics	17
2.3.	Compatibility with Other Products	17
2.4.	Performance	17
2.4.1.	MainTask Interval Time	17
2.4.2.	Application Times	18
2.4.3.	Time for Instructions Execution	18
2.4.4.	Initialization Times	18
2.5.	Physical Dimensions	19
2.6.	Purchase Data	19
2.6.1.	Included Items	19
2.6.2.	Product code	20
2.7.	Related Products	20
3.	Installation	21
3.1.	Mechanical Installation	21

3.2.	Electrical Installation	21
3.2.1.	Using the integrated power supply	21
3.2.2.	Using a NX8000 power supply module	23
3.3.	Ethernet Network Connection	25
3.3.1.	IP Address	25
3.3.2.	Gratuitous ARP	25
3.3.3.	Network Cable Installation	26
3.4.	Serial Network Connection RS-485 and CAN	27
3.5.	Memory Card Installation	27
3.6.	Architecture Installation	28
3.6.1.	Module Installation on the Main Backplane Rack	28
3.7.	Programmer Installation	28
4.	Initial Programming	29
4.1.	Memory Organization and Access	29
4.2.	Project Profiles	31
4.2.1.	Single	31
4.2.2.	Basic	32
4.2.3.	Normal	32
4.2.4.	Expert	32
4.2.5.	Custom	33
4.2.6.	Machine Profile	33
4.2.7.	General Table	34
4.2.8.	Maximum Number of Tasks	34
4.3.	CPU Configuration	35
4.4.	Libraries	36
4.5.	Inserting a Protocol Instance	36
4.5.1.	MODBUS RTU	36
4.5.2.	MODBUS Ethernet	38
4.6.	Finding the Device	40
4.7.	Login	42
4.8.	Run Mode	44
4.9.	Stop Mode	45
4.10.	Writing and Forcing Variables	45
4.11.	Logout	46
4.12.	Project Upload	46
4.13.	CPU Operating States	48
4.13.1.	Run	48
4.13.2.	Stop	48
4.13.3.	Breakpoint	48
4.13.4.	Exception	48
4.13.5.	Reset Warm	48
4.13.6.	Reset Cold	48
4.13.7.	Reset Origin	48
4.13.8.	Reset Process Command (IEC 60870-5-104)	49
4.14.	Programs (POUs) and Global Variable Lists (GVLs)	49
4.14.1.	MainPrg Program	49
4.14.2.	StartPrg Program	49
4.14.3.	UserPrg Program	49

4.14.4.	GVL System_Diagnostics	50
4.14.5.	GVL Disables	51
4.14.6.	GVL IOQualities	51
4.14.7.	GVL Module_Diagnostics	52
4.14.8.	GVL Qualities	53
4.14.9.	GVL ReqDiagnostics	54
5.	Configuration	56
5.1.	Device	56
5.1.1.	User Management and Access Rights	56
5.1.2.	PLC Settings	56
5.2.	CPU Configuration	58
5.2.1.	General Parameters	58
5.2.1.1.	Hot Swap	59
5.2.1.1.1.	Hot Swap Disabled, for Declared Modules Only	60
5.2.1.1.2.	Hot Swap Disabled	60
5.2.1.1.3.	Hot Swap Disabled, without Startup Consistency	60
5.2.1.1.4.	Hot Swap Enabled, with Startup Consistency for Declared Modules Only	60
5.2.1.1.5.	Hot Swap Enabled with Startup Consistency	60
5.2.1.1.6.	Hot Swap Enabled without Startup Consistency	61
5.2.1.1.7.	How to do the Hot Swap	61
5.2.1.2.	Retain and Persistent Memory Areas	63
5.2.1.3.	CAN Port Parameters	64
5.2.2.	External Event Configuration	64
5.2.3.	Time Synchronization	66
5.2.3.1.	IEC 60870-5-104	67
5.2.3.2.	SNTP	67
5.2.3.3.	Daylight Saving Time (DST)	68
5.2.4.	Internal Points	68
5.2.4.1.	Quality Conversions	70
5.2.4.1.1.	Internal Quality	70
5.2.4.1.2.	IEC 60870-5-104 Conversion	72
5.2.4.1.3.	MODBUS Internal Quality	73
5.2.4.1.4.	Local Bus I/O Modules Quality	74
5.2.4.1.5.	PROFIBUS I/O Modules Quality	74
5.2.4.1.6.	PROFIBUS Digital Inputs Quality	75
5.2.4.1.7.	PROFIBUS Digital Output Quality	75
5.2.4.1.8.	PROFIBUS Analog Inputs Quality	76
5.2.4.1.9.	PROFIBUS Analog Output Quality	78
5.3.	Serial Interfaces Configuration	80
5.3.1.	COM 1	80
5.3.1.1.	Advanced Configurations	81
5.4.	CAN Interface Configuration (Controller Area Network)	81
5.4.1.	CAN	81
5.5.	Management Tab Access	82
5.5.1.	System Section	82
5.5.1.1.	Clock Setting	82
5.5.1.1.1.	Computer Time (UTC)	83
5.5.1.1.2.	Custom Time (UTC)	83

5.5.2.	Network Section	83
5.5.2.1.	Network Section Configurations	84
5.5.2.1.1.	Defined by Application	84
5.5.2.1.2.	Defined by web page	85
5.5.2.2.	Network Sniffer	86
5.6.	USB Interface Configuration	87
5.6.1.	Mass Storage Device	89
5.6.1.1.	General Storage	89
5.6.1.2.	Application Not Loading on Startup	90
5.6.1.3.	Transferring an Application from a USB Device	91
5.6.2.	USB to RS-232 Converter	91
5.6.3.	Modem Devices	92
5.6.4.	WiFi Adapters	95
5.6.5.	USB Interface Control User Function	97
5.7.	Ethernet Interfaces Configuration	98
5.7.1.	Internal Ethernet Interfaces	98
5.7.1.1.	NET 1	99
5.7.1.2.	NET 2	99
5.7.1.3.	NET 3	99
5.7.1.4.	Configuration of Internal Ethernet Interfaces	99
5.7.1.4.1.	Single Mode	100
5.7.1.4.2.	Redundant Mode	100
5.7.1.4.3.	Switch Mode	101
5.7.1.4.4.	Switch Mode - Disabled	101
5.7.1.4.5.	Switch Mode - MRP	101
5.7.1.4.6.	Switch Mode - RSTP	102
5.7.2.	NX5000 Remote Ethernet Interface	103
5.7.2.1.	NET 1	103
5.7.2.2.	Operation Modes of the NX5000 Remote Ethernet Interface	103
5.7.2.2.1.	Redundant Mode	103
5.7.3.	Reserved TCP/UDP Ports	104
5.7.4.	Network Routing	104
5.8.	Protocols Configuration	105
5.8.1.	Protocol Behavior x CPU State	108
5.8.2.	Double Points	108
5.8.3.	CPU's Events Queue	108
5.8.3.1.	Consumers	109
5.8.3.2.	Queue Functioning Principles	110
5.8.3.2.1.	Overflow Sign	110
5.8.3.3.	Producers	110
5.8.4.	Interception of Commands Coming from the Control Center	110
5.8.5.	MODBUS RTU Master	115
5.8.5.1.	MODBUS Master Protocol Configuration by Symbolic Mapping	115
5.8.5.1.1.	MODBUS Master Protocol General Parameters – Symbolic Mapping Configuration	115
5.8.5.1.2.	Devices Configuration – Symbolic Mapping configuration	117
5.8.5.1.3.	Mappings Configuration – Symbolic Mapping Settings	118
5.8.5.1.4.	Requests Configuration – Symbolic Mapping Settings	119

5.8.5.2.	MODBUS Master Protocol Configuration for Direct Representation (%Q)	122
5.8.5.2.1.	General Parameters of MODBUS Master Protocol - setting by Direct Representation(%Q)	122
5.8.5.2.2.	Devices Configuration – Configuration for Direct Representation (%Q)	123
5.8.5.2.3.	Mappings Configuration – Configuration for Direct Representation (%Q)	124
5.8.6.	MODBUS RTU Slave	126
5.8.6.1.	MODBUS Slave Protocol Configuration via Symbolic Mapping	126
5.8.6.1.1.	MODBUS Slave Protocol General Parameters – Configuration via Symbolic Mapping	126
5.8.6.1.2.	Configuration of the Relations – Symbolic Mapping Setting	128
5.8.6.2.	MODBUS Slave Protocol Configuration via Direct Representation (%Q)	129
5.8.6.2.1.	General Parameters of MODBUS Slave Protocol – Configuration via Direct Representation (%Q)	130
5.8.6.2.2.	Mappings Configuration – Configuration via Direct Representation (%Q)	131
5.8.7.	MODBUS Ethernet	132
5.8.8.	MODBUS Ethernet Client	134
5.8.8.1.	MODBUS Ethernet Client Configuration via Symbolic Mapping	134
5.8.8.1.1.	MODBUS Client Protocol General Parameters – Configuration via Symbolic Mapping	135
5.8.8.1.2.	Device Configuration – Configuration via Symbolic Mapping	135
5.8.8.1.3.	Mappings Configuration – Configuration via Symbolic Mapping	137
5.8.8.1.4.	Requests Configuration – Configuration via Symbolic Mapping	138
5.8.8.2.	MODBUS Ethernet Client configuration via Direct Representation (%Q)	141
5.8.8.2.1.	General parameters of MODBUS Protocol Client - configuration for Direct Representation (%Q)	141
5.8.8.2.2.	Device Configuration – Configuration via Direct Representation (%Q)	142
5.8.8.2.3.	Mapping Configuration – Configuration via Direct Representation (%Q)	143
5.8.8.3.	MODBUS Client Relation Start in Acyclic Form	145
5.8.9.	MODBUS Ethernet Server	146
5.8.9.1.	MODBUS Server Ethernet Protocol Configuration for Symbolic Mapping	146
5.8.9.1.1.	MODBUS Server Protocol General Parameters – Configuration via Symbolic Mapping	146
5.8.9.1.2.	MODBUS Server Diagnostics – Configuration via Symbolic Mapping	148
5.8.9.1.3.	Mapping Configuration – Configuration via Symbolic Mapping	148
5.8.9.2.	MODBUS Server Ethernet Protocol Configuration via Direct Representation (%Q)	149
5.8.9.2.1.	General Parameters of MODBUS Server Protocol – Configuration via Direct Representation (%Q)	149
5.8.9.2.2.	Mapping Configuration – Configuration via Direct Representation (%Q)	150
5.8.10.	OPC DA Server	153
5.8.10.1.	Creating a Project for OPC DA Communication	154
5.8.10.2.	Configuring a PLC on the OPC DA Server	157
5.8.10.2.1.	Importing a Project Configuration	159
5.8.10.3.	OPC DA Communication Status and Quality Variables	160
5.8.10.4.	Limits of Communication with OPC DA Server	161
5.8.10.5.	Accessing Data Through an OPC DA Client	161
5.8.11.	OPC UA Server	163
5.8.11.1.	Creating a Project for OPC UA Communication	165
5.8.11.2.	Types of Supported Variables	167
5.8.11.3.	Limit Connected Clients on the OPC UA Server	167
5.8.11.4.	Limit of Communication Variables on the OPC UA Server	167

5.8.11.5.	Encryption Settings	167
5.8.11.6.	Main Communication Parameters Adjusted in an OPC UA Client	168
5.8.11.6.1.	Endpoint URL	168
5.8.11.6.2.	Publishing Interval (ms) and Sampling Interval (ms)	168
5.8.11.6.3.	Lifetime Count and Keep-Alive Count	169
5.8.11.6.4.	Queue Size and Discard Oldest	169
5.8.11.6.5.	Filter Type and Deadband Type	169
5.8.11.6.6.	PublishingEnabled, MaxNotificationsPerPublish and Priority	169
5.8.11.7.	Accessing Data Through an OPC UA Client	170
5.8.12.	EtherCAT Master	171
5.8.12.1.	Installing and inserting EtherCAT Devices	171
5.8.12.1.1.	EtherCAT - Scan Devices	172
5.8.12.2.	EtherCAT Master Settings	173
5.8.12.2.1.	EtherCAT Master - General	173
5.8.12.2.2.	EtherCAT Master - Sync Unit Assignment	174
5.8.12.2.3.	EtherCAT Master - Overview	174
5.8.12.2.4.	EtherCAT Master - I/O Mapping	174
5.8.12.2.5.	EtherCAT Master - IEC Objects	175
5.8.12.2.6.	EtherCAT Master - Status / Information Tabs	175
5.8.12.3.	EtherCAT Slave Configuration	175
5.8.12.3.1.	EtherCAT Slave - General	175
5.8.12.3.2.	EtherCAT Slave - Process Data	178
5.8.12.3.3.	EtherCAT Slave - Edit PDO List	180
5.8.12.3.4.	EtherCAT Slave - Startup Parameters	180
5.8.12.3.5.	EtherCAT Slave - I/O Mapping	180
5.8.12.3.6.	EtherCAT Slave - Status and Information	181
5.8.13.	EtherNet/IP	181
5.8.13.1.	Ethernet Adapter	182
5.8.13.2.	EtherNet/IP Scanner Configuration	184
5.8.13.2.1.	Geral	184
5.8.13.2.2.	Connections	185
5.8.13.2.3.	Assemblies	187
5.8.13.2.4.	User-Defined Parameters	188
5.8.13.2.5.	EtherNet/IP I/O Mapping	190
5.8.13.3.	EtherNet/IP Adapter Configuration	190
5.8.13.3.1.	General	190
5.8.13.3.2.	EtherNet/IP Adapter: I/O Mapping	190
5.8.13.4.	EtherNet/IP Module Configuration	191
5.8.13.4.1.	Assemblies	191
5.8.13.4.2.	EtherNet/IP Module: I/O Mapping	192
5.8.14.	IEC 60870-5-104 Server	192
5.8.14.1.	Type of data	192
5.8.14.2.	Double Points	194
5.8.14.2.1.	Digital Input Double Points	194
5.8.14.2.2.	Digital Output Double Points	195
5.8.14.3.	General Parameters	200
5.8.14.4.	Data Mapping	201
5.8.14.5.	Link Layer	203

5.8.14.6.	Application Layer	205
5.8.14.7.	Server Diagnostic	207
5.8.14.8.	Commands Qualifier	208
5.8.15.	CANOpen Manager	209
5.8.15.1.	Installing and inserting CANopen Devices	210
5.8.15.2.	CANOpen Manager Configuration	210
5.8.15.3.	CANopen Slave Configuration	211
5.8.16.	PROFINET Controller	212
5.9.	Communication Performance	212
5.9.1.	MODBUS Server	212
5.9.1.1.	CPU's Integrated Interfaces	212
5.9.1.2.	Remote Interfaces	213
5.9.2.	OPC UA Server	214
5.9.3.	IEC 60870-5-104 Server	214
5.10.	System Performance	214
5.10.1.	I/O Scan Time	215
5.10.2.	Memory Card	215
5.11.	RTC Clock	215
5.11.1.	Function Blocks for RTC Reading and Writing	216
5.11.1.1.	Function Blocks for RTC Reading	216
5.11.1.1.1.	GetDateAndTime	216
5.11.1.1.2.	GetTimeZone	217
5.11.1.1.3.	GetDayOfWeek	218
5.11.1.2.	RTC Writing Functions	218
5.11.1.2.1.	SetDateAndTime	218
5.11.1.2.2.	SetTimeZone	220
5.11.2.	RTC Data Structure	221
5.11.2.1.	EXTENDED_DATE_AND_TIME	221
5.11.2.2.	DAYS_OF_WEEK	221
5.11.2.3.	RTC_STATUS	222
5.11.2.4.	TIMEZONESETTINGS	222
5.11.3.	RTC Operating Limits	222
5.12.	User Files Memory	223
5.13.	Memory Card	225
5.13.1.	Memory Card Configuration	225
5.13.1.1.	Formatting the Memory Card	226
5.13.1.2.	Unmounting the Memory Card	227
5.13.1.3.	Memory Card Interface Management	229
5.13.1.4.	Memory Card Interface Management by Application	230
5.14.	CPU's Informative and Configuration Menu	231
5.15.	Function Blocks and Functions	233
5.15.1.	Special Function Blocks for Serial Interfaces	233
5.15.1.1.	SERIAL_CFG	236
5.15.1.2.	SERIAL_GET_CFG	238
5.15.1.3.	SERIAL_GET_RX_QUEUE_STATUS	239
5.15.1.4.	SERIAL_PURGE_RX_QUEUE	241
5.15.1.5.	SERIAL_RX	242
5.15.1.6.	SERIAL_RX_EXTENDED	245

5.15.1.7.	SERIAL_SET_CTRL	247
5.15.1.8.	SERIAL_TX	249
5.15.2.	Inputs and Outputs Update	251
5.15.2.1.	REFRESH_INPUT	251
5.15.2.2.	REFRESH_OUTPUT	252
5.15.3.	PID Function Block	253
5.15.4.	Timer Retain	254
5.15.4.1.	TOF_RET	254
5.15.4.2.	TON_RET	255
5.15.4.3.	TP_RET	257
5.15.5.	User Log	258
5.15.5.1.	UserLogAdd	259
5.15.5.2.	UserLogDeleteAll	260
5.15.6.	ClearRtuDiagnostic	261
5.15.7.	ClearEventQueue	261
5.16.	User Web Pages	262
5.17.	SNMP	262
5.17.1.	SNMP on Nexto CPUs	262
5.17.2.	SNMP Configuration	263
5.17.3.	User and SNMP Communities	264
5.18.	FTP Server	265
5.18.1.	Configuration	265
5.18.1.1.	General Configuration	266
5.18.1.1.1.	Enable Server	266
5.18.1.1.2.	Enable Encrypted Communication (FTPS)	266
5.18.1.1.3.	Read-only Access	266
5.18.1.1.4.	Idle Timeout (Seconds)	266
5.18.1.2.	User Configuration	266
5.18.1.2.1.	Username	266
5.18.1.2.2.	Password	267
5.18.1.3.	Status	267
5.18.1.3.1.	Current State	267
5.18.1.3.2.	Connected Clients	267
5.19.	Firewall	267
5.19.1.	Configuration	267
5.19.2.	General Configuration	268
5.19.3.	User Rules	269
5.20.	OpenVPN	271
5.20.1.	Import Configuration	272
5.20.2.	OpenVPN Configuration	273
5.20.2.1.	Common Configurations	274
5.20.2.1.1.	Mode	274
5.20.2.1.2.	Protocol	274
5.20.2.1.3.	Logs level	274
5.20.2.1.4.	Keep Alive Ping	274
5.20.2.1.5.	Keep Alive Timeout	274
5.20.2.1.6.	Security Files	274
5.20.2.1.7.	TA Key	275

5.20.2.2.	Exclusive Server Configurations	275
5.20.2.2.1.	Network Address	275
5.20.2.2.2.	Communication between Clients	275
5.20.2.2.3.	Maximum Connected Clients	275
5.20.2.2.4.	Private Networks	275
5.20.2.3.	Exclusive Client Configurations	277
5.20.2.3.1.	Remote IP	277
5.20.2.4.	Application Settings	277
5.20.3.	Security Files	277
5.20.4.	Status Table	278
5.20.5.	Files to Download	280
5.20.6.	Architectures Configuration	280
5.20.6.1.	Host-to-Host	280
5.20.6.2.	Host-to-Site	281
5.20.6.3.	Site-to-Site	281
5.21.	Docker	282
5.21.1.	How to access a Docker Container	282
5.21.1.1.	How to access Portainer	282
5.21.2.	Quick Setup	283
5.21.2.1.	Local Environment Informations	284
5.21.3.	Environment's Dashboard	284
5.21.3.1.	Containers Menu	285
5.21.3.2.	Images Menu	285
5.21.4.	Creating and Configuring a Container	286
5.21.4.1.	Configuring a Container	287
5.21.4.1.1.	Command & Logging Menu	287
5.21.4.1.2.	Network Menu	287
5.21.4.1.3.	Runtime & Resources Menu	288
5.21.4.1.4.	Capabilities Menu	288
5.21.4.2.	Using a Container	289
5.21.4.3.	How to create an image of an existing container to backup its data	290
5.21.4.4.	Monitoring a Container	291
5.21.4.5.	Technical Characteristics	291
5.21.4.5.1.	Flash Memory	291
5.21.4.5.2.	RAM Memory	291
5.21.4.5.3.	CPU	292
5.21.4.6.	How to access the Docker's folders	292
5.21.4.6.1.	Mastertool	292
5.21.4.7.	Using External Memory as Docker Volumes	292
5.21.4.8.	Troubleshooting	293
5.21.4.8.1.	Container Installation Failure due to expired or not valid Certificate	293
5.21.4.8.2.	Portainer is inaccessible, returning after CPU reboot	293
6.	Maintenance	294
6.1.	Module Diagnostics	294
6.1.1.	One Touch Diag	294
6.1.2.	Diagnostics via LED	296
6.1.2.1.	DG (Diagnostic)	296
6.1.2.2.	WD (Watchdog)	297

6.1.2.3.	RJ45 Connector LEDs	297
6.1.3.	Diagnostics via System Web Page	297
6.1.4.	Diagnostics via Variables	300
6.1.4.1.	Summarized Diagnostics	300
6.1.4.2.	Detailed Diagnostics	302
6.1.4.2.1.	Target Detailed Diagnostics Group	302
6.1.4.2.2.	Hardware Detailed Diagnostics Group	302
6.1.4.2.3.	Exception Detailed Diagnostics Group	303
6.1.4.2.4.	WebVisualization Detailed Diagnostics Group	303
6.1.4.2.5.	RetainInfo Detailed Diagnostics Group	304
6.1.4.2.6.	Reset Detailed Diagnostics Group	304
6.1.4.2.7.	Thermometer Detailed Diagnostics Group	304
6.1.4.2.8.	Serial Detailed Diagnostics Group	305
6.1.4.2.9.	CAN Detailed Diagnostics Group	305
6.1.4.2.10.	USB Detailed Diagnostics Group	305
6.1.4.2.11.	Ethernet Detailed Diagnostics Group	306
6.1.4.2.12.	UserFiles Detailed Diagnostics Group	308
6.1.4.2.13.	UserLogs Detailed Diagnostics Group	308
6.1.4.2.14.	MemoryCard Detailed Diagnostics Group	308
6.1.4.2.15.	WHSB Detailed Diagnostics Group	308
6.1.4.2.16.	Application Detailed Diagnostics Group	310
6.1.4.2.17.	Rack Detailed Diagnostics Group	310
6.1.4.2.18.	ApplicationInfo Detailed Diagnostics Group	310
6.1.4.2.19.	SNTP Detailed Diagnostics Group	310
6.1.5.	Diagnostics via Function Blocks	311
6.1.5.1.	GetTaskInfo	311
6.2.	Graphic Display	312
6.3.	System Log	314
6.4.	Not Loading the Application at Startup	314
6.5.	Common Problems	314
6.6.	Troubleshooting	315
6.7.	Preventive Maintenance	315
7.	Appendixes	316
7.1.	TLS Key and Certificate Management	316
7.1.1.	Easy-RSA Certificate Generation	316
7.1.2.	OpenSSL Certificate Generation	320
7.1.3.	TA Key Generation by OpenVPN	322

1. Introduction

Nexto Series programmable controllers are the ultimate solution for industrial automation and system control. With high technology embedded, the products of the family are able to control, in a distributed and redundant way, complex industrial systems, machines, high performance production lines and the most advanced processes of Industry 4.0. Modern and high-speed, the Nexto series uses cutting-edge technology to provide reliability and connectivity, helping to increase the productivity of different businesses.

Compact, robust and with high availability, the series products have excellent processing performance and rack expansion possibilities. Its architecture allows easy integration with supervision, control and field networks, in addition to PLC redundancy. The series equipment also offers advanced diagnostics and hot swapping, minimizing or eliminating maintenance downtime and ensuring a continuous production process.

With a powerful 64-bit, 1 GHz ARM processor, the CPU NX3008 is ideal for controlling small to large industrial machines and processes. In addition to advanced diagnostics and the diversity of consolidated communication protocols, it has cybersecurity resources, firewall, remote operation and the ability to customize the user's application with the installation of external programs, thanks to the Docker platform and the Linux operating system used on all Nexto Series controllers.



Figure 1: NX3008

1.1. Nexto Series

Nexto Series is a powerful and complete series of Programmable Controllers (PLC) with exclusive and innovative characteristics. Due to its flexibility, functional design, advanced diagnostic resources and modular architecture, the Nexto PLC can be used to control systems in small, medium and large scale applications.

Nexto Series architecture has a great variety of input and output modules. These modules combined with a powerful processor and a high speed bus based on Ethernet, fit to several application kinds as high speed control for small machines, complex distributed processes, redundant applications and systems with a great number of I/O as building automation. Furthermore, Nexto Series has modules for motion control, communication modules encompassing the most popular field networks among other features.

Nexto Series uses an advanced technology in its bus, which is based on a high speed Ethernet interface, allowing input and output information and data to be shared between several controllers inside the same system. The system can be easily divided and distributed throughout the whole field, allowing the use of bus expansion with the same performance of a local module, turning possible the use of every module in the local frame or in the expansion frames with no restrictions. For interconnection between frames expansions a simple standard Ethernet cable is used.



Figure 2: Nexto Series – Overview

1.2. Innovative Features

Nexto Series brings to the user many innovations regarding utilization, supervision and system maintenance. These features were developed focusing a new concept in industrial automation.



VPN: Nexto products have an embedded VPN service, which creates a private tunnel that connects directly to the CPU. This functionality, available on some models of the family, allows accessing a control network remotely and completely securely..



FTP: Supporting FTP-type connections, the series equipment is able to exchange data with a server that uses this same technology model. This functionality allows the files generated by the controller, such as logs collected through a datalogger function, to be accessed remotely.



Linux: Another innovative feature of the series is its embedded Linux platform. The feature makes possible the virtualization of software developed for operating systems with Unix technology. The feature gives more versatility and speed to the operation of the system, as it allows the processing of multiple data within the CPU itself.



Battery Free Operation: Nexto Series does not require any kind of battery for memory maintenance and real time clock operation. This feature is extremely important because it reduces the system maintenance needs and allows the use in remote locations where maintenance can be difficult to be performed. Besides, this feature is environmentally friendly.



Easy Plug System: Nexto Series has an exclusive method to plug and unplug I/O terminal blocks. The terminal blocks can be easily removed with a single movement and with no special tools. In order to plug the terminal block back to the module, the frontal cover assists the installation procedure, fitting the terminal block to the module.



Multiple Block Storage: Several kinds of memories are available to the user in Nexto Series CPUs, offering the best option for any user needs. These memories are divided in volatile memories and non-volatile memories. For volatile memories, Nexto Series CPUs offer addressable input (%I), addressable output (%Q), addressable memory (%M), data memory and redundant data memory. For applications that require non-volatile functionality, Nexto Series CPUs bring retain addressable memory (%Q), retain data memory, persistent addressable memory (%Q), persistent data memory, program memory, source code memory, CPU file system (doc, PDF, data) and memory card interface.



One Touch Diag: One Touch Diag is an exclusive feature that Nexto Series brings to PLCs. With this new concept, the user can check diagnostic information of any module present in the system directly on CPU's graphic display with one single press in the diagnostic switch of the respective module. OTD is a powerful diagnostic tool that can be used offline (without supervisor or programmer), reducing maintenance and commissioning times.

OFD – On Board Full Documentation: Nexto Series CPUs are capable of storing the complete project documentation in its own memory. This feature can be very convenient for backup purposes and maintenance, since the complete information is stored in a single and reliable place.

ETD – Electronic Tag on Display: Another exclusive feature that Nexto Series brings to PLCs is the Electronic Tag on Display. This new functionality brings the process of checking the tag names of any I/O pin or module used in the system directly to the CPU’s graphic display. Along with this information, the user can check the description, as well. This feature is extremely useful during maintenance and troubleshooting procedures.

DHW – Double Hardware Width: Nexto Series modules were designed to save space in user cabinets or machines. For this reason, Nexto Series delivers two different module widths: Double Width (two backplane rack slots are required) and Single Width (only one backplane rack slot is required). This concept allows the use of compact I/O modules with a high-density of I/O points along with complex modules, like CPUs, fieldbus masters and power supply modules.

High-speed CPU: All Nexto Series CPUs were designed to provide an outstanding performance to the user, allowing the coverage of a large range of applications requirements.

1.3. Documents Related to this Manual

In order to obtain additional information regarding the Nexto Series, other documents (manuals and technical features) besides this one, may be accessed. These documents are available in its last version on the site <https://www.altus.com.br/en/>.

Each product has a document designed by Technical Features (CE), where the product features are described. Furthermore, the product may have Utilization Manuals (the manuals codes are listed in the CE).

It is advised the following documents as additional information source:

Code	Description	Language
CE114000 CT114000	Nexto Series – Technical Characteristics Série Nexto – Características Técnicas	English Portuguese
CE114109 CT114109	NX3008 Technical Characteristics Características Técnicas NX3008	English Portuguese
CE114700 CT114700	Nexto Series Backplane Racks Technical Characteristic Características Técnicas dos Bastidores da Série Nexto	English Portuguese
CE114810 CT114810	Nexto Series Accessories for Backplane Rack Technical Characteristics Características Técnicas Acessórios para Bastidor Série Nexto	English Portuguese
CE114902 CT114902	Nexto Series PROFIBUS-DP Master Technical Characteristics Características Técnicas do Mestre PROFIBUS-DP da Série Nexto	English Portuguese
CE114908 CT114908	NX5110 and NX5210 PROFIBUS-DP Heads Technical Characteristics Características Técnicas Interfaces Cabeça PROFIBUSDP NX5110 e NX5210	English Portuguese
MU214600 MU214000	Nexto Series User Manual Manual de Utilização Série Nexto	English Portuguese
MU214620 MU214109	NX3008 CPU User Manual Manual de Utilização UCP NX3008	English Portuguese
MU299609 MU299048	MasterTool IEC XE User Manual Manual de Utilização MasterTool IEC XE	English Portuguese
MP399609 MP399048	MasterTool IEC XE Programming Manual Manual de Programação MasterTool IEC XE	English Portuguese
MU214601 MU214001	NX5001 PROFIBUS DP Master User Manual Manual de Utilização Mestre PROFIBUS-DP NX5001	English Portuguese
MU214608 MU214108	Nexto PROFIBUS-DP Head Utilization Manual Manual de Utilização da Cabeça PROFIBUS-DP Nexto	English Portuguese

Code	Description	Language
MU214603	Nexto Series HART Manual	English
MU214606	MQTT User Manual	English
MU214609	OPC UA Server for Altus Controllers User Manual	English
MU214610	PID - Advanced Control Functions User Manual	English
MU214621	Nexto Series PROFINET Manual	English
MU223603	IEC 60870-5-104 Server Device Profile Document	English
NAP151	Utilização do Tunneller OPC	Portuguese
NAP169	RSTP in Nexto CPUs	English

Table 1: Related documents

1.4. Visual Inspection

Before resuming the installation process, it is advised to carefully visually inspect the equipment, verifying the existence of transport damage. Verify if all parts requested are in perfect shape. In case of damages, inform the transport company or Altus distributor closest to you.

CAUTION

Before taking the modules off the case, it is important to discharge any possible static energy accumulated in the body. For that, touch (with bare hands) on any metallic grounded surface before handling the modules. Such procedure guarantees that the module static energy limits are not exceeded.

It's important to register each received equipment serial number, as well as software revisions, in case they exist. This information is necessary, in case the Altus Technical Support is contacted.

1.5. Technical Support

To contact Altus Technical Support, send an email to support@altusautomation.com or visit our website at www.altusautomation.com/support. If the equipment is already installed, please have the following information available when requesting assistance:

- Model of the equipment used and the installed system configuration
- Product serial number
- Equipment revision and executive software version, indicated on the label attached to the side of the product
- CPU operating mode information, obtained using the programming tool
- Application software content, obtained using the programming tool
- Programming tool version used

1.6. Warning Messages Used in this Manual

In this manual, the warning messages will be presented in the following formats and meanings:

DANGER

Reports potential hazard that, if not detected, may be harmful to people, materials, environment and production.

CAUTION

Reports configuration, application or installation details that must be taken into consideration to avoid any instance that may cause system failure and consequent impact.

ATTENTION

Identifies configuration, application and installation details aimed at achieving maximum operational performance of the system.

2. Technical Description

This chapter presents all technical features from Nexto Series CPU NX3008.

2.1. Panels and Connections

The following figure shows the CPU front panel.



Figure 3: NX3008

As it can be seen on the figure, on the front panel upper part is placed the graphic display used to show the whole system status and diagnostics, including the specific diagnostics of each module. The graphic display also offers an easy-to-use menu which brings to the user a quick mode for parameters reading or defining, such as: inner temperature (reading only) and local time (reading only).

Just below the graphic display, there are 2 LEDs used to indicate alarm diagnostics and watchdog circuit. The table below shows the LEDs description. For further information regarding the LEDs status and meaning, see [Diagnostics via LED](#) section.

LED	Description
DG	Diagnostics LED
WD	Watchdog LED

Table 2: LEDs Description

Nexto Series CPUs has two switches available to the user. The table below shows the description of these switches. For further information regarding the diagnostics switch, see sections [One Touch Diag](#).

Keys	Description
Diagnostics Switch	Switch placed on the module upper part. Used for diagnostics visualization on the graphic display or for navigation through the informative menu and CPU configuration.

Table 3: Keys Description

On the frontal panel the connection interfaces of Nexto Series CPUs are available. The table below presents a brief description of these interfaces.

Interfaces	Description
NET 1..NET 3	RJ45-type connector for standard 10/100/1000Base-TX communication. Allows point-to-point or network communication. For more information on usage, see the section Ethernet Interfaces Configuration .
COM 1	For further utilization information, see Serial Interfaces Configuration section.
CAN	For further utilization information, see CAN Interface Configuration (Controller Area Network) section.
MEMORY SLOT	Memory Card connector. Allows you to use a memory card for different types of data storage such as user logs, project documentation, and source files. For more usage information, see the section, Memory Card .
USB HOST	For further utilization information, see USB Interface Configuration section.

Table 4: Connection Interfaces

2.2. Product Features

2.2.1. General Features

	NX3008
Backplane rack occupation	2 sequential slots
Current consumption from backplane rack	-
Power supply integrated	Yes
Ethernet TCP/IP integrated interface	3
Serial Interface	1
CAN Interface	1
USB Port Host	1
Memory Card Interface	1
Real time clock (RTC)	Yes Resolution of 1 ms and maximum variance of 2 s per day.
Watchdog	Yes
Status and diagnostic Indication	Graphic display LEDs System Web Page CPU internal memory
Programming languages	Structured Text (ST) Ladder Diagram (LD) Sequential Function Chart (SFC) Function Block Diagram (FBD) Continuous Function Chart (CFC)

	NX3008
Tasks	Cyclic (periodic) Event (software interruption) External (hardware interruption) Freewheeling (continuous) Status (software interruption)
Online changes	Yes
Maximum number of tasks	24
Maximum number of expansion bus	24
Bus expansion redundancy support	Yes
Maximum number of I/O modules on the bus	128
Maximum number of additional Ethernet TCP/IP interface modules	2
Ethernet TCP/IP interface redundancy support	Yes
Maximum number of PROFIBUS-DP network (using master modules PROFIBUS-DP)	4
PROFIBUS-DP network redundancy support	Yes
Redundancy support (half-clusters)	No
Hot Swap support	Yes
Event oriented data reporting (SOE) Protocol	No
Maximum Event Queue Size	-
User web pages (Webvisu)	Yes
Firewall	Yes
Docker	Yes
One Touch Diag (OTD)	Yes
Electronic Tag on Display (ETD)	Yes

Table 5: Common Features

Notes:

Real Time Clock (RTC): The retention time, time that the real time clock will continue to update the date and time after a CPU power down, is 15 days for operation at 25 °C. At the maximum product temperature, the retention time is reduced to 10 days.

Maximum number of I/O modules on bus: The maximum number of I/O modules refers to the sum of all modules on the local bus and expansions.

2.2.2. Standards and Certifications

Standards and Certifications	
IEC	<p>61131-2: Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests</p> <p>61131-3: Programmable controllers - Part 3: Programming languages</p>
	DNV Type Approval – DNV-CG-0339 (TAA000013D)
CE	<p>2014/30/EU (EMC)</p> <p>2014/35/EU (LVD)</p> <p>2011/65/EU and 2015/863/EU (ROHS)</p>
UK CA	<p>S.I. 2016 No. 1091 (EMC)</p> <p>S.I. 2016 No. 1101 (Safety)</p> <p>S.I. 2012 No. 3032 (ROHS)</p>
	<p>UL/cUL Listed – UL 61010-1</p> <p>UL 61010-2-201 (file E473496)</p>
EAC	<p>TR 004/2011 (LVD)</p> <p>CU TR 020/2011 (EMC)</p>

Table 6: Standards and Certifications

2.2.3. Memory

	NX3008
Addressable input variables memory (%I)	64 Kbytes
Addressable output variables memory (%Q)	64 Kbytes
Direct representation variable memory (%M)	32 Kbytes
Symbolic variable memory	24 Mbytes
Maximum amount of memory configurable as retentive or persistent	1 Mbytes
Full Redundant Data Memory	-
Direct representation input variable memory (%I)	-
Direct representation output variable memory (%Q)	-
Direct representation variable memory (%M)	-
Symbolic variable memory	-
Total memory	256 Mbytes
Program memory (limited to 32 MBytes) + Source code memory (backup) + Webvisu files memory	
User files memory	4 Gbytes
CPU Memory + Docker Memory	

Table 7: Memory

Notes:

Addressable input variables memory (%I): Area where the addressable input variables are stored. Addressable variables means that the variables can be accessed directly using the desired address. For instance: %IB0, %IW100. Addressable input variables can be used for mapping digital or analog input points. As reference, 8 digital inputs can be represented per byte and one analog input point can be represented per two bytes.

Total addressable output variables memory (%Q): Area where the addressable output variables are stored. Addressable variables means that the variables can be accessed directly using the desired address. For instance: %QB0, %QW100. Addressable output variables can be used for mapping digital or analog output points. As reference, 8 digital outputs can be represented per byte and one analog output point can be represented per two bytes. The addressable output variables can be configured as retain, persistent or redundant variables, but the total size is not modified due to configuration.

Addressable variables memory (%M): Area where the addressable marker variables are stored. Addressable variables means that the variables can be accessed directly using the desired address. For instance: %MB0, %MW100.

Symbolic variables memory: Area where the symbolic variables are allocated. Symbolic variables are IEC variables created in POU's and GVL's during application development, which are not addressed directly in memory. Symbolic variables can be defined as retentive or persistent, in which case the memory areas of retentive symbolic variables or memory of persistent symbolic variables respectively will be used. The PLC system allocates variables in this area, so the space available for the allocation of variables created by the user is lower than that reported in the table. The occupation of the system variables depends on the characteristics of the project (number of modules, drivers, etc...), so it is recommended to observe the space available in the compilation messages of the MasterTool IEC XE tool.

Persistent or Retain symbolic variables memory: Area where are allocated the retentive symbolic variables. The retentive data keep its respective values even after a CPU's cycle of power down and power up. The persistent data keep its respective values even after the download of a new application in the CPU.

ATTENTION

The declaration and use of symbolic persistent variables should be performed exclusively through the *Persistent Vars* object, which may be included in the project through the tree view in *Application* -> *Add Object* -> *Persistent Variables*. It should not be used to *VAR PERSISTENT* expression in the declaration of field variables of POU's.

The full list of when the symbolic persistent variables keep their values and when the value is lost can be found in the table below. Besides the persistent area size declared in the table above, are reserved these 44 bytes to store information about the persistent variables (not available for use).

2. TECHNICAL DESCRIPTION

The table below shows the behavior of retentive and persistent variables for different situations in which “-“ means the value is lost and “X” means the value is kept.

Command/Operation	VAR	VAR RETAIN	VAR PERSISTENT
Power cycle	-	X	X
Reset warm	-	X	X
Reset cold	-	-	X
Reset origin	-	-	-
Remove CPU with integrated power supply from the rack while powered on	-	X	X
Remove the power supply or a CPU without integrated power supply from the rack while powered on	-	-	-
Download	-	-	X
Online change	X	X	X
Clean All	-	-	X
Reset Process (IEC 60870-5-104)	-	X	X
Runtime Reset	-	-	-

Table 8: Variables Behavior after the Event

In the case of Clean All command, if the application has been modified so that persistent variables have been removed, inserted into the top of the list or otherwise have had its modified type, the value of these variables is lost (when prompted by the tool MasterTool to download). Thus it is recommended that changes to the persistent variables GVL only include adding new variables on the list.

Program memory: Program memory is the maximum size that can be used to store the user application. This area is shared with source code memory, being the total area the sum of (Program Memory + Source Code Memory + Compilation Memory).

Source code memory (backup): This memory area is used as project backup. If the user wants to import the project, MasterTool IEC XE will get the information required in this area. Care must be taken to ensure that the project saved as a backup is up to date to avoid the loss of critical information. This area is shared with source code memory, being the total area the sum of (Program Memory + Source Code Memory).

User files memory: This memory area offers another way for the user to store files such as doc, pdf, images, and other files. This function allows data recording as in a memory card. For further information check [User Files Memory](#) section.

2.2.4. Protocols

	NX3008	Interface
Communication with programming software	Yes	NET 1 / NET 2 / NET 3 / USB
Open Protocol	Yes	COM 1 / USB
MODBUS RTU Master	Yes	COM 1
MODBUS RTU Slave	Yes	COM 1
MODBUS TCP Client	Yes	NET 1 / NET 2 / NET 3
MODBUS TCP Server	Yes	NET 1 / NET 2 / NET 3
MODBUS RTU over TCP Client	Yes	NET 1 / NET 2 / NET 3
MODBUS RTU over TCP Server	Yes	NET 1 / NET 2 / NET 3
CANopen Master	Yes	CAN
CANopen Slave	No	-
CAN low level	Yes	CAN
SAE J-1939	Yes	CAN
OPC DA Server	Yes	NET 1 / NET 2 / NET 3

2. TECHNICAL DESCRIPTION

	NX3008	Interface
OPC UA Server	Yes	NET 1 / NET 2 / NET 3
EtherCAT Master	Yes	NET 1 / NET 2 / NET 3
SNMP Agent	Yes	NET 1 / NET 2 / NET 3
SOE (Event-oriented data)	No	-
IEC 60870-5-104 Server	Yes	NET 1 / NET 2 / NET 3
EtherNet/IP Scanner	Yes	NET 1 / NET 2 / NET 3
EtherNet/IP Adapter	Yes	NET 1 / NET 2 / NET 3
MQTT Client	Yes	NET 1 / NET 2 / NET 3 / USB
SNTP Client (for clock synchronism)	Yes	NET 1 / NET 2 / NET 3 / USB
PROFINET Controller	Yes	NET 1 / NET 2 / NET 3
PROFINET Device	No	-
OpenVPN Client	Yes	NET 1 / NET 2 / NET 3
OpenVPN Server	Yes	NET 1 / NET 2 / NET 3
FTP Server	Yes	NET 1 / NET 2 / NET 3 / USB
RSTP	Yes	NET 2 / NET 3
MRP	Yes	NET 2 / NET 3

Table 9: Protocols

Note:

USB: Need to use Serial, WiFi or Modem adapter.

Communication with programming software: To communicate with the CPU from an interface other than NET 1, it is necessary to add a gateway with the IP address of the given interface.

2.2.5. Serial Interfaces

2.2.5.1. COM 1

	COM 1
Connector	Terminal block, D+ and D- with shield
Physical interface	RS-485
Communication direction	half duplex
RS-485 max. transceivers	32
Termination	Yes (optional through parameter)
Cross section	0.5 mm ²
Baud rate	2400, 4800, 9600, 19200, 38400, 57600, 115200 bps
Isolation	
Logic to Serial Port	1000 Vac / 1 minute
Serial Port to protection earth ⊕	1000 Vac / 1 minute

Table 10: COM 1 Serial Interface Features

Note:

RS-485 maximum transceivers: It is the maximum number of RS-485 interfaces that can be used on the same bus.

2.2.6. CAN Interface

	CAN
Connector	Terminal block, H and L with shield
Physical interface	CAN bus
Supported standards	CAN 2.0A 2.0B (11-bit and 29-bit identifiers)
Max. number of nodes	64
Termination	Yes (Configurable)
Cross section	0.5 mm ²
Baud rate	10, 20, 50, 100, 125, 250, 500, 1000 kbit/s
Isolation	
Logic to CAN	1000 Vac / 1 minute
CAN to protection earth ⚡	1000 Vac / 1 minute

Table 11: CAN Interface Features

2.2.7. USB Interface

	USB
Connector	USB A Female
Physical interface	USB V2.0
Baud rate	1.5 Mbps (Low-Speed), 12 Mbps (Full-Speed) and 480 Mbps (Hi-Speed)
Maximum current	500 mA
Supported devices	Mass storage USB RS-232 Serial Converter USB 3G/4G Modem USB WiFi Adapter
Isolation	
Logic to USB	Not isolated
USB to protection earth ⚡	1000 Vac / 1 minute

Table 12: USB Interface Features

Notes:

USB RS-232 serial converter: See the list of supported devices in the [USB to RS-232 Converter](#) section.

USB 3G/4G Modem: See the list of supported devices in the [Modem Devices](#) section.

USB WiFi Adapter: See the list of supported devices in the [WiFi Adapters](#) section.

ATTENTION:

The CPU supports the use of only one USB device at a time. Devices such as USB HUBs, for example, are not supported.

2.2.8. Ethernet Interfaces

2.2.8.1. NET 1

	NET 1
Connector	Shielded female RJ45
Auto crossover	Yes
Maximum cable length	100 m
Cable type	UTP or ScTP, category 5
Baud rate	10/100/1000 Mbps
Physical layer	10BASE-Te/100BASE-TX/1000BASE-T
Data link layer	LLC (Logical Link Control)
Network layer	IP (Internet Protocol)
Transport layer	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Diagnostics	LED - green 1000 Mbps (link/activity) LED – yellow 100 Mbps (link/activity) LEDs – green and yellow 10 Mbps (link/activity)
Isolation	
Ethernet interface to logic	1500 Vac / 1 minute
Ethernet interface to Ethernet interface	1500 Vac / 1 minute
Ethernet interface to protection earth ⚡	1500 Vac / 1 minute

Table 13: Ethernet NET 1 Interface Features

ATTENTION:

NET1 does not supports 4 wire cables, requiring a complete CAT5 cable.

2.2.8.2. NET 2

	NET 2
Connector	Shielded female RJ45
Auto crossover	Yes
Maximum cable length	100 m
Cable type	UTP or ScTP, category 5
Baud rate	10/100 Mbps
Physical layer	10BASE-Te/100BASE-TX
Data link layer	LLC (Logical Link Control)
Network layer	IP (Internet Protocol)
Transport layer	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Diagnostics	LED – yellow 100 Mbps (link/activity) LEDs – green and yellow 10 Mbps (link/activity)
Isolation	
Ethernet interface to logic	1500 Vac / 1 minute
Ethernet interface to Ethernet interface	1500 Vac / 1 minute
Ethernet interface to protection earth 	1500 Vac / 1 minute

Table 14: Ethernet NET 2 Interface Features

2.2.8.3. NET 3

	NET 3
Connector	Shielded female RJ45
Auto crossover	Yes
Maximum cable length	100 m
Cable type	UTP or ScTP, category 5
Baud rate	10/100 Mbps
Physical layer	10BASE-Te/100BASE-TX
Data link layer	LLC (Logical Link Control)
Network layer	IP (Internet Protocol)
Transport layer	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Diagnostics	LED – yellow 100 Mbps (link/activity) LEDs – green and yellow 10 Mbps (link/activity)
Isolation	
Ethernet interface to logic	1500 Vac / 1 minute
Ethernet interface to Ethernet interface	1500 Vac / 1 minute
Ethernet interface to protection earth 	1500 Vac / 1 minute

Table 15: Ethernet NET 3 Interface Features

2.2.9. Memory Card Interface

The memory card can be used for different data to be stored such as user logs, project documentation and source files.

	Memory Card
Maximum Capacity	32 Gbytes
Minimum Capacity	2 Gbytes
Type	MicroSD
File System	FAT32
Remove card safely	Yes, through a specific menu for this function.

Table 16: Memory Card Interface Features

Notes:

Maximum Capacity: The memory card capacity must be less than or equal to this limit for correct operation on Nexto CPU, otherwise the Nexto CPU may not detect the memory card or even present problems during data transfer.

Minimum Capacity: The memory card capacity must be greater than or equal to this limit for correct operation on Nexto CPU, otherwise the Nexto CPU may not detect the memory card or even present problems during data transfer.

File System: It is recommended to format the memory card using the Nexto CPU, otherwise it may result in performance loss in the memory card interface.

2.2.10. Power Supply

Nominal input voltage	24 Vdc
Maximum output power	15W ^{1,2}
Maximum output current	3 A ¹
Input voltage	18 to 30 Vdc
Maximum input current (in-rush)	15 A
Maximum input current	1,5 A ¹
Maximum input voltage interruption	10 ms @ 24 Vdc
Isolation	
Input to logic	1000 Vac / 1 minute
Input to protective earth 	1000 Vac / 1 minute
Cross section	0.5 mm ²
Polarity inversion protection	Yes
Internal fuse	Yes
Output short-circuit protection	No
Overcurrent protection	No

Table 17: Power Supply Features

Notes:

¹ **Maximum output power/current:** For use with an extended maximum output power/current of 20W/4A, certain conditions must be met: use Nexto Jet I/O modules only; reduce the maximum ambient operating temperature to 50°C; do not hot-swap I/O modules, as this may affect the system's operation; NJ6000, NJ6010 and NJ6100 modules must be of revision AB or higher. In this case, the Maximum Input Current information becomes 2.0A.

² **NX8000 support:** Operation of the NX3008 with NX8000 support feeding the bus is intended to extend the maximum output power/current to 30W/6A. To do this, certain conditions must be met: these are detailed in the section [Using a NX8000 power supply module](#).

2.2.11. Environmental Characteristics

Dissipation	9 W
Operating temperature	-20 to 60 °C @ 15W -20 to 50 °C @ 20W
Storage temperature	-40 to 75 °C
Relative humidity	5% to 96%, non-condensing
Conformal coating	Yes
IP Level	IP 20
Module dimensions (W x H x D)	36,00 x 114,63 x 115,30 mm
Package dimensions (W x H x D)	44,00 x 122,00 x 147,00 mm
Weight	330 g
Weight with package	380 g

Table 18: Environmental Characteristics

Note:

Conformal coating of electronic circuits: The covering of electronic circuits protects internal parts of the product against moisture, dust and other harsh elements to electronic circuits.

2.3. Compatibility with Other Products

To develop an application for Nexto Series CPUs, it is necessary to check the version of MasterTool IEC XE. The following table shows the minimum version required (where the controllers were introduced) and the respective firmware version at that time:

Nexto Series CPUs	MasterTool IEC XE	Firmware version
NX3008	3.40 or above	1.10.0.0 or above

Table 19: Compatibility with other products

Additionally, along the development roadmap of MasterTool IEC XE some features may be included (like special Function Blocks, etc...), which can introduce a requirement of minimum firmware version. During the download of the application, MasterTool IEC XE checks the firmware version installed on the controller and, if it does not meets the minimum requirement, will show a message requesting to update. The latest firmware version can be downloaded from Altus website, and it is fully compatible with previous applications.

2.4. Performance

The Nexto Series CPUs performance relies on:

- User Application Time
- Application Interval
- Operational System Time
- Module quantity (process data, input/output, among others)

2.4.1. MainTask Interval Time

The MainTask interval time setting depends on the selected project profile. For the profiles Simple, Normal, Experienced, and Custom profiles, the interval can be set with values from 1 ms to 750 ms. For the Machine Machine Profile, the interval can be configured with values from 1 ms to 100 ms.

2.4.2. Application Times

The execution time of Nexto CPUs application depends on the following variables:

- Input read time (local and remote)
- Tasks execution time
- Output write time (local and remote)

It is important to stress that the execution time of the “MainTask” will be directly influenced by the “Configuration” system task, a task of high priority, executed periodically by the system. The “Configuration” task may interrupt the “MainTask” and, when using the communication modules, as the Ethernet NX5000 module, for instance, the time addition to the “MainTask” may be up to 25% of the execution average time.

2.4.3. Time for Instructions Execution

The table below presents the necessary execution time for different instructions.

Instruction	Language	Variable Type	Time (μ s)
1000 Contacts	LD	BOOL	2,1
1000 Divisions	LD, ST	INT	9,2
		REAL	17,0
1000 Multiplications	LD, ST	INT	6,4
		REAL	8,2
1000 Sums	LD, ST	INT	4,4
		REAL	8,2

Table 20: Instruction Times

2.4.4. Initialization Times

Nexto Series CPUs have initialization times of 30 s, and the initial screen with the NEXTO logo (Splash) is presented after 2 s from the power switched on.

2.5. Physical Dimensions

Dimensions in mm.

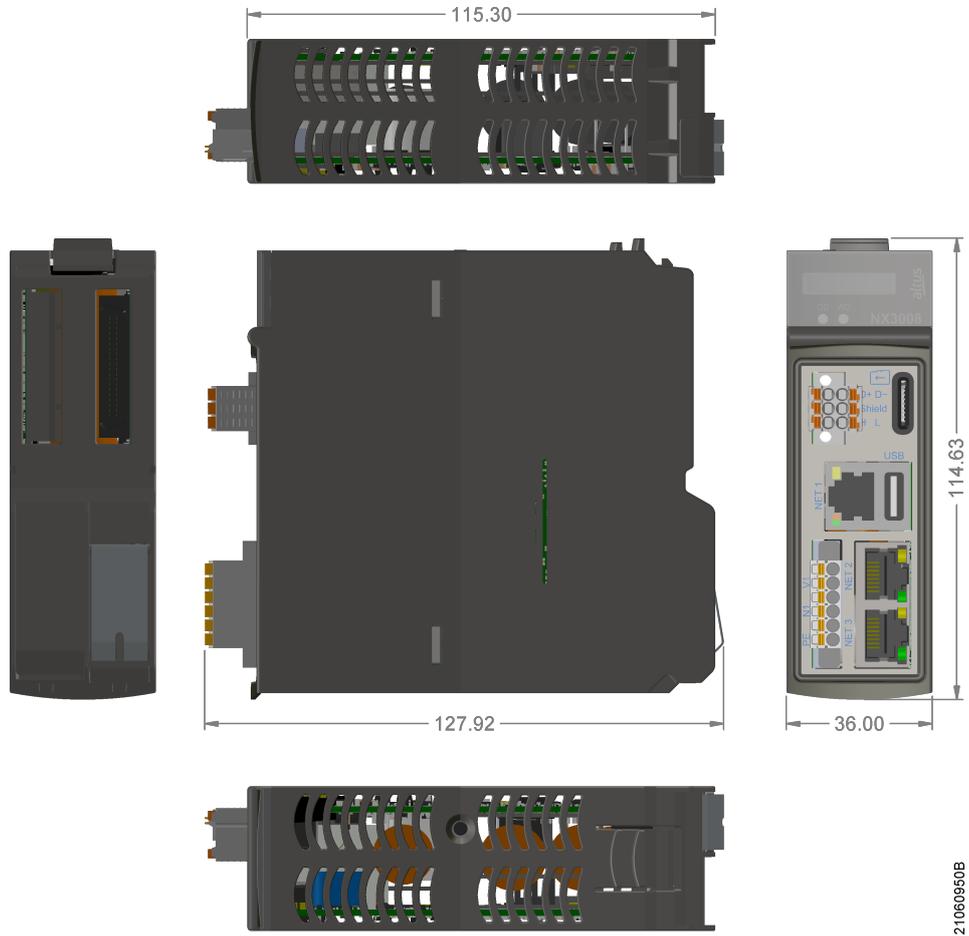


Figure 4: Dimensions in mm.

2.6. Purchase Data

2.6.1. Included Items

The product package contains the following items:

- NX3008 module
- 6-terminal connector with fixing
- 2x3 connector with fixing

2.6.2. Product code

The following code should be used to purchase the product:

Code	Description
NX3008	CPU, 3 Ethernet port, 1 USB, 1 serial, 1 CAN, memory card interface, remote rack expansion support, power supply integrated and user web pages support

Table 21: Product Code

2.7. Related Products

The following products must be purchased separately when necessary:

Code	Description
MT8500	MasterTool IEC XE
AL-2600	RS-485 network branch and terminator
AL-2306	RS-485 cable for MODBUS or CAN network
NX9101	32 GB microSD memory card with miniSD and SD adapters
NX9202	RJ45-RJ45 2 m Cable
NX9205	RJ45-RJ45 5 m Cable
NX9210	RJ45-RJ45 10 m Cable
NX9000	8-Slot Backplane Rack
NX9001	12-Slot Backplane Rack
NX9002	16-Slot Backplane Rack
NX9003	24-Slot Backplane Rack
NX9010	8-Slot Backplane Rack (No Hot Swap)
NX9020	2-Slot base for panel assembly

Table 22: Related Products

Notes:

MT8500: MasterTool IEC XE is available in four different versions: LITE, BASIC, PROFESSIONAL and ADVANCED. For more details, please check MasterTool IEC XE User Manual - MU299609.

AL-2600: This module is used for branch and termination of RS-422/485 networks. For each network node, an AL-2600 is required. The AL-2600 that is at the ends of network must be configured with termination, except when there is a device with active internal termination, the rest must be configured without termination.

AL-2306: Two shielded twisted pairs cable without connectors, used for networks based on RS-485 or CAN.

NX9202/NX9205/NX9210: Cables used for Ethernet communication and to interconnect the bus expansion modules.

NX9020: 2 slot base for panel assembly.

3. Installation

This chapter presents the necessary proceedings for the physical installation, as well as the care that should be taken with other installation within the panel where the controller is been installed.

CAUTION

If the equipment is used in a manner not specified by in this manual, the protection provided by the equipment may be impaired.

3.1. Mechanical Installation

This product must be inserted in the backplane rack position 0. It requires two sequential positions, this means that it uses positions 0 and 1 of the rack.

The mechanical assembly of this module is described in the Nexto Series User's Manual – MU214600.

3.2. Electrical Installation

3.2.1. Using the integrated power supply

The figure below shows the CPU NX3008 electric diagram installed in a Nexto Series backplane rack. The connectors placement depicted are merely illustrative.

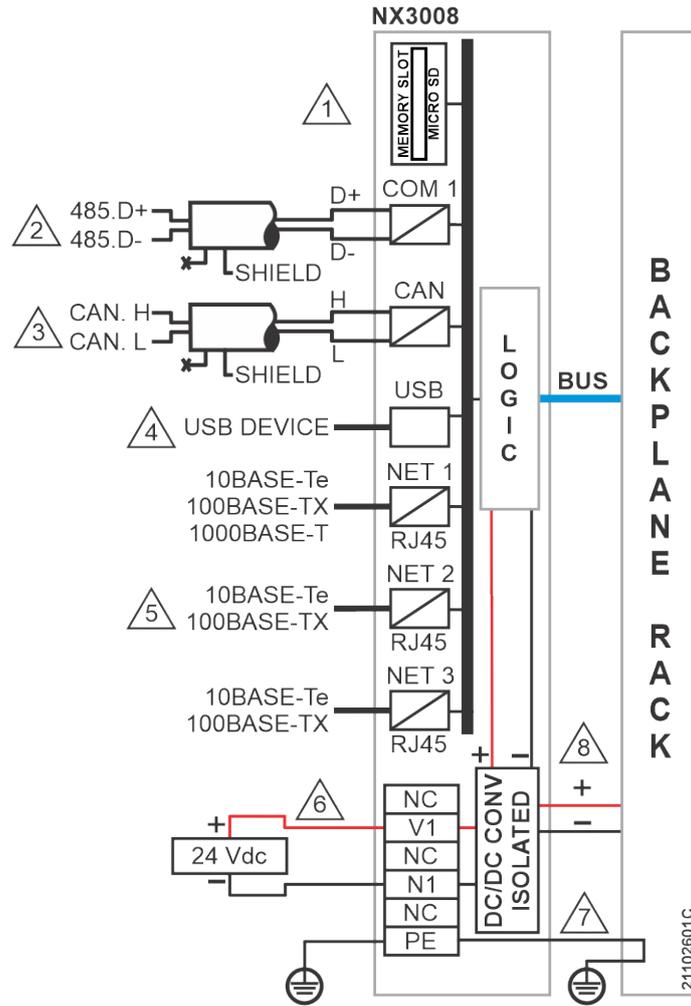


Figure 5: NX3008 CPU Electric Diagram

Diagram Notes:

- ① MicroSD card interface.
- ② RS-485 interface.
- ③ CAN interface.
- ④ USB 2.0 interface.
- ⑤ Standard Ethernet interfaces NET 1 10BASE-Te/100BASE-TX/1000BASE-T and NET 2/NET 3 10BASE-Te/100BASE-TX.
- ⑥ The power supply is connected to terminals V1 and N1. Use 0.5 mm² cable.
- ⑦ The CPU is grounded through the Nexto Series backplane racks. It is recommended to reinforce the ground connecting to the PE terminal. Use 0.5 mm² cable.
- ⑧ The CPU supplies the other modules through the connection to the backplane rack.
- ⊕ Functional earth terminal.

3.2.2. Using a NX8000 power supply module

If the power requirement of the group of I/O modules connected to the local bus exceeds the capacity of the integrated power supply of NX3008, allow the use of a NX8000 power supply module to supply the bus. In this configuration, the NX3008 must still be powered (to feed the internal electronics), but its bus power output will stay disabled, i.e., there won't be parallelism, and the NX8000 will deliver all the current supplied to the I/O modules of the bus.

DANGER

To operate on this configuration, it is **MANDATORY** to have NX3008 firmware version 1.14.35.0 or greater and the MasterTool version 3.63 or greater. Please check if the firmware version is updated before proceeding with the installation.
If this condition is not accomplished, **DO NOT** connect the NX8000 on the local bus, under the risk of permanent damage to the hardware.

DANGER

When executing any installation in an electric panel, certify that the main energy supply is **OFF**.

The figure below shows the CPU NX3008 electric diagram using the NX8000 power supply module in a Nexto Series backplane rack. The layout of the connectors and terminals in the figure is for illustrative purposes only.

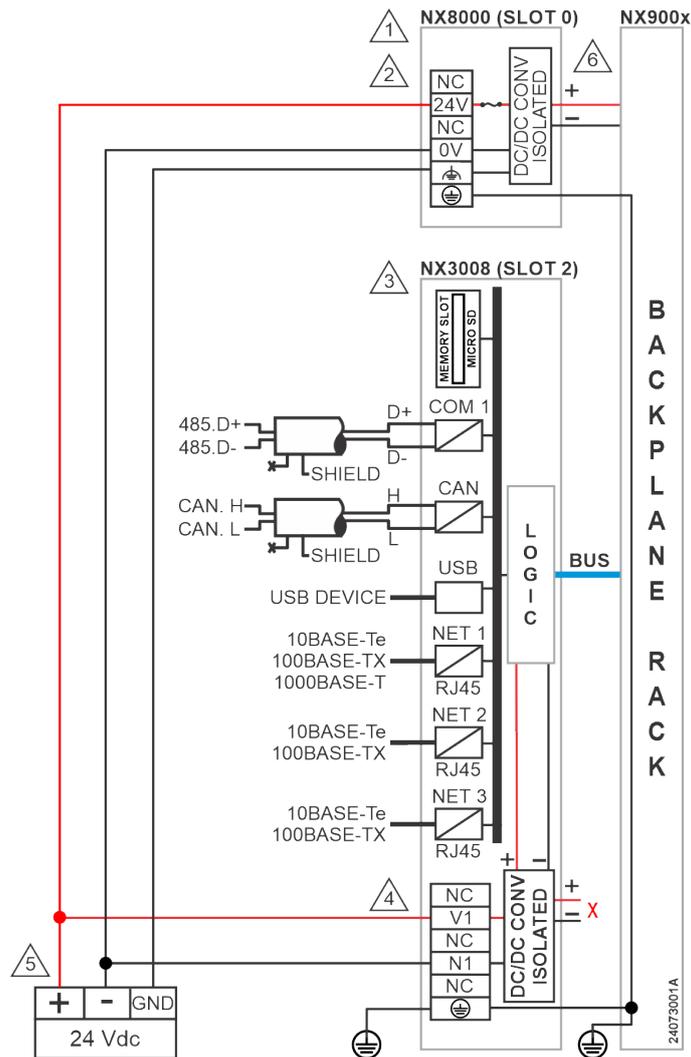


Figure 6: Electrical diagram of the NX3008 CPU using the NX8000 power supply module

Diagram Notes:

- ① The NX8000 must be positioned in Slot 0.
- ② The NX3008 must be positioned in Slot 2.
- ③ The power supply is connected to the 24V and 0V terminals of the NX8000. Use 2.5 mm² cables. NC terminals: Not connected.
- ④ The power supply is connected to the V1 and N1 terminals of the NX3008. Use 0.5 mm² cables. NC terminals: Not connected.
- ⑤ The NX8000 and NX3008 must be powered from the same 24V power supply.
- ⑥ The NX8000 module powers the other bus modules via the connection to the rack. In this condition, the NX3008 does not supply power to the bus modules.
- ⊕ Functional earth terminal.

3.3. Ethernet Network Connection

The NET 1, NET 2, and NET 3 isolated communication interface allows the connection with an Ethernet network, however, the NET 1 interface is the most suitable to be used for communication with MasterTool IEC XE.

The Ethernet network connection uses twisted pair cables (10Base-T/100Base-TX/1000Base-T) and the speed detection is automatically made by the Nexto CPU. This cable must have one of its endings connected to the interface that is likely to be used and another one to the HUB, switch, microcomputer or other Ethernet network point.

3.3.1. IP Address

The NET 1 Ethernet interface is used for Ethernet communication and for CPU configuration which comes with the following default parameters configuration:

NET 1	
IP Address	192.168.15.1
Subnetwork Mask	255.255.255.0
Gateway Address	192.168.15.253

Table 23: Default Parameters Configuration for Ethernet NET 1 Interface

The IP Address and Subnet Mask parameters can be seen on the CPU graphic display via parameters menu, as described in [CPU's Informative and Configuration Menu](#) section.

Initially, the NET 1 interface must be connected to a PC network with the same subnet mask to communicate with MasterTool IEC XE, where the network parameters can be modified. For further information regarding configuration and parameters modifications, see [Ethernet Interfaces Configuration](#) section.

The NET 2 Ethernet interface is used only for Ethernet communication and comes with the following default parameters configuration:

NET 2	
IP Address	192.168.16.1
Subnetwork Mask	255.255.255.0
Gateway Address	0.0.0.0

Table 24: Default Parameters Configuration for Ethernet NET 2 Interface

The IP Address and Subnet Mask parameters can be seen on the CPU graphic display via parameters menu, as described in [CPU's Informative and Configuration Menu](#) section.

The NET 2 interface network parameters can be changed through MasterTool IEC XE. For further information regarding configuration and parameters modifications, see [Ethernet Interfaces Configuration](#) section.

NET 3	
IP Address	192.168.17.1
Subnetwork Mask	255.255.255.0
Gateway Address	0.0.0.0

Table 25: Default Parameters Configuration for Ethernet NET 3 Interface

3.3.2. Gratuitous ARP

The NETx Ethernet interface promptly sends ARP packets type in broadcast informing its IP and MAC address for all devices connected to the network. These packets are sent during a new application download by the MasterTool IEC XE software and in the CPU startup when the application goes into Run mode.

Five ARP commands are triggered within a 200 ms initial interval, doubling the interval every new triggered command, totaling 3 s. Example: first trigger occurs at time 0, the second one at 200 ms and the third one at 600 ms and so on until the fifth trigger at time 3 s.

3.3.3. Network Cable Installation

Nexto Series CPUs Ethernet ports, identified on the panel by NET, have standard pinout which are the same used in PCs. The connector type, cable type, physical level, among other details regarding the CPU and the Ethernet network device are defined in the [Ethernet Interfaces](#).

The table below present the RJ-45 Nexto CPU female connector, with the identification and description of the valid pinout for 10BASE-TE and 100BASE-TX physical levels.

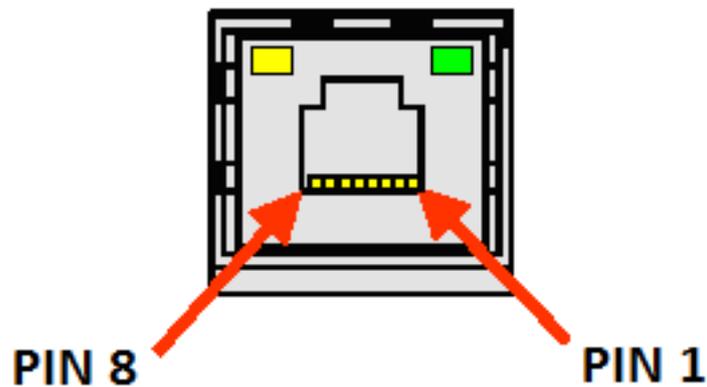


Figure 7: RJ45 Female Connector

Pin	Signal	Description
1	TXD +	Data transmission, positive
2	TXD -	Data transmission, negative
3	RXD +	Data reception, positive
4	NU	Not used
5	NU	Not used
6	RXD -	Data reception, negative
7	NU	Not used
8	NU	Not used

Table 26: RJ45 Female Connector Pinout - 10BASE-TE and 100BASE-TX

The table below shows the female RJ45 connector of Nexto CPUs, with the identification and description of the valid pinout for the 1GBASE-T physical level.

Pin	Signal	Description
1	TxRx A +	Bidirectional, positive
2	TxRx A -	Bidirectional, negative
3	TxRx B +	Bidirectional, positive
4	TxRx C +	Bidirectional, positive
5	TxRx C -	Bidirectional, negative
6	TxRx B -	Bidirectional, negative
7	TxRx D +	Bidirectional, positive
8	TxRx D -	Bidirectional, negative

Table 27: RJ45 Female Connector Pinout - 1GBASE-T

The interface can be connected in a communication network through a hub or switch, or straight from the communication equipment. In this last case, due to Nexto CPUs Auto Crossover feature, there is no need for a cross-over network cable, the one used to connect two PCs point to point via Ethernet port.

It is important to stress that it is understood by network cable a pair of RJ45 male connectors connected by a UTP or ScTP cable, category 5 whether straight connecting or cross-over. It is used to communicate two devices through the Ethernet port.

These cables normally have a connection lock which guarantees a perfect connection between the interface female connector and the cable male connector. At the installation moment, the male connector must be inserted in the module female connector until a click is heard, assuring the lock action. To disconnect the cable from the module, the lock lever must be used to unlock one from the other.

3.4. Serial Network Connection RS-485 and CAN

As the [Electrical Installation](#) diagram illustrates, the RS-485 and CAN interfaces use two communication signals and ground. The recommended cable is AL-2306, using one of the two pairs and the shielding. If the controller is placed at one end of the network, internal termination must be enabled (see the configuration sections [CAN Interface Configuration \(Controller Area Network\)](#) and [Advanced Configurations](#) for CAN and RS-485 respectively).

3.5. Memory Card Installation

This section presents how to insert the memory card into the models Nexto Series CPUs. For further information see [Memory Card](#) section.

Initially, care must be taken with the correct position the memory card must be inserted. One corner of it is different from the other three and this one must be used as reference for the card correct insertion. Therefore, the memory card must be inserted following the depiction on the CPU frontal part or the way showed on figure below.

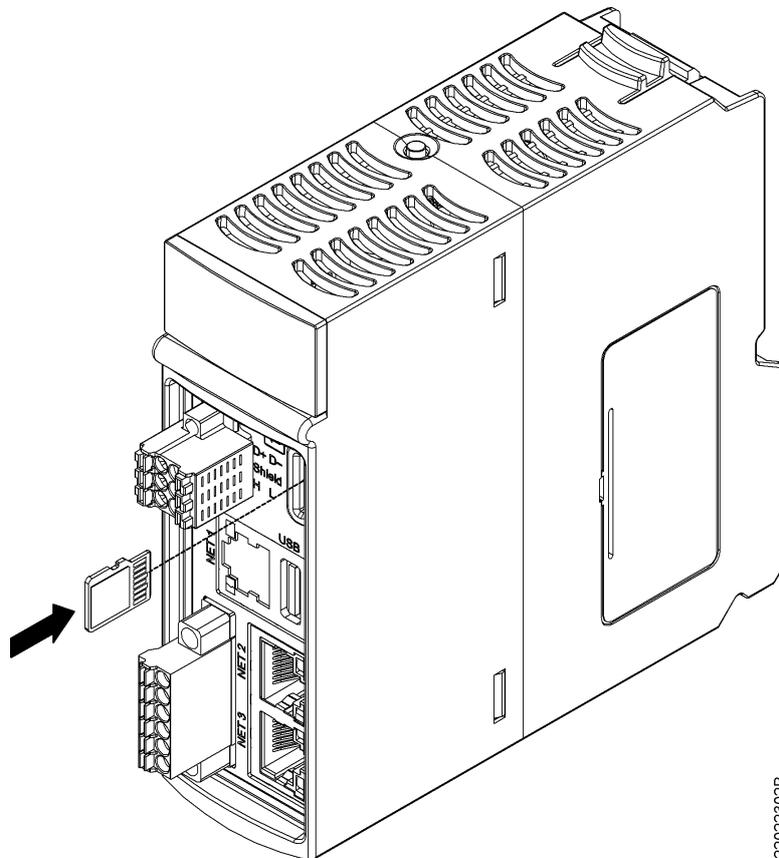


Figure 8: Inserting the Memory Card

When the card is correctly installed, a symbol will appear on the CPU graphic display. For card secure removing the MS key must be pressed then there is a little delay and the card symbol will disappear from the graphic display. The card is now ready to be taken off. For that, the card must be pressed against the CPU until a click is heard, then release it and withdraw it from the compartment as showed on figure below. At this moment the card will be loose.

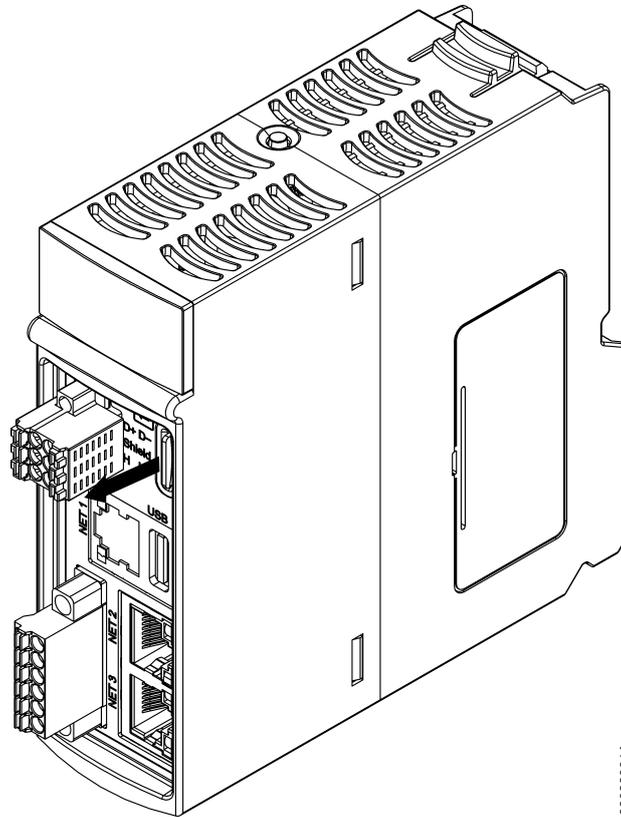


Figure 9: Removing the Memory Card from the CPU

3.6. Architecture Installation

3.6.1. Module Installation on the Main Backplane Rack

Nexto Series has an exclusive method for connecting and disconnecting modules on the bus which does not require much effort from the operator and guarantee the connection integrity. For further information regarding Nexto Series products fixation, please see Nexto Series User Manual – MU214600.

3.7. Programmer Installation

To execute the MasterTool IEC XE development software installation, it is necessary to have the distribution CD-ROM or download the installation file from the site <https://www.altus.com.br/en/>. For further information about the step by step to installation, consult MasterTool IEC XE User Manual MT8500 – MU299609.

4. Initial Programming

The main goal of this chapter is to help the programming and configuration of Nexto Series CPUs, allowing the user to take the first steps before starting to program the device.

Nexto Series CPU uses the standard IEC 61131-3 for language programming, which are: IL, ST, LD, SFC and FBD, and besides these, an extra language, CFC. These languages can be separated in text and graphic. IL and ST are text languages and are similar to Assembly Language and C, respectively. LD, SFC, FBD and CFC are graphic languages. LD uses the relay block representation and it is similar to relay diagrams. SFC uses the sequence diagram representation, allowing an easy way to see the event sequence. FBD and CFC use a group of function blocks, allowing a clear vision of the functions executed by each action.

The programming is made through the MasterTool IEC XE (IDE) development interface. The MasterTool IEC XE allows the use of the six languages in the same project, so the user can apply the best features offered by each language, resulting in more efficient applications development, for easy documentation and future maintenance.

For further information regarding programming, see MasterTool IEC XE User Manual - MU299609, MasterTool IEC XE Programming Manual - MP399609 or IEC 61131-3 standard.

4.1. Memory Organization and Access

Different from other devices of the Nexto Series (which are based on a big-endian CPU), this CPU model is based on an ARM CPU, which uses the traditional little-endian memory organization (the same found on x86 and Intel processors). On this type of memory organization, the least significant byte is stored first and will always be the smallest address (e.g. %QB0 will always be less significant than %QB1, as shown on the table below, where, for CPUNEXTO string, the letter O is byte 0 and the letter C is the byte 7).

Besides this, the memory access must be done carefully as the variables with higher number of bits (WORD, DWORD, LONG), use as index the most significant byte, in other words, the %QD4 will always have as most significant byte the %QB4. Therefore it will not be necessary to make calculus to discover which DWORD correspond to defined bytes. The table below, shows little and big endian organization.

MSB ← Little-endian → LSB								
BYTE	%QB7	%QB6	%QB5	%QB4	%QB3	%QB2	%QB1	%QB0
	C	P	U	N	E	X	T	O
WORD	%QW6		%QW4		%QW2		%QW0	
	CP		UN		EX		TO	
DWORD	%QD4				%QD0			
	CPUN				EXTO			
LWORD	%QL0							
	CPUNEXTO							
MSB ← Big-endian → LSB								
BYTE	%QB0	%QB1	%QB2	%QB3	%QB4	%QB5	%QB6	%QB7
	C	P	U	N	E	X	T	O
WORD	%QW0		%QW2		%QW4		%QW6	
	CP		UN		EX		TO	
DWORD	%QD0				%QD4			
	CPUN				EXTO			
LWORD	%QL0							
	CPUNEXTO							

Table 28: Memory Organization and Access Example

4. INITIAL PROGRAMMING

SIGNIFICANCE					OVERLAPPING					
Bit	Byte	Word	DWord	LWord	Byte	Word	DWord			
%QX0.7	%QB 00	%QW			%QB00	%QW				
%QX0.6										
%QX0.5										
%QX0.4										
%QX0.3										
%QX0.2										
%QX0.1										
%QX0.0										
%QX1.7	%QB 01	%QW			%QB01	%QW				
%QX1.6										
%QX1.5										
%QX1.4										
%QX1.3										
%QX1.2										
%QX1.1										
%QX1.0		%QD				%QD				
%QX2.7	%QB 02	%QW			%QB02	%QW				
%QX2.6										
%QX2.5										
%QX2.4										
%QX2.3										
%QX2.2										
%QX2.1										
%QX2.0						%QD				
%QX3.7	%QB 03	%QW			%QB03	%QW				
%QX3.6										
%QX3.5										
%QX3.4										
%QX3.3										
%QX3.2										
%QX3.1										
%QX3.0			%QL				%QD			
%QX4.7	%QB 04	%QW			%QB04	%QW				
%QX4.6										
%QX4.5										
%QX4.4										
%QX4.3										
%QX4.2										
%QX4.1										
%QX4.0							%QD			
%QX5.7	%QB 05	%QW			%QB05	%QW				
%QX5.6										
%QX5.5										
%QX5.4										
%QX5.3										
%QX5.2										
%QX5.1										
%QX5.0		%QD						%QD		
%QX6.7	%QB 06	%QW			%QB06	%QW				
%QX6.6										
%QX6.5										
%QX6.4										
%QX6.3										
%QX6.2										
%QX6.1										
%QX6.0										
%QX7.7	%QB 07	%QW			%QB07	%QW				
%QX7.6										
%QX7.5										
%QX7.4										
%QX7.3										
%QX7.2										
%QX7.1										
%QX7.0										

Table 29: Memory Organization and Access

The table above shows the organization and memory access, illustrating the significance of bytes and the disposition of other variable types, including overlapping.

4.2. Project Profiles

A project profile in the MasterTool IEC XE consists in an application template together with a group of verification rules which guides the development of the application, reducing the programming complexity. The applications can be created according to the following profiles:

- Single
- Basic
- Normal
- Expert
- Custom
- Machine Profile

The Project Profile is selected on the project creation wizard. Each project profile defines a template of standard names for the tasks and programs, which are pre-created according to the selected Project Profile. Also, during the project compilation (generate code), MasterTool IEC XE verify all the rules defined by the selected profile.

The following sections details the characteristics of each profile, which follow a gradual complexity slope. Based in these definitions, it's recommended that the user always use the simplest profile that meets his application needs, migrating to a more sophisticated profile only when the corresponding rules are being more barriers to development than didactic simplifications. It is important to note that the programming tool allows the profile change from an existent project (see project update section in the MasterTool IEC XE User Manual – MU299609), but it's up to the developer to make any necessary adjustments so that the project becomes compatible with the rules of the new selected profile.

ATTENTION

Through the description of the Project profiles some tasks types are mentioned, which are described in the section 'Task Configuration', of the MasterTool IEC XE User Manual – MU299609.

4.2.1. Single

In the Single Project Profile, the application has only one user task, MainTask. This task is responsible for the execution of a single Program type programming unit called MainPrg. This single program can call other programming unit, of the Program, Function or Function Block types, but the whole code will be executed exclusively by the MainTask.

In this profile, the MainTask will be of the cyclical type (Cyclic) with priority fixed as 13 (thirteen) and runs exclusively the MainPrg program in a continuous loop. The MainTask is already fully defined and the developer needs to create the MainPrg program, using any of the languages of the IEC 61131-3 standard. It is not always possible to convert a program to another language, but it's always possible to create a new program, built in a different language, with the same name and replace it. The MasterTool IEC XE standard option is to use the MasterTool Standard Project associated with the Single profile, which also include the MainPrg created in the language selected during the project creation.

This type of application never needs to consider issues as data consistence, resource sharing or mutual exclusion mechanisms.

Task	POU	Priority	Type	Interval	Event
MainTask	MainPrg	13	Cyclic	100 ms	-

Table 30: Single Profile Task

4.2.2. Basic

In the Basic Project Profile, the application has one user task of the Continuous type called MainTask, which executes the program in a continuous loop (with no definition of cycle time) with priority fixed in 13 (thirteen). This task is responsible for the execution of a single programming unit POU called MainPrg. It's important to notice that the cycle time may vary according to the quantity of communication tasks used, as in this mode, the main task is interrupted by communication tasks.

This profile also allows the inclusion of two event tasks with higher priority, that can interrupt (preempt) the MainTask at any given moment: the task named ExternInterruptTask00 is an event task of the External type with priority fixed in 02 (two); the task named TimeInterruptTask00 is an event task of the Cyclic type with priority fixed as 01 (one).

The Basic project template model includes three tasks already completely defined as presented in table below. The developer need only to create the associated programs.

Tasks	POU	Priority	Type	Interval	Event
MainTask	MainPrg	13	Continuous	-	-
ExternInterruptTask00	ExternInterruptPrg00	02	External	-	IO_EVT_0
TimeInterruptTask00	TimeInterruptPrg00	01	Cyclic	20 ms	-

Table 31: Basic Profile Tasks

4.2.3. Normal

In the Normal Project Profile, the application has one user task of the Cyclic type, called MainTask. This task is responsible for the execution of a single programming unit POU called MainPrg. This program and this task are similar to the only task and only program of the Single profile, but here the application can integrate additional user tasks. These other tasks, named CyclicTask00 and CyclicTask01, each one responsible for the exclusive execution of its respective CyclicPrg<nn> program. The CyclicTask<nn> tasks are always of the cyclic type and with priority fixed in 13 (thirteen), same priority as MainTask. These two types form a group called basic tasks, which associated programs can call other POUs of the Program, Function and Function Block types.

Furthermore, this profile can include event tasks with higher priority than the basic tasks, which can interrupt (preempt) these tasks execution at any time.

The task called ExternInterruptTask00 is an event task of the External type which execution is triggered by some external event, such as the variation of a control signal on a serial port or the variation of a digital input on the NEXTO bus. This task priority is fixed in 02 (two), being responsible exclusively for the execution of the ExternInterruptPrg00 program. The task called TimeInterruptTask00 is an event task of the Cyclic type with a priority fixed as 01 (one), being responsible for the execution exclusively of TimeInterruptPrg00 program.

In the Normal project model, there are five tasks, and its POUs, already fully defines as shown in table below. The developer needs only to implement the programs content, opting, on the wizard, for any of the languages in IEC 61131-3 standard. The tasks interval and trigger events can be configured by the developer and the unnecessary tasks can be eliminated.

Tasks	POU	Priority	Type	Interval	Event
MainTask	MainPrg	13	Cyclic	100 ms	-
CyclicTask00	CyclicPrg00	13	Cyclic	200 ms	-
CyclicTask01	CyclicPrg01	13	Cyclic	500 ms	-
ExternInterruptTask00	ExternInterruptPrg00	02	External	-	IO_EVT_0
TimeInterruptTask00	TimeInterruptPrg00	01	Cyclic	20 ms	-

Table 32: Normal Profile Tasks

4.2.4. Expert

The Expert Project Profile includes the same basic tasks, CyclicTask<nn>, ExternInterruptTask00 and TimeInterruptTask00 with the same priorities (13, 02 and 01 respectively), but it's an expansion from the previous ones, due to accept multiple events tasks. That is, the application can include various ExternInterruptTask<nn> or TimeInterruptTask<nn> tasks that execute the ExternInterruptPrg<nn> and TimeInterruptPrg<nn> programs. The additional event tasks priorities can be freely selected from 08 to 12. In this profile, besides the standard programs, each task can execute additional programs.

In this project profile, the application may also include the user task FreeTask of the Freewheeling type with priority 31, responsible for the FreePrg program execution. As this task is low priority it can be interrupted by all others so it can execute codes that might be blocked.

There are eight tasks already fully defined, as shown in table below, as well as their associated programs in the chosen language. Intervals and trigger events of any task, as well as the priorities of the event tasks can be configured by the user.

When developing the application using Expert project's profile, a special care is needed with the event tasks scaling. If there is information and resource sharing between these tasks or between them and the basic tasks, it is strongly recommended to adopt strategies to ensure data consistency.

Tasks	POU	Priority	Type	Interval	Event
MainTask	MainPrg	13	Cyclic	100 ms	-
CyclicTask00	CyclicPrg00	13	Cyclic	200 ms	-
CyclicTask01	CyclicPrg01	13	Cyclic	500 ms	-
ExternInterruptTask00	ExternInterruptPrg00	02	External	-	IO_EVT_0
TimeInterruptTask00	TimeInterruptPrg00	01	Cyclic	20 ms	-
ExternInterruptTask01	ExternInterruptPrg01	11	External	-	IO_EVT_1
TimeInterruptTask01	TimeInterruptPrg01	09	Cyclic	30 ms	-
FreeTask	FreePrg	31	Continuous	-	-

Table 33: Expert Profile Tasks

4.2.5. Custom

The Custom project profile allows the developer to explore all the potential of the Runtime System implemented in the CPUs. No functionality is disabled; no priority, task and programs association or nomenclatures are imposed. The only exception is for MainTask, which must always exist with this name in this Profile.

Beyond the real time tasks, with priority between 00 and 15, which are scheduled by priority, in this profile it is also possible to define tasks with lower priorities in the range 16 to 31. In this range, it's used the Completely Fair Scheduler (time sharing), which is necessary to run codes that can be locked (for example, use of sockets).

The developer is free to partially follow or not the organization defined in other project profiles, according to the characteristics of the application. On the other hand, the Custom model associated with this profile needs no pre-defining elements such as task, program or parameter, leaving the developer to create all the elements that make up the application.

Tasks	POU	Priority	Type	Interval	Event
MainTask	MainPrg	13	Cyclic	100 ms	-
CyclicTask00	CyclicPrg00	13	Cyclic	200 ms	-
CyclicTask01	CyclicPrg01	13	Cyclic	500 ms	-
ExternInterruptTask00	ExternInterruptPrg00	02	External	-	IO_EVT_0
TimeInterruptTask00	TimeInterruptPrg00	01	Cyclic	20 ms	-
ExternInterruptTask01	ExternInterruptPrg01	11	External	-	IO_EVT_1
TimeInterruptTask01	TimeInterruptPrg01	09	Cyclic	30 ms	-
FreeTask	FreePrg	31	Continuous	-	-

Table 34: Custom Profile Tasks

4.2.6. Machine Profile

In the Machine Profile, by default, the application has a user task of the Cyclic type called MainTask. This task is responsible for implementing a single Program type POU called MainPrg. This program can call other programming units of the Program, Function or Function Block types, but any user code will run exclusively by MainTask.

This profile is characterized by allowing shorter intervals in the MainTask, allowing faster execution of user code. This optimization is possible because MainTask also performs the processing of the bus. This way, different from other profiles, the machine profile requires no context switch for the bus treatment, which reduces the overall processing time.

This profile may further include an interruption task, called TimeInterruptTask00, with a higher priority than the MainTask, and hence, can interrupt its execution at any time.

Tasks	POU	Priority	Type	Interval	Event
MainTask	MainPrg	13	Cyclic	100 ms	-
TimeInterruptTask00	TimeInterruptPrg00	01	Cyclic	4 ms	-

Table 35: Machine Profile Tasks

Also, this profile supports the inclusion of additional tasks associated to the external interruptions.

4.2.7. General Table

		Project Profiles					
		Single	Machine	Basic	Normal	Expert	Custom
Total tasks		01	04	[01..03]	[01..32]	[01..32]	[01..32]
Tasks per program		01		01	01	<n>	<n>
Main Task	Type	Cyclic	Cyclic	Continuous	Cyclic	Cyclic	Cyclic
	Priority	13	13	13	13	13	13
	Quantity	01	01	01	01	01	01
Time Interrupt Task	Type		Cyclic	Cyclic	Cyclic	Cyclic	Cyclic
	Priority		01	01	01	01 or [08..12]	01 or [08..12]
	Quantity		[00..01]	[00..01]	[00..01]	[00..31]	[00..31]
Extern Interrupt Task	Type		External	External	External	External	External
	Priority		02	02	02	02 or [08..12]	02 or [08..12]
	Quantity		[00..01]	[00..01]	[00..01]	[00..31]	[00..31]
Cyclic Task	Type				Cyclic	Cyclic	Cyclic
	Priority				13	13	13
	Quantity				[00..31]	[00..31]	[00..31]
Free Task	Type					Continuous	Continuous
	Priority					31	31
	Quantity					[00..01]	[00..01]
Event Task	Type						Event
	Priority						<n>
	Quantity						[00..31]

Table 36: General Profile x Tasks Table

ATTENTION

The suggested POU names associated with the tasks are not consisted. They can be changed, as long as they are also changed in the tasks configurations.

4.2.8. Maximum Number of Tasks

The maximum number of tasks that the user can create is only defined for the Custom profile, the only one which has this permission. The others already have their tasks created and configured. However, the tasks that will be created must use the following prefixes, according to the type of each of the tasks: CyclicTaskxx, TimeInterruptTaskxx, ExternInterruptTaskxx, where xx represents the number of the task that being created.

The table below describes the maximum IEC task quantity per CPU and project profile, where the protocol instances are also considered communication tasks by the CPU.

	Task Type	NX3008					
		S	B	N	E	P	M
Configuration Task (Task WHSB)	Cyclic	1	1	1	1	1	0
User Tasks	Cyclic	1	1	31	31	31	2
	Triggered by Event	0	0	0	0	31	0
	Trig. by External Event	0	1	0	30	31	0
	Freewheeling	0	1	0	1	31	0
	State-triggered	0	0	0	0	31	0
NETs - Client or Server Instances	Cyclic	16					
COM(n) - Master or Slave instances	Cyclic	1					
TOTAL		32					

Table 37: Maximum Number of Tasks IEC NX3008

Notes:

Profile Legend: The S, B, N, E, C and M letters correspond to the Single, Basic, Normal, Expert, Custom and Machine profiles respectively.

Values:: The number defined for each task type represents the maximum values allowed.

Task WHSB: The WHSB is a system task that must be considered so the total value is not surpassed.

NETs - Client or Server Instances: The maximum value defined considers all system Ethernet interfaces, including the expansion modules when these are applied. E.g. MODBUS protocol instances.

COM (n) - Master or Slave Instances: The "n" represents the number of the serial interface. Even with expansion modules, the table value will be the maximum per interface. E.g. MODBUS protocol instances.

Total: The total value does not represent the sum of all profile tasks, but the maximum value allowed per CPU. Therefore, the user can create several task types, while the established numbers for each one and the total value are not surpassed.

4.3. CPU Configuration

The Nexto CPU configuration is located in the device tree, as shown on figure below, and can be accessed by a double-click on the corresponding object. In this tab it's possible to configure the diagnostics area, the retentive and persistent memory area and hot swap mode, among other parameters, as described in the [CPU Configuration](#).

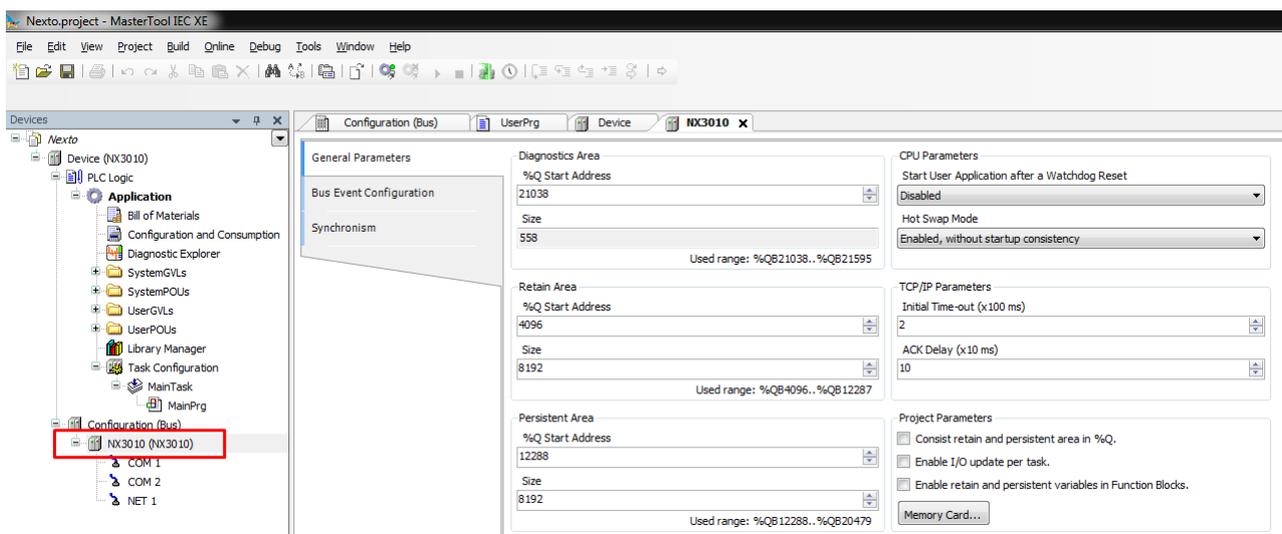


Figure 10: CPU Configuration

Besides that, by double-clicking on CPU's NET 1 icon, it's possible to configure the Ethernet interface that will be used for communication between the controller and the software MasterTool IEC XE.

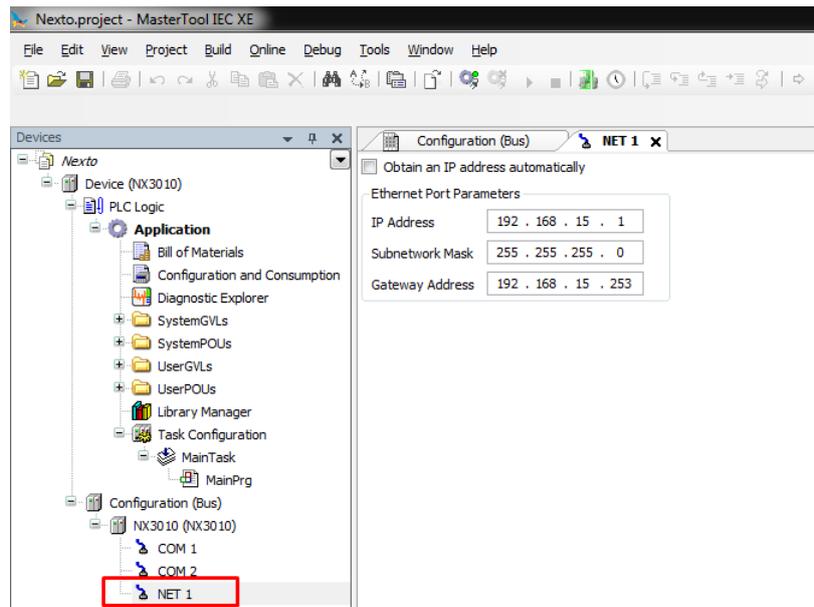


Figure 11: Configuring the CPU Communication Port

The configuration defined on this tab will be applied to the device only when sending the application to the device (download), which is described further on sections [Finding the Device](#) and [Login](#).

4.4. Libraries

There are several programming tool resources which are available through libraries. Therefore, these libraries must be inserted in the project so its utilization becomes possible. The insertion procedure and more information about available libraries must be found in the MasterTool Programming Manual – MP399609.

4.5. Inserting a Protocol Instance

The Nexto Series CPUs, as described in the [Protocols](#) section, offers several communication protocols. Except for the OPC DA and OPC UA communication, which have a different configuration procedure, the insertion of a protocol can be done by simply right-clicking on the desired communication interface, selecting to add the device and finally performing the configuration as shown in the [Protocols Configuration](#) section. Below is presented an examples.

4.5.1. MODBUS RTU

The first step for configuring the MODBUS RTU, in slave mode, is to include the instance in the desired COM (COM 1 in this case) by clicking with the right button on the *COM* and select *Add Device...*, as shown on figure below:

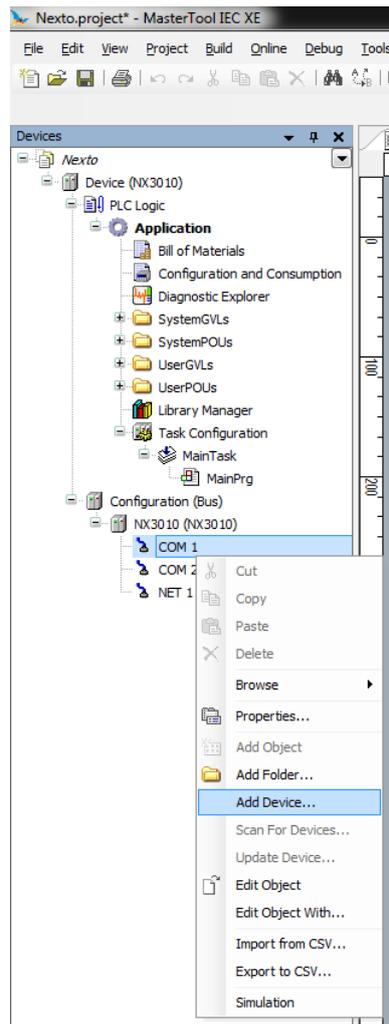


Figure 12: Adding an Instance

After that, the available protocols for the user will appear on the screen. Define the protocol configuration mode selecting *MODBUS Symbol RTU Slave*, for *symbolic mapping* setting or *MODBUS RTU Slave*, for *direct addressing (%Q)* and click on *Add Device*, as depicted on figure below.

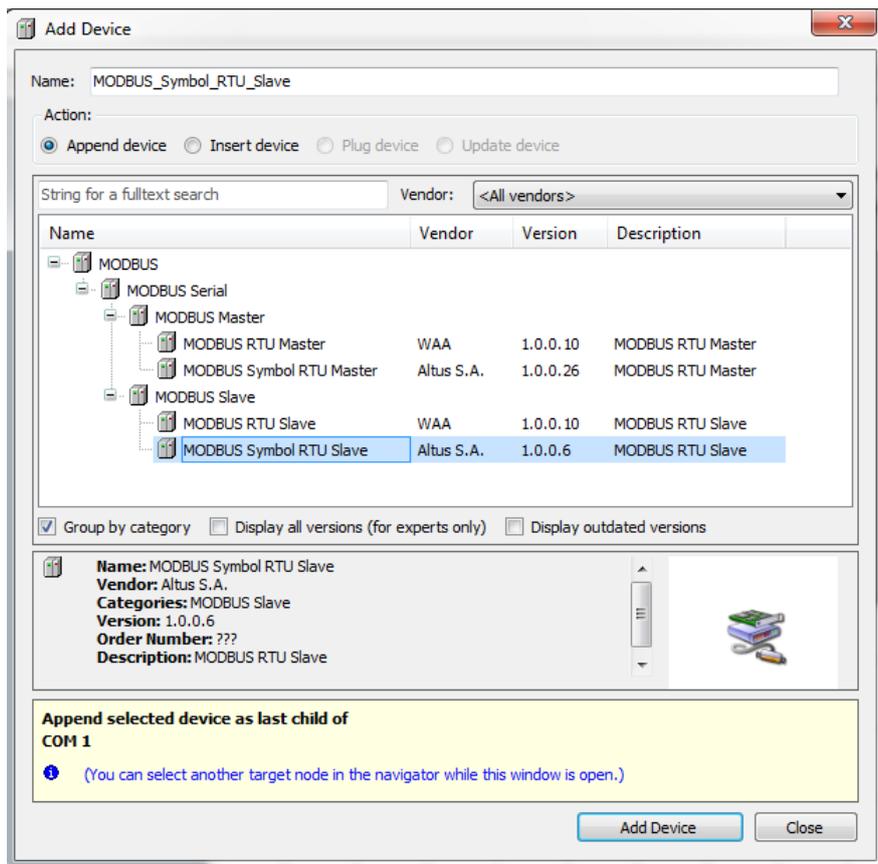


Figure 13: Selecting the Protocol

4.5.2. MODBUS Ethernet

The first step to configure the MODBUS Ethernet (Client in this example), is to include the instance in the desired NET (in this case, NET 1, as the CPU NX3010 has only one Ethernet interface). Click on the *NET* with the mouse right button and select *Add Device...*, as shown on figure below.

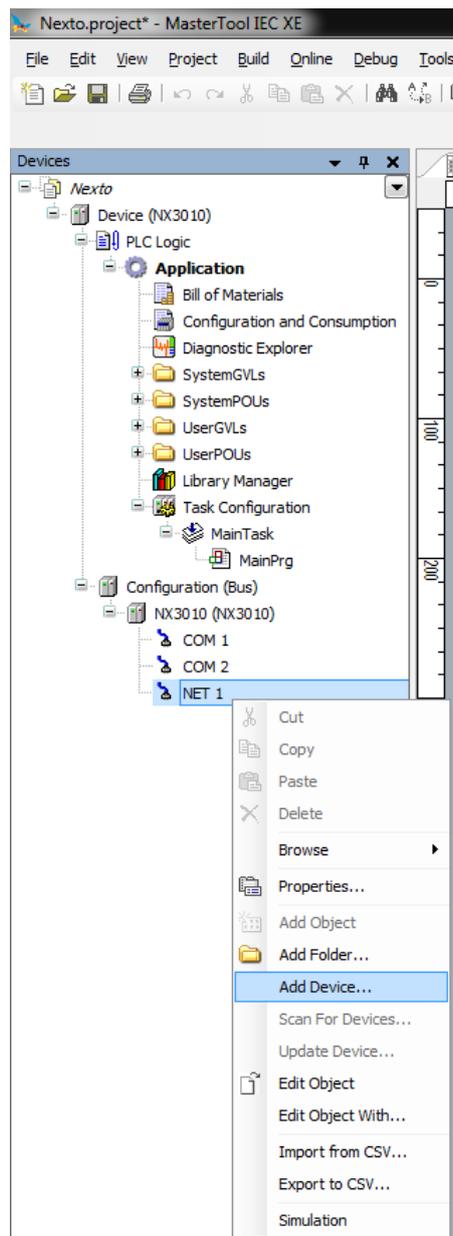


Figure 14: Adding the Instance

After that, the available protocols for the user will appear on the screen. In this menu is defined the configuration mode of the protocol. Selecting the option *MODBUS Symbol Client*, for Symbolic Mapping setting or *MODBUS Client*, for Direct Addressing (%Q). Then, click *Add Device*, as shown in the figure below.

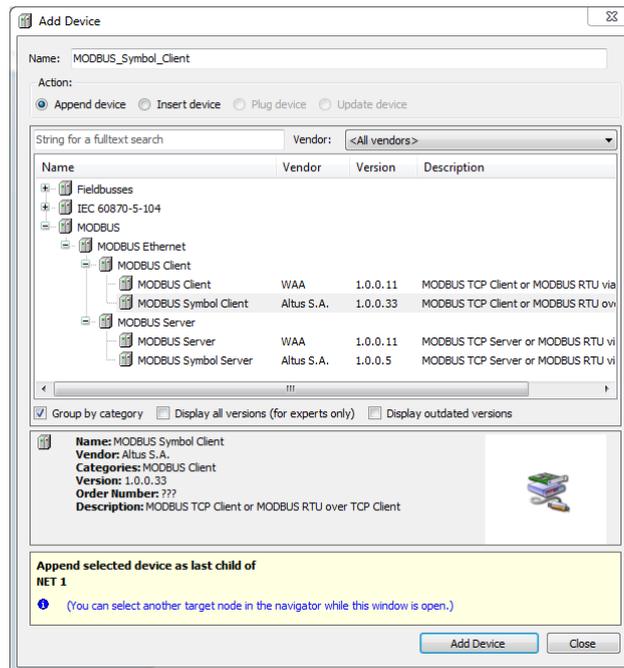


Figure 15: Selecting the Protocol

4.6. Finding the Device

To establish the communication between the CPU and MasterTool IEC XE, first it's necessary to find and select the desired device. The configuration of this communication is located on the object *Device* on device tree, on *Communication Settings* tab. On this tab, after selecting the *Gateway* and clicking on button *Scan network*, the software MasterTool IEC XE performs a search for devices and shows the CPUs found on the network of the Ethernet interface of the station where the tool is running.

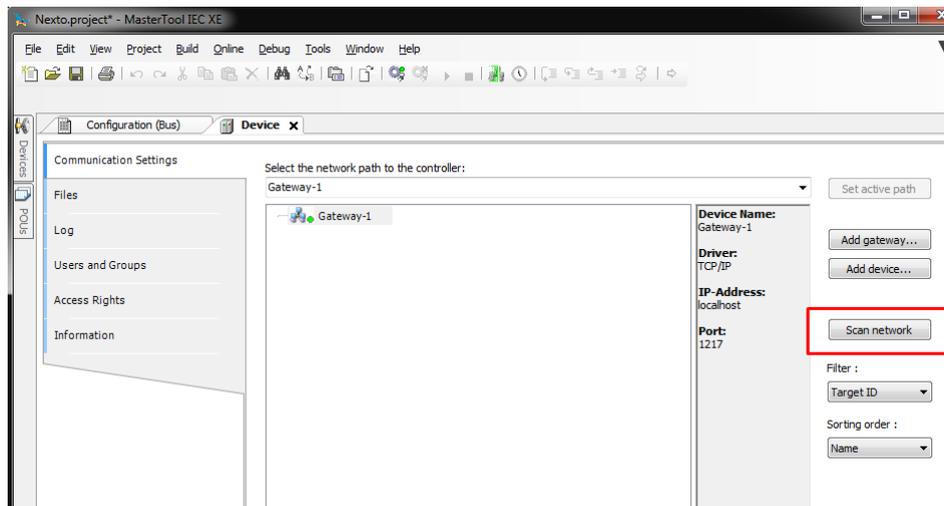


Figure 16: Finding the CPU

If there is no gateway previously configured, it can be included by the button *Add gateway*, using the default IP address *localhost* to use the gateway resident on the station or changing the IP address to use the device internal gateway.

Next, the desired controller must be selected by clicking on *Set active path*. This action selects the controller and informs the configuration software which controller shall be used to communicate and send the project.

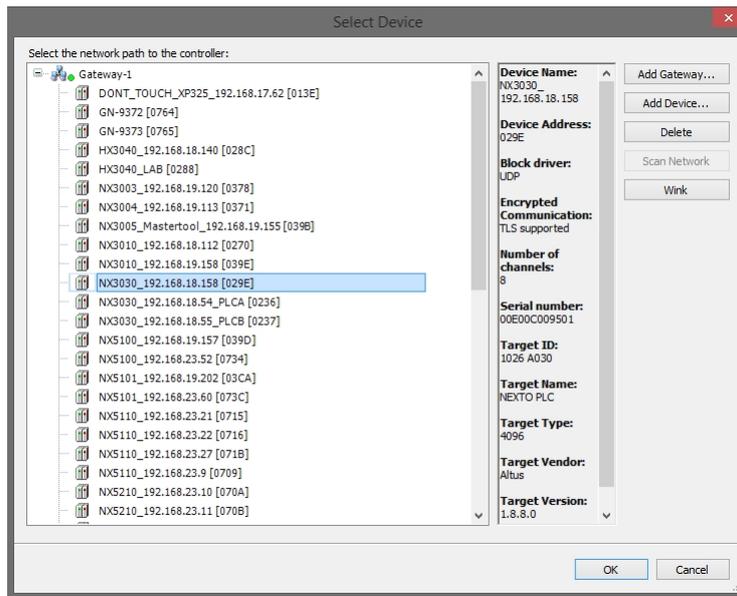


Figure 17: Selecting the CPU

Additionally, the user can change the default name of the device that is displayed. For that, you must click the right mouse button on the desired device and select *Change Device Name*. After a name change, the device will not return to the default name under any circumstances.

In case the Ethernet configuration of the CPU to be connected is in a different network from the Ethernet interface of the station, the software MasterTool IEC XE will not be able to find the device. In this case, it's recommended to use the command *Easy Connection* located on Online menu.

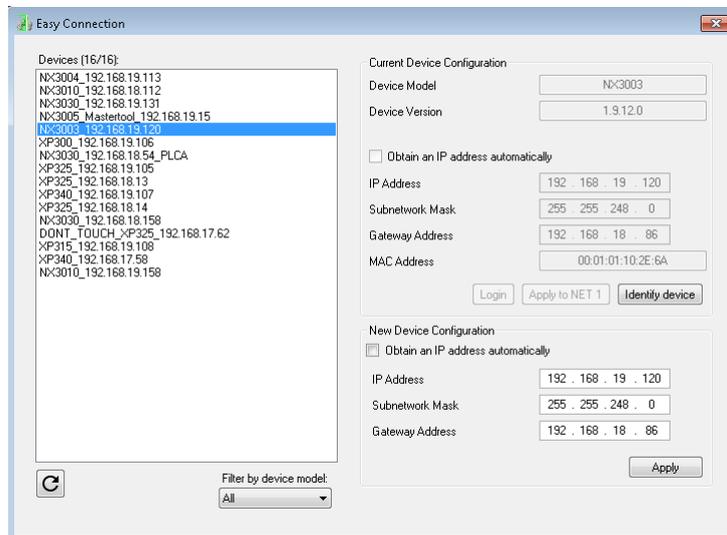


Figure 18: Easy Connection

This command performs a MAC level communication with the NET 1 interface of the device, allowing to permanently change the configuration of the CPU's Ethernet interface, independently of the IP configuration of the station and from the one previously configured on the device. So, with this command, it's possible to change the device configuration to put it on the same network of the Ethernet interface of the station where MasterTool IEC XE is running, allowing to find and select the device for the communication. The complete description of *Easy Connection* command can be found on User Manual of MasterTool IEC XE code MU299609.

4.7. Login

After compiling the application and fixing errors that might be found, it's time to send the project to the CPU. To do this, simply click on *Login* command located on *Online* menu of MasterTool IEC XE as shown on the following figure. This operation may take a few seconds, depending on the size of the generated file.

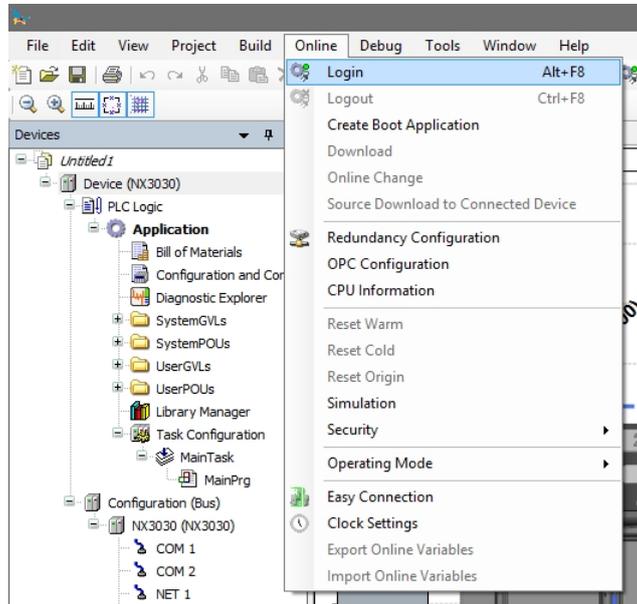


Figure 19: Sending the Project to the CPU

After the command execution, some user interface messages may appear, which are presented due to differences between an old project and the new project been sent, or simply because there was a variation in some variable.

If the Ethernet configuration of the project is different from the device, the communication may be interrupted at the end of download process when the new configuration is applied on the device. So, the following warning message will be presented, asking the user to proceed or not with this operation.

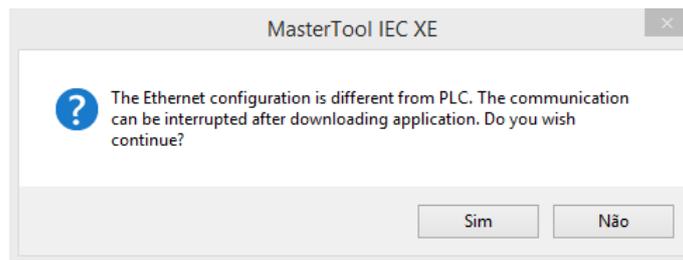


Figure 20: IP Configuration Warning

If there is no application on the CPU, the following message will be presented.



Figure 21: No application on the device

If there is already an application on the CPU, depending on the differences between the projects, the following options will be presented:

- **Login with online change:** execute the login and send the new project without stopping the current CPU application (see [Run Mode](#) item), updating the changes when a new cycle is executed.
- **Login with download:** execute the login and send the new project with the CPU stopped (see [Stop Mode](#)). When the application is initiated, the update will have been done already.
- **Login without any change:** executes the login without sending the new project.

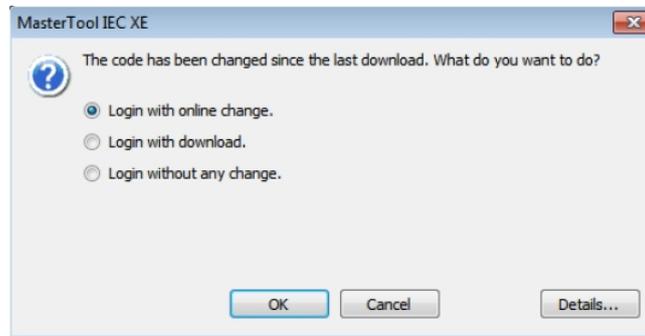


Figure 22: Project Update at the CPU

ATTENTION

In the online changes is not permitted to associate symbolic variables mapping from a global variable list (GVL) and use these variables in another global variable list (GVL).

If the new application contains changes on the configuration, the online change will not be possible. In this case, the MasterTool IEC XE requests whether the login must be executed as download (stopping the application) or if the operation must be cancelled.

PS.: The button *Details...* shows the changes made in the application.

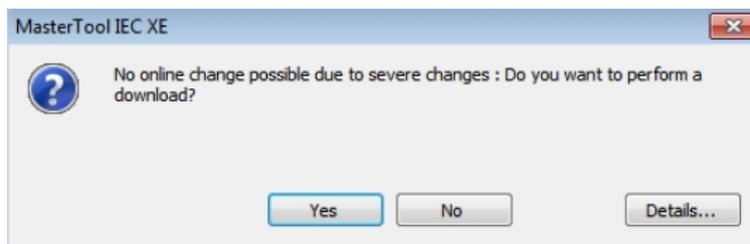


Figure 23: Configuration Changes

Finally, at the end of this process the MasterTool IEC XE offers the option to transfer (download) the source code to the internal memory of the device, as shown on the following figure:

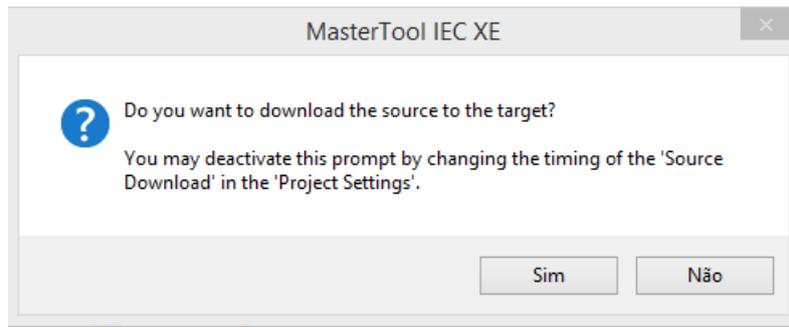


Figure 24: Source code download

Transferring the source code is fundamental to ensure the future restoration of the project and to perform modifications on the application that is loaded into the device.

4.8. Run Mode

Right after the project has been sent to the CPU, the application will not be immediately executed (except for the case of an online change). For that to happen, the command Start must be executed. This way, the user can control the execution of the application sent to the CPU, allowing pre-configuring initial values which will be used by the CPU on the first execution cycle.

To execute this command, simply go to the *Debug* menu and select the option *Start*, as shown on figure below.

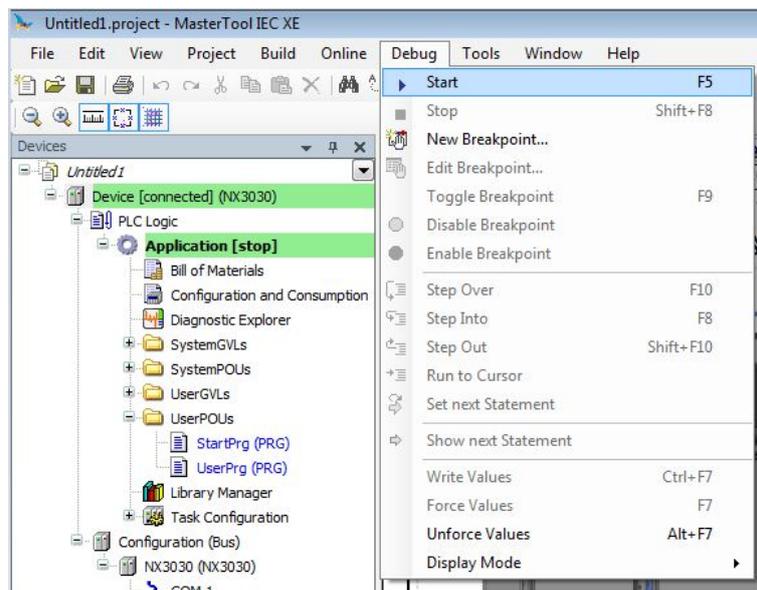


Figure 25: Starting the Application

The figure below shows the application in execution. In case the POU tab is selected, the created variables are listed on a monitoring window, in which the values can be visualized and forced by the user.

4. INITIAL PROGRAMMING

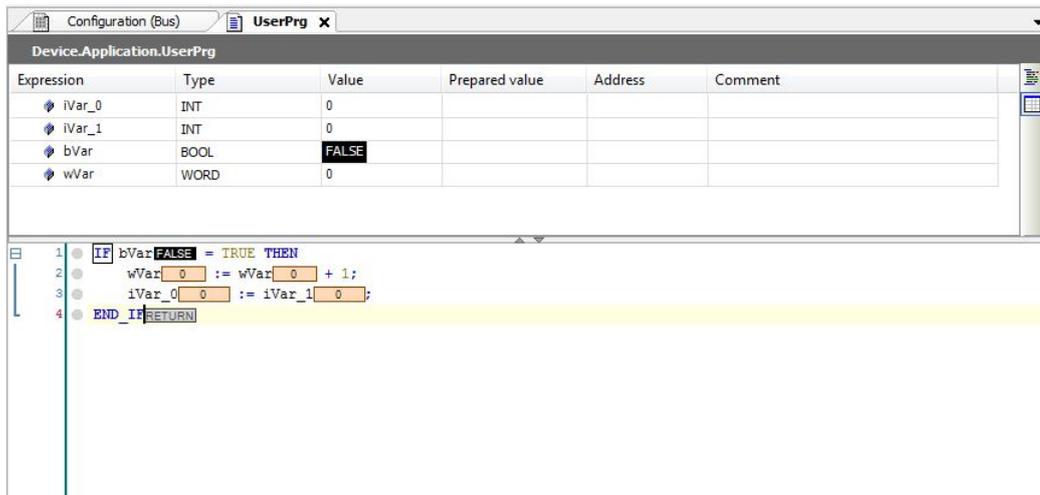


Figure 26: Program running

If the CPU already have a boot application internally stored, it goes automatically to Run Mode when the device is powered on, with no need for an online command through MasterTool IEC XE.

4.9. Stop Mode

To stop the execution of the application, the user must execute the *Stop* command, available at the menu *Debug*, as shown on figure below.

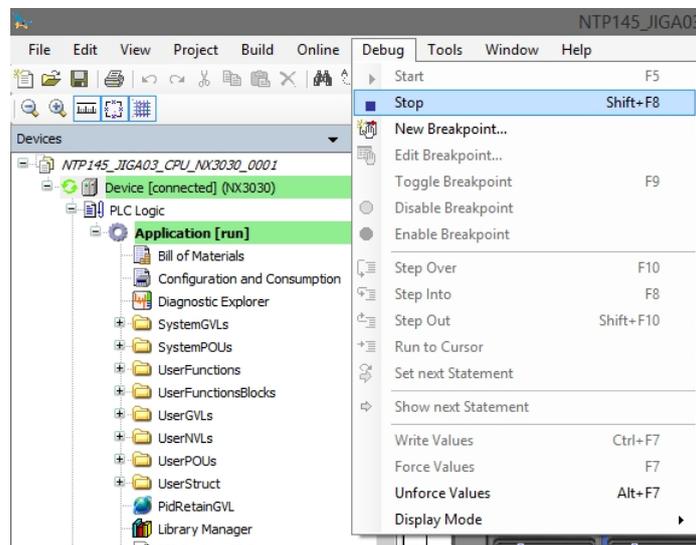


Figure 27: Stopping the Application

In case the CPU is initialized without the stored application, it automatically goes to Stop Mode, as it happens when a software exception occurs.

4.10. Writing and Forcing Variables

After Logging into a PLC, the user can write or force values to a variable of the project.

The writing command (*CTRL + F7*) writes a value into a variable and this value could be overwritten by instructions executed in the application.

Moreover, the forced writing command (*F7*) writes a value into a variable without allowing this value to be changed until the forced variables are released.

It is important to highlight that, when used the MODBUS RTU Slave and the MODBUS Ethernet Server, and the *Read-only* option from the configured relations is not selected, the forced writing command (*F7*) must be done over the available variables in the monitoring window as the writing command (*CTRL + F7*) leaves the variables to be overwritten when new readings are done.

ATTENTION

The variables forcing can be done in Online mode.
Diagnostic variables cannot be forced, only written, because diagnostics are provided by the CPU and will be overwritten by it.

ATTENTION

When a CPU is with forced variables and it is de-energized, the variables will lose the forcing in the next initialization.
The limit of forcing for the Nexto CPUs is 128 variables, regardless of model or configuration of CPU used.

4.11. Logout

To finalize the online communication with the CPU, the command *Logout* must be executed, located in the *Online* menu, as shown on figure below.

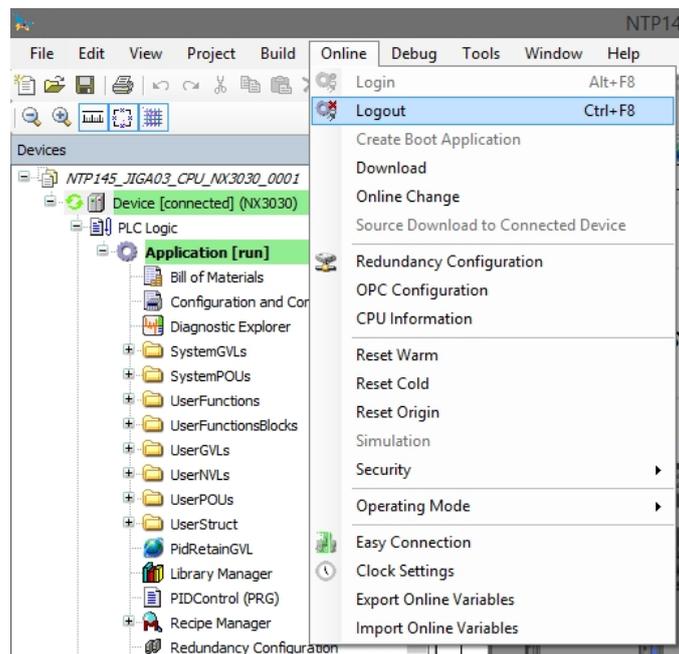


Figure 28: Finalizing the online communication with the CPU

4.12. Project Upload

Nexto Series CPUs are capable to store the source code of the application on the internal memory of the device, allowing future retrieval (upload) of the complete project and to modify the application.

To recover a project previously stored on the internal memory of the CPU, the command located on *File* menu must be executed as shown on the following figure.

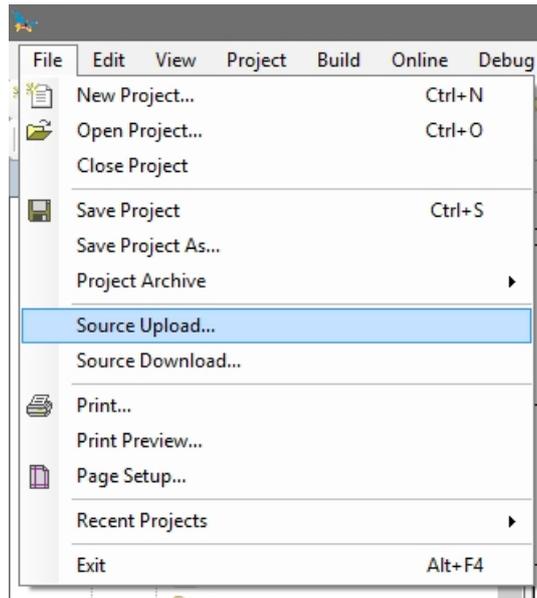


Figure 29: Project Upload Option

Next, just select the desired CPU and click *OK*, as shown on figure below.

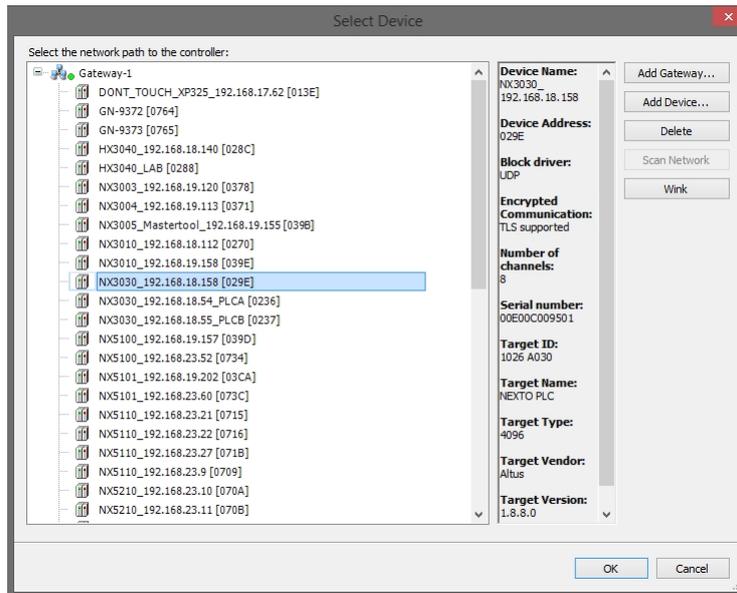


Figure 30: Selecting the CPU

To ensure that the project loaded in the CPU is identical and can be accessed in other workstations, consult the chapter *Projects Download/Login Method without Project Differences* at the MasterTool IEC XE User Manual MT8500 - MU299609.

ATTENTION

The memory size area to store a project in the Nexto CPUs is defined on section [Memory](#).

ATTENTION

The upload recovers the last project stored in the controller as described in the previous paragraphs. In case only the application was downloaded, without transferring its source code, it will not be possible to be recovered by the Upload procedure.

4.13. CPU Operating States

4.13.1. Run

When a CPU is in *Run* mode, all application tasks are executed.

4.13.2. Stop

When a CPU is in *Stop* mode, all application tasks are stopped. The variable values in the tasks are kept with the current value and output points go to the safe state.

When a CPU goes to the *Stop* mode due to the download of an application, the variables in the application tasks will be lost except the persistent variables type.

4.13.3. Breakpoint

When a debugging mark is reached in a task, it is interrupted. All the active tasks in the application will not be interrupted, continuing their execution. With this feature, it's possible to go through and investigate the program flow step by step in *Online* mode according to the positions of the interruptions included through the editor.

For further information about the use of breakpoints, please consult the MasterTool IEC XE Utilization Manual - MU299609.

4.13.4. Exception

When a CPU is in *Exception* it indicates that some improper operation occurred in one of the application active tasks. The task which caused the Exception will be suspended and the other tasks will pass for the Stop mode. It is only possible to take off the tasks from this state and set them in execution again after a new CPU start condition. Therefore, only with a *Reset Warm*, *Reset Cold*, *Reset Origin* or a CPU restart puts the application again in Run mode.

4.13.5. Reset Warm

This command puts the CPU in *Stop* mode and initializes all the application tasks variables, except the persistent and retentive type variables. The variables initialized with a specific value will assume exactly this value, the other variables will assume the standard initialization value (zero).

4.13.6. Reset Cold

This command puts the CPU in *Stop* mode and initializes all the application tasks variables, except the persistent type variables. The variables initialized with a specific value will assume exactly this value, the other variables will assume the standard initialization value (zero).

4.13.7. Reset Origin

This command removes all application task variables, including persistent type variables, deletes the application CPU and puts the CPU in Stop mode.

Notes:

Reset: When a Reset is executed, the breakpoints defined in the application are disabled.

Command: To execute the commands *Reset Warm*, *Cold* or *Origin*, it's necessary to have MasterTool IEC XE in *Online* mode with the CPU.

4.13.8. Reset Process Command (IEC 60870-5-104)

This process reset command can be solicited by IEC 60870-5-104 clients. After answer the client, the CPU start a rebooting process, as if being done an energizing cycle.

In case of redundant PLCs, the process reset command is synchronized with the non-active PLC, resulting the reboot of both PLCs.

The standard IEC 60870-5-104 foresee a qualification value pass (0..255) with the process reset command, but this “parameter” is not considered by the CPU.

4.14. Programs (POUs) and Global Variable Lists (GVLs)

The project created by MasterTool IEC XE contains a set of program modules (POUs) and global variables lists that aims to facilitate the programming and utilization of the controller. The following sections describe the main elements that are part of this standard project structure.

4.14.1. MainPrg Program

The MainTask is associated to one unique POU of program type, named MainPrg. The MainPrg program is created automatically and cannot be edited by user.

The MainPrg program code is the following, in ST language:

```
(*Main POU associated with MainTask that calls StartPrg,  
UserPrg/ActivePrg and NonSkippedPrg.  
This POU is blocked to edit.*)  
  
PROGRAM MainPrg  
VAR  
    isFirstCycle : BOOL := TRUE;  
END_VAR  
  
SpecialVariablesPrg();  
IF isFirstCycle THEN  
    StartPrg();  
    isFirstCycle := FALSE;  
ELSE  
    UserPrg();  
END_IF;
```

MainPrg call other two POUs of program type, named *StartPrg* and *UserPrg*. While the *UserPrg* is always called, the *StartPrg* is only called once in the PLC application start.

To the opposite of *MainPrg* program, that must not be modified, the user can change the *StartPrg* and *UserPrg* programs. Initially, when the project is created from the wizard, these two programs are created *empty*, but the user might insert code in them.

4.14.2. StartPrg Program

In this POU the user might create logics, loops, start variables, etc. that will be executed only one time in the first PLC's cycle, before execute *UserPrg* POU by the first time. And not being called again during the project execution.

In case the user load a new application, or if the PLC gets powered off, as well as in *Reset Origin*, *Reset Cold* and *Reset Warm* conditions, this POU is going to be executed again.

4.14.3. UserPrg Program

In this POU the user must create the main application, responsible by its own process control. This POU is called by the main POU (MainPrg).

The user can also create additional POU's (programs, functions or function blocks), and called them or instance them inside UserPrg POU, to ends of its program instruction. Also it is possible to call functions and instance function blocks defined in libraries.

4.14.4. GVL System_Diagnostics

The *System_Diagnostics* GVL contains the diagnostic variables of the CPU, of the communication interface (Ethernet and PROFIBUS) and of all communication drivers. This GVL isn't editable and the variables are declared automatically with type specified by the device to which it belongs when it is added to the project.

ATTENTION

In *System_Diagnostics* GVL, are also declared the diagnostic variables of the direct representation MODBUS Client/Master Requests.

Some devices, like the MODBUS Symbol communication driver, doesn't have its diagnostics allocated at %Q variables with the AT directive. The same occurs with newest communication drivers, as Server IEC 60870-5-104.

The following picture shows an example of the presentation of this GVL when in *Online* mode.

Device.Application.System_Diagnostics				
Expression	Type	Value	Address	Con
⊕ DG_IEC_60870_5_104_Server	T_DIAG_IEC104_SERVER_1			DG_I
⊖ DG_MODBUS_Symbol_Client	T_DIAG_MODBUS_ETH_CLIENT_1			DG_I
⊕ tDiag	T_DIAG_MODBUS_DIAGNOSTICS_CLIENT			
⊖ byDiag_1_reserved	BYTE	0		Rese
⊕ tCommand	T_DIAG_MODBUS_COMMANDS			
⊖ byDiag_3_reserved	BYTE	0		Rese
⊖ tStat	T_DIAG_MODBUS_ETH_CLIENT_STATS			
⊖ wTXRequests	WORD	1589		Coun
⊖ wRXNormalResponses	WORD	1589		Coun
⊖ wRXExceptionResponses	WORD	0		Coun
⊖ wRXIllegalResponses	WORD	0		Coun
⊖ wDiag_12_reserved	WORD	0		Rese
⊖ wDiag_14_reserved	WORD	0		Rese
⊖ wDiag_16_reserved	WORD	0		Rese
⊖ wDiag_18_reserved	WORD	0		Rese
⊕ DG_MODBUS_Symbol_Client_NX5000	T_DIAG_MODBUS_ETH_CLIENT_1			DG_I
⊕ DG_MODBUS_Symbol_RTU_Master	T_DIAG_MODBUS_RTU_MASTER_1			DG_I
⊕ DG_MODBUS_Symbol_Server_NX5000	T_DIAG_MODBUS_ETH_SERVER_1			DG_I
⊖ DG_NX3030	T_DIAG_NX3030_1		%QB66229	DG_I
⊕ tSummarized	T_DIAG_SUMMARIZED_1			
⊕ tDetailed	T_DIAG_DETAILED_1			
⊕ DG_NX5001	T_DIAG_NX5001_1		%QB66922	DG_I
⊕ DG_MODBUS_Client	T_DIAG_MODBUS_ETH_CLIENT_1		%QB67191	DG_I
⊕ DG_MBUS_Direct_1_Mapping_000	T_DIAG_MODBUS_ETH_MAPPING_1		%QB67211	DG_I
⊖ byStatus	T_DIAG_MODBUS_ETH_MAPPING_STAT...			
⊖ bCommIdle	BIT	FALSE		Comr
⊖ bCommExecuting	BIT	FALSE		Comr
⊖ bCommPostponed	BIT	TRUE		Comr
⊖ bCommDisabled	BIT	FALSE		Comr
⊖ bCommOk	BIT	TRUE		Previ
⊖ bCommError	BIT	FALSE		Previ
⊖ bCommAborted	BIT	FALSE		Previ
⊖ bDiag_7_reserved	BIT	FALSE		Rese
⊖ eLastErrorCode	MASTER_ERROR_CODE	NO_ERROR		Last
⊖ eLastExceptionCode	MODBUS_EXCEPTION	NO_EXCEPTION		Last
⊖ byDiag_3_reserved	BYTE	0		reser
⊖ wCommCounter	WORD	397		Coun
⊖ wCommErrorCounter	WORD	0		Coun
⊕ DG_MBUS_Direct_1_Mapping_001	T_DIAG_MODBUS_ETH_MAPPING_1		%QB67219	DG_I
⊕ DG_MBUS_Direct_1_Mapping_003	T_DIAG_MODBUS_ETH_MAPPING_1		%QB67235	DG_I
⊕ DG_MBUS_Direct_1_Mapping_002	T_DIAG_MODBUS_ETH_MAPPING_1		%QB67243	DG_I
⊕ DG_NX5000	T_DIAG_NX5000_1		%QB67251	DG_I

Figure 31: System_Diagnostics GVL in Online Mode

4.14.5. GVL Disables

The *Disables* GVL contains the MODBUS Master/Client by symbolic mapping requisition disabling variables. It is not mandatory, but it is recommended to use the automatic generation of these variables, which is done clicking in the button *Generate Disabling Variables* in device requisition tab. These variables are declared as type BOOL and follow the following structure:

Requisition disabling variables declaration:

```
[Device Name]_DISABLE_[Requisition Number] : BOOL;
```

Where:

Device name: Name that shows on Tree View to the MODBUS device.

Requisition Number: Requisition number that was declared on the MODBUS device requisition table following the sequence from up to down, starting on 0001.

Example:

Device.Application.Disables

```
VAR_GLOBAL
MODBUS_Device_DISABLE_0001 : BOOL;
MODBUS_Device_DISABLE_0002 : BOOL;
MODBUS_Device_DISABLE_0003 : BOOL;
MODBUS_Device_1_DISABLE_0001 : BOOL;
MODBUS_Device_1_DISABLE_0002 : BOOL;
END_VAR
```

The automatic generation through button *Generate Disabling Variables* only create variables, and don't remove automatically. This way, in case any relation is removed, its respective disabling variable must be removed manually.

The *Disables* GVL is editable, therefore the requisition disabling variables can be created manually without need of following the model created by the automatic declaration and can be used both ways at same time, but must always be of BOOL type. And it is need to take care to do not delete or change the automatic declared variables, cause them can being used for some MODBUS device. If the variable be deleted or changed then an error is going to be generated while the project is being compiled. To correct the automatically declared variable name, it must be followed the model exemplified above according to the device and the requisition to which they belong.

The following picture shows an example of the presentation of this GVL when in *Online* mode. If the variable values are TRUE it means that the requisition to which the variables belong is disabled and the opposite is valid when the variable value is FALSE.

Device.Application.Disables			
Expression	Type	Value	Prepared
 MODBUS_Slave_1_DISABLE_0001	BOOL	FALSE	
 MODBUS_Slave_1_DISABLE_0002	BOOL	TRUE	
 MODBUS_Slave_1_DISABLE_0003	BOOL	FALSE	
 MODBUS_Slave_1_DISABLE_0004	BOOL	FALSE	
 MODBUS_Server_1_DISABLE_0001	BOOL	FALSE	
 MODBUS_Server_1_DISABLE_0002	BOOL	FALSE	
 MODBUS_Server_1_DISABLE_0003	BOOL	FALSE	
 MODBUS_Server_1_DISABLE_0004	BOOL	TRUE	

Figure 32: Disable GVL in Online Mode

4.14.6. GVL IOQualities

The *IOQualities* GVL contains the quality variables of I/O modules declared on CPU's bus. This GVL is not editable and the variables are automatically declared as *LibDataTypes.QUALITY* type arrays, and dimensions according to I/Os quantities of the module to which it belongs when that is added to the project.

4. INITIAL PROGRAMMING

Example: Device.Application.IOQualities

```

VAR_GLOBAL
QUALITY_NX1001: ARRAY[0..15] OF LibDataTypes.QUALITY;
QUALITY_NX2020: ARRAY[0..15] OF LibDataTypes.QUALITY;
QUALITY_NX6000: ARRAY[0..7] OF LibDataTypes.QUALITY;
QUALITY_NX6100: ARRAY[0..3] OF LibDataTypes.QUALITY;
END_VAR

```

Once the application is in *RUN* it is possible to watch the I/O modules quality variables values that were added to the project through *IOQualities* GVL.

4.14.7. GVL Module_Diagnostics

The *Module_Diagnostics* GVL contains the diagnostics variables of the I/O modules used in the project, except by the CPU and communication drivers. This GVL isn't editable and the variables are automatically declared with type specified by the module, to which it belongs, when that is added to the project.

The following picture shows an example of the presentation of this GVL when in *Online* mode.

Expression	Type	Value	Address	Comment
DG_NX1001	T_DIAG_NX1001_1		%QB67008	DG_NX1001 diagnostics variable
tGeneral	T_DIAG_GENERAL_NX1001_1			
bReserved_8	BIT	FALSE		Reserved
bReserved_9	BIT	FALSE		Reserved
bReserved_10	BIT	FALSE		Reserved
bReserved_11	BIT	FALSE		Reserved
bReserved_12	BIT	FALSE		Reserved
bReserved_13	BIT	FALSE		Reserved
bReserved_14	BIT	FALSE		Reserved
bReserved_15	BIT	FALSE		Reserved
bActiveDiagnostics	BIT	FALSE		Module has active diagnostics
bFatalError	BIT	FALSE		Module has fatal error
bConfigMismatch	BIT	FALSE		Module has parameterization error
bWatchdogError	BIT	FALSE		Module has watchdog expired
bOTDSwitchError	BIT	FALSE		Module one touch diag switch error
bReserved_5	BIT	FALSE		Reserved
bReserved_6	BIT	FALSE		Reserved
bReserved_7	BIT	FALSE		Reserved
DG_NX1005	T_DIAG_NX1005_1		%QB67010	DG_NX1005 diagnostics variable
DG_NX2001	T_DIAG_NX2001_1		%QB67014	DG_NX2001 diagnostics variable
DG_NX2020	T_DIAG_NX2020_1		%QB67018	DG_NX2020 diagnostics variable
DG_NX6000	T_DIAG_NX6000_1		%QB67022	DG_NX6000 diagnostics variable
DG_NX6100	T_DIAG_NX6100_1		%QB67040	DG_NX6100 diagnostics variable
tGeneral	T_DIAG_GENERAL_NX6100_1			
bActiveDiagnosticsOutput00	BIT	FALSE		Output 00 with diagnostics
bActiveDiagnosticsOutput01	BIT	FALSE		Output 01 with diagnostics
bActiveDiagnosticsOutput02	BIT	FALSE		Output 02 with diagnostics
bActiveDiagnosticsOutput03	BIT	FALSE		Output 03 with diagnostics
bReserved_12	BIT	FALSE		Reserved
bReserved_13	BIT	FALSE		Reserved
bReserved_14	BIT	FALSE		Reserved
bReserved_15	BIT	FALSE		Reserved
bActiveDiagnostics	BIT	FALSE		Module has active diagnostics
bFatalError	BIT	FALSE		Module has fatal error
bConfigMismatch	BIT	FALSE		Module has parameterization error
bWatchdogError	BIT	FALSE		Module has watchdog expired
bOTDSwitchError	BIT	FALSE		Module one touch diag switch error
bCalibrationError	BIT	FALSE		Module has calibration error
bNoExternalSupply	BIT	FALSE		External power s...y is below the ...
bReserved_07	BIT	FALSE		Reserved
tDetailed	T_DIAG_DETAILED_NX6100_1			
tAnalogOutput_00	T_DIAG_ANALOG_OUTPUT			
tAnalogOutput_01	T_DIAG_ANALOG_OUTPUT			
tAnalogOutput_02	T_DIAG_ANALOG_OUTPUT			

Figure 33: Module_Diagnostics GVL in Online Mode

4.14.8. GVL Qualities

The *Qualities* GVL contains the quality variable of the internal variables MODBUS Master/Client of symbolic mapping. It is not mandatory but is recommended to use these variables' automatic generation, what is done clicking on button *Generate Quality Variables* in the device mapping tab. These variables are declared as *LibDataTypes.QUALITY* type and follow the following structure:

Quality mapping variable declaration:

```
[Device Name]_QUALITY_[Mapping Number]: LibDataTypes.QUALITY;
```

Where:

Device Name: Name that appear at the Tree View to the device.

Mapping Number: Number of the mapping that was declared on the device mapping table, following the up to down sequence, starting with 0001.

ATTENTION

It is not possible to associate quality variables to the direct representation MODBUS Master/Client drivers' mappings. Therefore it is recommended the use of symbolic mapping MODBUS drivers.

Example: Device.Application.Qualities

```
VAR_GLOBAL
MODBUS_Device_QUALITY_0001: LibDataTypes.QUALITY;
MODBUS_Device_QUALITY_0002: LibDataTypes.QUALITY;
MODBUS_Device_QUALITY_0003: LibDataTypes.QUALITY;
END_VAR
```

The *Qualities* GVL is editable, therefore the mapping quality variables can be created manually without need to follow the automatic declaration model, and can be used both ways at same time. But must always be of *LibDataTypes.QUALITY* type and take care to don't delete or change a variable automatically declared, because they might being used by some device. If the variable be deleted or changed an error is going to be generated while the project is being compiled. To correct the automatically declared variable name, it must be followed the model exemplified above according to the device and the requisition to which they belong.

To the MODBUS communication devices the quality variables behave on the way showed at Table 49.

The following picture shows an example of the presentation of this GVL when in *Online* mode.

ATTENTION

If a symbolic mapping MODBUS Client/Master driver's variable be mapped in IEC 60870-5-104 Server driver, it is necessary that the MODBUS mapping quality variables had been created to generate valid quality events to such IEC 60870-5-104 Server points. Case opposite, aren't going to be generated "bad" quality events to IEC 60870-5-104 Server clients in the situations that MODBUS Master/Client can't communicate with its slaves/servers, by example.

Device.Application.Qualities				
Expression	Type	Value	Address	Comment
MODBUS_Slave_1_QUALITY_0001	LibDataTypes.QUALITY			
VALIDITY	QUALITY_VALIDITY	VALIDITY_GOOD		Quality validity
FLAGS	QUALITY_FLAGS			Quality flags
FLAG_OUT_OF_RANGE	BIT	FALSE		Bit 8
FLAG_INACCURATE	BIT	FALSE		Bit 9
FLAG_OLD_DATA	BIT	FALSE		Bit 10
FLAG_FAILURE	BIT	FALSE		Bit 11
FLAG_OPERATOR_BLOCKED	BIT	FALSE		Bit 12
FLAG_TEST	BIT	FALSE		Bit 13
FLAG_RESERVED_0	BIT	FALSE		Bit 14
FLAG_RESERVED_1	BIT	FALSE		Bit 15
FLAG_RESTART	BIT	FALSE		Bit 0
FLAG_COMM_FAIL	BIT	FALSE		Bit 1
FLAG_REMOTE_SUBSTITU...	BIT	FALSE		Bit 2
FLAG_LOCAL_SUBSTITUTED	BIT	FALSE		Bit 3
FLAG_FILTER	BIT	FALSE		Bit 4
FLAG_OVERFLOW	BIT	FALSE		Bit 5
FLAG_REFERENCE_ERROR	BIT	FALSE		Bit 6
FLAG_INCONSISTENT	BIT	FALSE		Bit 7
MODBUS_Slave_1_QUALITY_0002	LibDataTypes.QUALITY			
MODBUS_Slave_1_QUALITY_0003	LibDataTypes.QUALITY			
MODBUS_Slave_1_QUALITY_0004	LibDataTypes.QUALITY			
MODBUS_Server_1_QUALITY_0001	LibDataTypes.QUALITY			
MODBUS_Server_1_QUALITY_0002	LibDataTypes.QUALITY			
MODBUS_Server_1_QUALITY_0003	LibDataTypes.QUALITY			
VALIDITY	QUALITY_VALIDITY	VALIDITY_QUESTIONABLE		Quality validity
FLAGS	QUALITY_FLAGS			Quality flags
FLAG_OUT_OF_RANGE	BIT	FALSE		Bit 8
FLAG_INACCURATE	BIT	FALSE		Bit 9
FLAG_OLD_DATA	BIT	TRUE		Bit 10
FLAG_FAILURE	BIT	FALSE		Bit 11
FLAG_OPERATOR_BLOCKED	BIT	FALSE		Bit 12
FLAG_TEST	BIT	FALSE		Bit 13
FLAG_RESERVED_0	BIT	FALSE		Bit 14
FLAG_RESERVED_1	BIT	FALSE		Bit 15
FLAG_RESTART	BIT	FALSE		Bit 0
FLAG_COMM_FAIL	BIT	TRUE		Bit 1
FLAG_REMOTE_SUBSTITU...	BIT	FALSE		Bit 2
FLAG_LOCAL_SUBSTITUTED	BIT	FALSE		Bit 3
FLAG_FILTER	BIT	FALSE		Bit 4
FLAG_OVERFLOW	BIT	FALSE		Bit 5
FLAG_REFERENCE_ERROR	BIT	FALSE		Bit 6
FLAG_INCONSISTENT	BIT	FALSE		Bit 7
MODBUS_Server_1_QUALITY_0004	LibDataTypes.QUALITY			

Figure 34: Qualities GVL in Online Mode

4.14.9. GVL ReqDiagnostics

The *ReqDiagnostics* GVL contains the requisition diagnostics variables of symbolic mapping MODBUS Master/Client. It is not mandatory, but recommended the use of these variables' automatic generation, what is done by clicking in the button *Generate Diagnostics Variables* in device requests tab. These variables declaration follow the following structure:

Requisition diagnostic variable declaration:

```
[Device Name]_REQDG_[Requisition Number]: [Variable Type];
```

Where:

Device Name: Name that appear at the Tree View to the device.

Mapping Number: Number of the mapping that was declared on the device mapping table, following the up to down sequence, starting with 0001.

Variable Type: NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS_RTU_MAPPING_1 to MODBUS Master and NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS_ETH_MAPPING_1 to MODBUS Client.

ATTENTION

The requisition diagnostics variables of direct mapping MODBUS Master/Client are declared at *System_Diagnostics* GVL.

Example:

Device.Application.ReqDiagnostics

VAR_GLOBAL

```

MODBUS_Device_REQDG_0001 : NXMODBUS_DIAGNOSTIC_STRUCTS.
                           T_DIAG_MODBUS_RTU_MAPPING_1;
MODBUS_Device_REQDG_0002 : NXMODBUS_DIAGNOSTIC_STRUCTS.
                           T_DIAG_MODBUS_RTU_MAPPING_1;
MODBUS_Device_REQDG_0003 : NXMODBUS_DIAGNOSTIC_STRUCTS.
                           T_DIAG_MODBUS_RTU_MAPPING_1;
MODBUS_Device_1_REQDG_0001 : NXMODBUS_DIAGNOSTIC_STRUCTS.
                              T_DIAG_MODBUS_ETH_MAPPING_1;
MODBUS_Device_1_REQDG_0002 : NXMODBUS_DIAGNOSTIC_STRUCTS.
                              T_DIAG_MODBUS_ETH_MAPPING_1;
    
```

END_VAR

The *ReqDiagnostics* GVL is editable, therefore the requisitions diagnostic variables can be manually created without need to follow the model created by the automatic declaration. Both ways can be used at same time, but the variables must always be of type referring to the device. And take care to don't delete or change a variable automatically declared, because they might be used by some device. If the variable be deleted or changed an error is going to be generated while the project is being compiled. To correct the automatically declared variable name, it must be followed the model exemplified above according to the device and the requisition to which they belong.

The following picture shows an example of the presentation of this GVL when in *Online* mode.

Device.Application.ReqDiagnostics		
Expression	Type	Value
MODBUS_Slave_1_REQDG_0001	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	
byStatus	T_DIAG_MODBUS_RTU_MAPPING_STATUS	
eLastErrorCode	MASTER_ERROR_CODE	NO_ERROR
eLastExceptionCode	MODBUS_EXCEPTION	NO_EXCEPTION
byDiag_3_reserved	BYTE	0
wCommCounter	WORD	969
wCommErrorCounter	WORD	0
MODBUS_Slave_1_REQDG_0002	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	
MODBUS_Slave_1_REQDG_0003	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	
MODBUS_Slave_1_REQDG_0004	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	
MODBUS_Server_1_REQDG_0001	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	
MODBUS_Server_1_REQDG_0002	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	
MODBUS_Server_1_REQDG_0003	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	
byStatus	T_DIAG_MODBUS_ETH_MAPPING_STATUS	
eLastErrorCode	MASTER_ERROR_CODE	ERR_CONNECTION_TIMEOUT
eLastExceptionCode	MODBUS_EXCEPTION	NO_EXCEPTION
byDiag_3_reserved	BYTE	0
wCommCounter	WORD	116
wCommErrorCounter	WORD	49
MODBUS_Server_1_REQDG_0004	NXMODBUS_DIAGNOSTIC_STRUCTS.T_DIAG_MODBUS...	

Figure 35: ReqDiagnostics GVL in Online Mode

5. Configuration

The Nexto Series CPUs are configured and programmed through the MasterTool IEC XE software. The configuration made defines the behavior and utilization modes for peripherals use and the CPUs special features. The programming represents the Application developed by the user.

5.1. Device

5.1.1. User Management and Access Rights

It provides functions to define users accounts and to configure the access rights to the project and to the CPU. Using the software MasterTool IEC XE, it's possible to create and manage users and groups, setting, different access right levels to the project.

Simultaneously, the Nexto CPUs have an user permissions management system that blocks or allows certain actions for each user group in the CPU. For more information, consult the MasterTool IEC XE User Manual MT8500 – MU299609, in the User Management and Access Rights section.

5.1.2. PLC Settings

On this tab of the generic device editor, you make the basic settings for the configuration of the PLC, for example the handling of inputs and outputs and the bus cycle task.

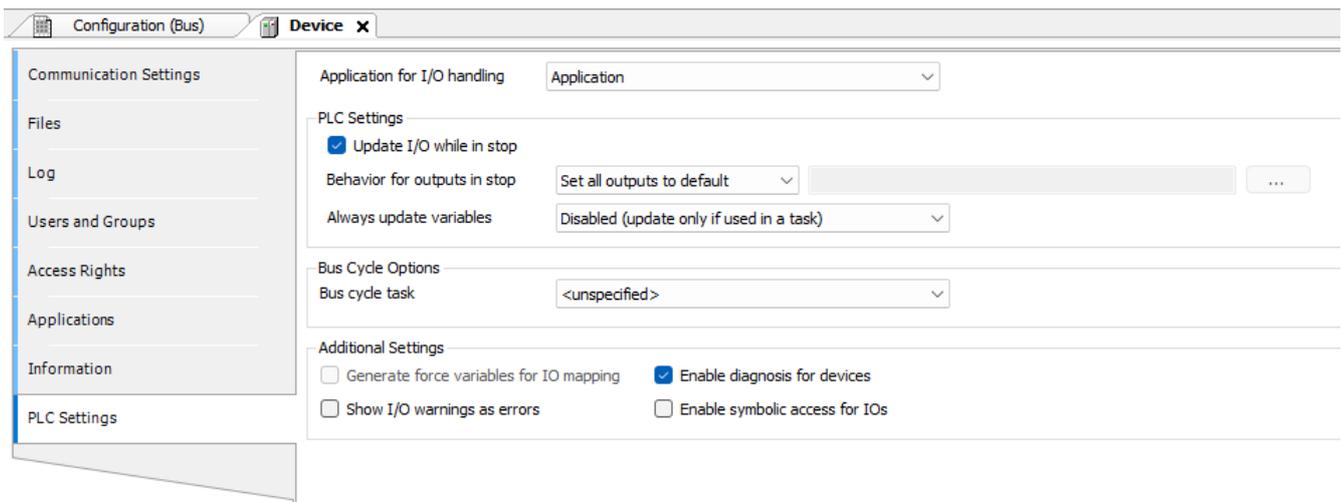


Figure 36: PLC Settings

Parameter	Description
Application for I/O handling	Application that is responsible for the I/O handling.
Update I/O while in stop	<p>TRUE: The values of the input and output channels are also refreshed when the PLC is in STOP mode. If the watchdog detects a malfunction, the outputs are set to the predefined default values.</p> <p>FALSE: The values of the input and output channels in STOP mode are not refreshed.</p>

Parameter	Description
Behavior for outputs in stop	<p>Handling of the output channels when the controller enters STOP mode:</p> <p>Retain values: The current values are retained.</p> <p>All outputs to default value: The default values resulting from the I/O mapping are assigned.</p> <p>Execute program: The handling of the output values is controlled by a program contained in the project which is executed in STOP mode. Enter the name of the program in the field on the right.</p>
Always update variables	<p>Globally defines whether or not the I/O variables are updated in the bus cycle task.</p> <p>This setting is effective for the I/O variables of the slaves and modules only if "deactivated" is defined in their update settings.</p> <p>Deactivated (update only if used in a task): The I/O variables are updated only if they are used in a task.</p> <p>Enabled 1 (use bus cycle task if not used in any task): The I/O variables in the bus cycle task are updated if they are not used in any other task.</p> <p>Enabled 2 (always in bus cycle task): All variables in each cycle of the bus cycle task are updated, regardless of whether they are used and whether they are mapped to an input or output channel.</p>
Bus cycle task	<p>Task that controls the bus cycle. By default the task defined by the device description is entered.</p> <p>By default, the bus cycle setting of the superordinate bus device applies (use cycle settings of the superordinate bus). This means that the device tree is searched upwards for the next valid definition of the bus cycle task.</p>
Generate force variables for IO mapping	<p>TRUE: When compiling the application, two global variables are created for each I/O channel which is mapped to a variable in the I/O Mapping dialog.</p>
Enable diagnostics for devices	<p>TRUE: The CAA Device Diagnosis library is integrated in the project. An implicit function block is generated for each device. If there is already a function block for the device, then either an extended function block is generated (example: EtherCAT) or another function block instance is added. This then contains a general implementation of the device diagnostics.</p>
Show I/O warnings as errors	<p>Warnings concerning the I/O configuration are displayed as errors.</p>
Enable symbolic access for IOs	<p>TRUE: It allows access to I/O points from the internal symbolic name generated in the device declaration. The symbolic name can be consulted in the <i>Channel</i> column on the <i>Bus I/O Mapping</i> tab of each device.</p>

Table 38: PLC Settings

ATTENTION

The Nexto (NX), Nexto Jet (NJ), Nexto XF and Xtorm (HX) products do not support the *Enable symbolic access for I/O* parameter.

5.2. CPU Configuration

5.2.1. General Parameters

The parameters related below are part of the CPU configuration included in the application. Each item must be properly verified for the correct project execution.

Besides these parameters, it is possible to change the name of each module inserted in the application by clicking the right button on the module. In the *Properties* item from the *Common* sheet, change the name, what is limited to 24 characters.

Settings	Description	Standard	Options
Diagnostics Area (%Q)			
%Q Start Address	Starting address of the UCP diagnostics (%Q)	Automatically allocated on project creation.	0 to 64682
Size	Size of diagnostics area in bytes	1253	It is not possible to change the size of the CPU diagnostics area
Retaining Area (%Q)			
%Q Start Address	Starting address of the retentive data memory (%Q)	4096	0 to 65535
Size	Retain data memory size in bytes	2048	0 to 65535
Persistent Area (%Q)			
%Q Start Address	Persistent data memory start address (%Q)	12288	0 to 65535
Size	Persistent data memory size in bytes	2048	0 to 65535
CPU Parameters			
Start User Application after Reset by Watchdog	When enabled, starts the user application after resetting the hardware watchdog or restarting Runtime, but maintaining the diagnostic indication via WD LED and via variables.	Disabled	Enabled Disabled
Hot Swap	Module hot swap mode	Enabled, without startup consistency (may vary according to CPU model)	<ul style="list-style-type: none"> - Disabled, only for declared modules - Disabled (with startup consistency) - Disabled, without startup consistency - Enabled, with startup consistency only for declared modules - Enabled, with startup consistency - Enabled, without startup consistency

Settings	Description	Standard	Options
Enable internal termination	CAN port Parameters		
	When enabled, use internal termination on the CAN interface	Unmarked	- Checked: internal termination on the CAN interface is enabled. - Unchecked: internal termination on the CAN interface is disabled.

Table 39: CPU settings

ATTENTION

When the initial address or the retentive or persistent data memory size is changed in the user application, the memory is reallocated, which makes the retentive and persistent variable area clean. So the user has to be careful so as not to lose the saved data in the memory.

ATTENTION

In situations where the symbolic persistent memory area is modified, a message will be displayed by MasterTool IEC XE programmer, to choose the behavior for this area after charging the modified program. The choice of this behavior does not affect the persistent area of direct representation, which is always clean.

5.2.1.1. Hot Swap

Nexto Series CPUs have the possibility of I/O modules change in the bus with no need for system turn off and without information loss. This feature is known as hot swap.

CAUTION

Nexto Series CPUs do not guarantee the persistent and retentive variables retentivity in case the power supply or even the CPU is removed from the energized backplane rack.

On the hot swap, the related system behavior modifies itself following the configuration table defined by the user which represents the options below:

- Disable, for declared modules only
- Disabled (with startup consistency)
- Disabled, without startup consistency
- Enabled, with startup consistency for declared modules only
- Enabled, with startup consistency
- Enabled, without startup consistency

Therefore, the user can choose the behavior that the system must assume in abnormal bus situations and when the CPU is in *Run Mode*. The table below presents the possible abnormal bus situations.

Situation	Possible causes
Incompatible configuration	- Some module connected to the bus is different from the model that is declared in configuration.
Absent module	- The module was removed from the bus. - Some malfunctioning module is not responding to CPU - Some bus position is malfunctioning.

Table 40: Bus Abnormal Situations

For further information regarding the diagnostics correspondent to the above described situations, see *Diagnostics via Variables*.

If a module is present in a specific position in which should not exist according to the configuration modules, this module is considered as non-declared. The options of hot swap *Disabled, for Declared Modules Only* and *Enabled, with Startup Consistency for Declared Modules Only* do not take into consideration the modules that are in this condition.

5.2.1.1.1. Hot Swap Disabled, for Declared Modules Only

In this configuration, the CPU is immediately in *Stop Mode* when an abnormal bus situation (as described on Table 40) happens. The LED DG starts to blink 4x (according to Table 41). In this case, in order to make the CPU to return to the normal state *Run*, in addition to undo what caused the abnormal situation, it is necessary to execute a *Reset Warm* or a *Reset Cold*. If a *Reset Origin* is carried out, it will be necessary to perform the download so that the CPU can return to the normal state (*Run*). The *Reset Warm*, *Reset Cold* and *Reset Origin* commands can be done by MasterTool IEC XE in the *Online* menu.

The CPU will remain in normal *Run* even if find a module not declared on the bus.

5.2.1.1.2. Hot Swap Disabled

This setting does not allow any abnormal situation in the bus (as shown in Table 40) modules including undeclared and present on the bus. The CPU enters in *Stop* mode, and the DG LED begins to blink 4x (as in Table 41). For these cases, to turn the CPU back to normal *Run*, in addition to undo what caused the abnormal situation it is necessary to perform a *Reset Warm* or *Reset Cold*. If a *Reset Origin* is done, you need to download the project so that the CPU can return to normal *Run*. The *Reset Warm*, *Reset Cold* and *Reset Origin* commands can be done by MasterTool IEC XE in the *Online* menu.

5.2.1.1.3. Hot Swap Disabled, without Startup Consistency

Allows the system to start up even when some module is in an abnormal bus situation (as shown in Table 40). Abnormal situations are reported via diagnosis.

Any modification to the bus will cause the CPU to enter *Stop Mode*, and the DG LED will start blinking 2x (as in Table 41). In order for the CPU to return to the normal *Run* state in these cases, it is necessary to perform a *Reset Warm* or *Reset Cold*. If a *Reset Origin* is performed, it will be necessary to download the CPU so that the CPU can return to the normal *Run* state. The *Reset Warm*, *Reset Cold* and *Reset Origin* commands can be done by MasterTool IEC XE in the *Online* menu.

5.2.1.1.4. Hot Swap Enabled, with Startup Consistency for Declared Modules Only

“Startup” is the interval between the CPU energization (or reset command or application download) until the first time the CPU gets in *Run Mode* after been switched on. This configuration verifies if any abnormal bus situation has occurred (as described on Table 40) during the start. In affirmative case, the CPU gets in *Stop Mode* and the LED DG starts to blink 4x (according to Table 41). Afterwards, in order to set the CPU in *Run* mode, further to fix what caused the abnormal situation, it is necessary to execute a *Reset Warm* or *Reset Cold* command, which can be done by the MasterTool IEC XE (*Online* menu). If a *Reset Origin* is carried out, it will be necessary to perform the download so that the CPU can return to the normal state (*Run*).

After the start, if any module present any situation described in the previous table, the system will continue to work normally and will signalize the problem via diagnostics.

If there is no other abnormality for the declared modules, the CPU will go to the normal state (*Run*) even if a non-declared module is present on the bus.

ATTENTION

In this configuration when a power fault occurs (even temporally), *Reset Warm* Command, *Reset Cold* Command or a new application *Download* has been executed, and if any module is in an abnormal bus situation, the CPU will get into *Stop Mode* and the LED DG will start to blink 4x (according to Table 41). This is considered a startup situation. This is the most advised option because guarantee the system integrity on its initialization and allows the modules change with a working system.

5.2.1.1.5. Hot Swap Enabled with Startup Consistency

This setting checks whether there has been any abnormal situation in the bus (as shown in Table 40) during the startup, even if there is no declared modules and present on the bus; if so, the CPU goes into *Stop* mode and the LED DG starts to blink 4x (as shown in Table 41). For these cases, to turn the CPU back to normal *Run*, in addition to undo what caused the abnormal situation it is necessary to perform a *Reset Warm* or *Reset Cold*. If a *Reset Origin* is done, you need to download the project so

that the CPU can return to normal *Run*. The *Reset Warm*, *Reset Cold* and *Reset Origin* commands can be done by MasterTool IEC XE in the *Online* menu.

5.2.1.1.6. Hot Swap Enabled without Startup Consistency

Allows the system to start working even if a module is in an abnormal bus situation (as described on Table 40). The abnormal situations are reported via diagnostics during and after the startup.

ATTENTION

This option is advised for the system implementation phase as it allows the loading of new applications and the power off without the presence of all configured modules.

5.2.1.1.7. How to do the Hot Swap

CAUTION

Before performing the Hot Swap it is important to discharge any possible static energy accumulated in the body. To do that, touch (with bare hands) on any metallic grounded surface before handling the modules. Such procedure guaranties that the module static energy limits are not exceeded.

ATTENTION

It is recommended the hot swapping diagnostics monitoring in the application control developed by the user in order to guarantee the value returned by the module is validated before being used.

The hot swap proceeding is described below:

- Unlock the module from the backplane rack, using the safety lock.
- Take off the module, pulling firmly.
- Insert the new module in the backplane rack.
- Certify the safety lock is completely connected. If necessary, push the module harder towards to the backplane rack.

In case of output modules is convenient the points to be disconnected when in the changing process, in order to reduce the generation of arcs in module connector. This must be done by switching off the power supply or by forcing the output points using the software tools. If the load is small, there is no need for disconnecting.

It is important to note that in the cases the CPU gets in *Stop* Mode and the DG LED starts to blink 4x (according to Table 41, due to any abnormal bus situation (as described on Table 40, the output modules have its points operation according to the module configuration when CPU toggles from *Run* Mode to *Stop* Mode. In case of application startup, when the CPU enters *Stop* Mode without having passed to the *Run* Mode, the output modules put their points in failure secure mode, in other words, turn it off (0 Vdc).

Regarding the input modules, if one module is removed from energized backplane rack, the logic point's state will remain in the last value. In the case a connector is removed, the logic point's state will be put in a safe state, it means zero or high impedance.

ATTENTION

Always proceed to the substitution of one module at a time for the CPU to update the modules state.

Below, Table 41 presents the bus conditions and the Nexto CPU DG LED operation state. For further information regarding the diagnostics LEDs states, see [Diagnostics via LED](#) section.

Condition	Enabled, with Startup Consistency	Enabled, with Startup Consistency for Declared Modules Only	Enabled, without Startup Consistency	Disabled	Disabled, for declared modules only	Disabled, without Startup Consistency
Non de- clared module	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Stop
Non de- clared module (startup condition)	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run
Absent module	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Stop
Absent module (startup condition)	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Run	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Run
Incompatible configura- tion	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run	LED DG: Blinks 2x Application: Run	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Stop
Incompatible configura- tion(startup condition)	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Run or LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Run
Duplicated slot address	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Stop
Non- operational module	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 4x Application: Stop	LED DG: Blinks 2x Application: Stop

Table 41: Hot Swap and Conditions Relations

Note:

Enabled, without startup consistency: When this hot-swap mode is configured, in normal situations when there's an incompatible module on the system's startup, the application will go from Stop to Run. However, if that module is configured as a NX5000 or a NX5001 and there's a different module in that position, the application will stay in Stop.

5.2.1.2. Retain and Persistent Memory Areas

The Nexto CPU allows the use of symbolic variables and output variables of direct representation as retentive or persistent variables.

The output variables of direct representation which will be retentive or persistent must be declared in the CPU *General Parameters*, as described at [CPU Configuration](#). Symbolic names also can be attributed to these output variables of direct representation using the AT directive, plus using the key word RETAIN or PERSISTENT on its declaration. For example, being %QB4096 and %QB20480 within the retentive and persistent memory, respectively:

```
PROGRAM UserPrg
VAR RETAIN
byRetentiveVariable_01 AT %QB4096 : BYTE;
END_VAR
VAR PERSISTENT
byPersistentVariable_01 AT %QB20480 : BYTE;
END_VAR
```

In case the symbolic variables declared with the AT directive are not inside the respective retentive and/or persistent memory, errors during the code generation in MasterTool can be presented, informing that there are non-retentive or non-persistent variables defined in the retentive or persistent memory spaces.

Regarding the symbolic variables which will be retentive or persistent, only the retentive variables may be local or global, as the persistent symbolic variables shall always be global. For the declaration of retentive symbolic variables, it must be used the key word *RETAIN*. For example, for local variables:

```
PROGRAM UserPrg
VAR RETAIN
  wLocalSymbolicRetentiveVariable_01 : WORD;
END_VAR
```

Or, for global variables, declared within a list of global variables:

```
VAR_GLOBAL RETAIN
  wGlobalSymbolicRetentiveVariable_01 : WORD;
END_VAR
```

On the other hand, the persistent symbolic variables shall be declared in a Persistent Variables object, being added to the application. These variables will be global and will be declared in the following way within the object:

```
VAR_GLOBAL PERSISTENT RETAIN
  wGlobalSymbolicPersistentVariable_01 : WORD;
END_VAR
```

```

VAR_GLOBAL PERSISTENT RETAIN
  wGlobalSymbolicPersistentVariable_01 : WORD;
END_VAR

VAR_GLOBAL RETAIN
  wGlobalSymbolicRetentiveVariable_01 : WORD;
END_VAR
    
```

5.2.1.3. CAN Port Parameters

The CAN port parameters are related to the CAN interface.

Configuration	Description	Default	Options
Enable internal termination	Enables internal CAN port termination	Unmarked	- Marked - Unmarked

Table 42: CAN Port Parameters

5.2.2. External Event Configuration

The external event is a feature available in the CPU which enables a digital input, configured by the user, when activated, triggers the execution of a specific task with user-defined code. Thus, it is possible that through this input, when triggered, interrupt the execution of the main application and run the set application in the task *ExternInterruptTask00*, which has higher priority than other application tasks. Because the inputs and outputs are updated in the context of the MainTask task, the External Event task does not have the input and output data updated at the time of its call. If necessary, use the I/O update functions.

It is also important to note that, to avoid the generation of several events in a very short space of time, that was limited the treatment of this type of event in every 10 ms, i.e., if two or more events occurs during 10 ms after the first event, the second and subsequent events are discarded. This limitation is imposed to prevent an external event that is generated in an uncontrolled way, do not block the CPU, since the task has a higher priority over the others.

To configure an external event is necessary to insert a digital input module and perform the configurations described below, in the CPU, through the MT8500 programming tool software.

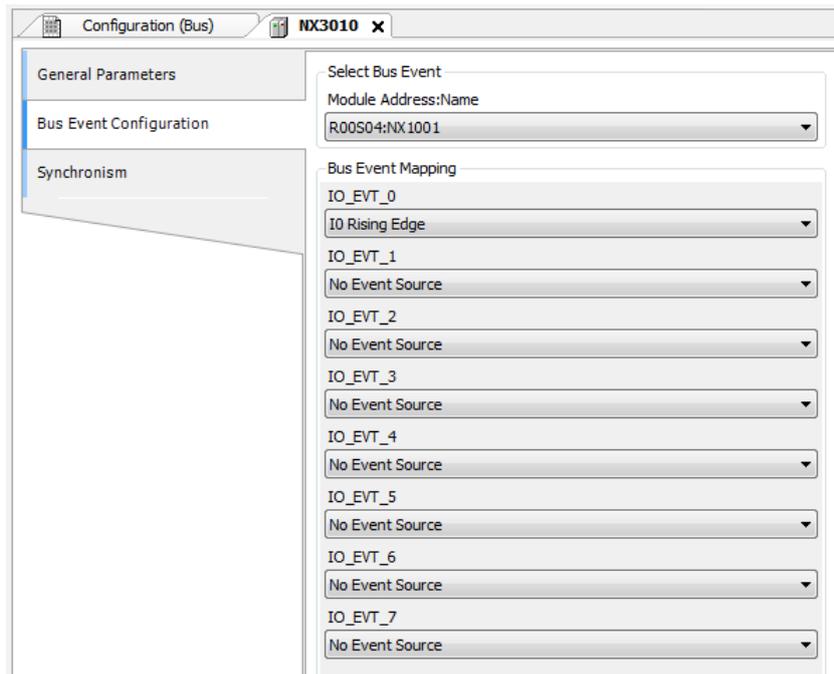


Figure 37: Configuration Screen for External Event in CPU

In the configuration external event tab, within the CPU settings, it is necessary to select which module will be the interruption source, in the field *Module Address: Name*. Then it must be selected which input of this module will be responsible for the event generation (*IO_EVT_0*). In this selection the options described in the figure below can be chosen.

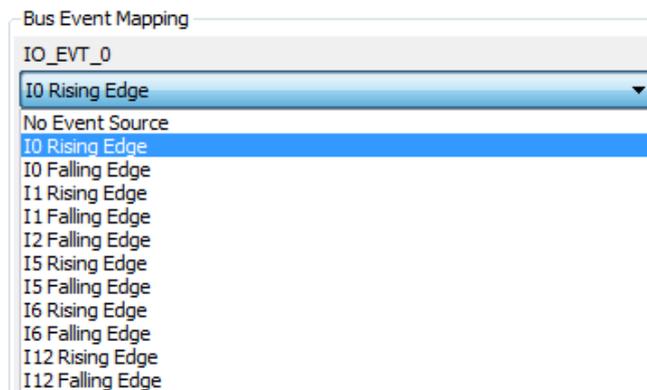


Figure 38: NX1001 Module External Event Source Options

In addition to configuring the CPU it is required to configure the task responsible for executing user-defined actions. In this case the user must use a project profile that supports external events. For further information see the section [Project Profiles](#). In the configuration screen of the *ExternInterruptTask00* (figure below), it is necessary to select the event source in the corresponding field. In this case, *IO_EVT_0* should be selected since the other origin sources (*IO_EVT_1* to *IO_EVT_7*) are not available. In the sequence, the field *POU* should be checked if the right POU is selected, because it will be used by the user to define the actions to be performed when an external event occurs.

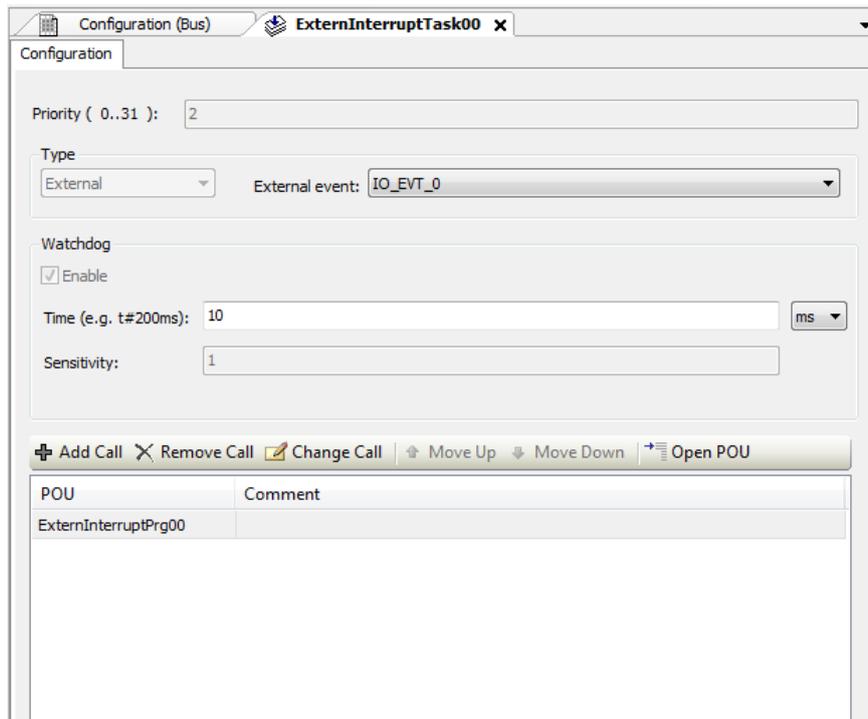


Figure 39: ExternInterruptTask00 Configuration Screen

5.2.3. Time Synchronization

For the time synchronization, Nexto Series CPUs use the SNTP (*Simple Network Time Protocol*) or the synchronism through IEC 60870-5-104.

To use the time sync protocols, the user must set the following parameters at *Synchronism* tab, accessed through the CPU, in the device tree:

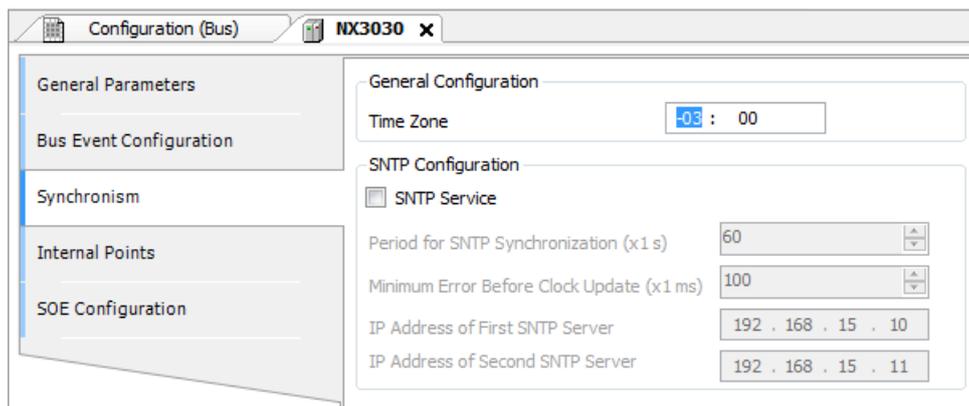


Figure 40: SNTP Configuration

Configuration	Description	Default	Options
Time Zone (hh:mm)	Time zone of the user location. Hours and minutes can be inserted.	-3:00	-12:59 to +13:59
SNTP Service	Enables the SNTP service.	Disabled	Disabled Enabled
Period for SNTP Synchronization (x1 s)	Time interval of the synchronization requests (seconds).	60	1 to 255
Minimum Error Before Clock Update (x1 ms)	Offset value acceptable between the server and client (milliseconds).	100	1 to 65519
IP Address of First SNTP Server	IP Address of the primary SNTP server.	192.168.15.10	1.0.0.1 to 223.255.255.254
IP Address of Second Second SNTP Server	IP Address of the secondary SNTP server.	192.168.15.11	1.0.0.1 to 223.255.255.254

Table 43: SNTP Configurations

Notes:

SNTP Server: It is possible to define a preferential address and another secondary one in order to access a SNTP server and, therefore, to obtain a synchronism of time. If both fields are empty, the SNTP service will remain disabled.

Time zone: The time zone configuration is used to convert the local time into UTC and vice versa. While some sync sources use the local time (IEC 60870-5-104 protocol, SetDateAndTime Function), others use the UTC time (SNTP). The UTC time is usually used to stamp events (DNP3, IEC 60870-5-104 and MasterTool Device Log), while the local time is used by others CPU's features (GetDateAndTime function, OTD date and time info).

It is allowed to enable more than one sync source on the project, however the device doesn't support the synchronism from more than one sync source during operation. Therefore there are implicitly defined a priority mechanism. The synchronism through SNTP is more priority than through IEC 60870-5-104 protocol. So, when both sources are enabled and SNTP server is present, it is going to be responsible for the CPU's clock sync, and any sync command from IEC 60870-5-104 is going to be denied.

5.2.3.1. IEC 60870-5-104

In case the synchronism is through IEC 60870-5-104 protocol, the user must enable the time sync at the protocol configuration screen to receive the clock synchronization. To set this option on the device, check the parameter *Enable Time Synchronization* available at the [Application Layer](#) section.

ATTENTION

If the PLC receives a time sync command from the control center, and this option is disabled, an error answer will be returned to that command. But if this option is enabled then a success message will be returned to the control center, even that the sync command be discarded for there is another synchronism method active with higher priority.

This synchronism method should be used only as an auxiliary synchronism method, once the precision of the clock sync process depends a lot on delays and traffic on the network, as well as the processor load on the CPU, as this mechanism is treated by a low priority task.

5.2.3.2. SNTP

When enabled, the CPU will behave as a SNTP client, which is, it will send requests of time synchronization to a SNTP/NTP server which can be in the local net or in the internet. SNTP client works with a resolution of 1 ms, but with an accuracy of 100 ms. The precision of the time sync through SNTP depends on the protocol configurations (minimum error to clock update) and the features of the Ethernet network where it is, if both client and server are in the same network (local) or in different networks (remote). Typically the precision is in tens of milliseconds order.

The CPU sends the cyclic synchronization requests according to the time set in the *Period for SNTP Synchronization* field. In the first synchronization attempt, just after the service start up, the request is for the first server set in the first server IP

address. In case it does not respond, the requests are directed to the second server set in the second server IP address providing a redundancy of SNTP servers. In case the second server does not respond either, the same process of synchronization attempt is performed again but only after the Period of Synchronization having been passed. In other words, at every synchronization period the CPU tries to connect once in each server, it tries the second server in case the first one does not respond. The waiting time for a response from the SNTP server is defined by default in 5 s and it cannot be modified.

If, after a synchronization, the difference between the current time of the CPU and the one received by the server is higher than the value set in the *Minimum Error Before Clock Update* parameter, the CPU time is updated. SNTP uses the time in the UTC (Universal Time Coordinated) format, so the *Time Zone* parameter needs to be set correctly so the time read by the SNTP will be properly converted to a local time.

The execution process of the SNTP client can be exemplified with the following steps:

1. Attempt of synchronization through the first server. In case the synchronization occurs successfully, the CPU waits the time for a new synchronization (*Period for SNTP Synchronization*) and will synchronize again with this server, using it as a primary server. In case of failure (the server does not respond in less than 5 s) step 2 is performed.
2. Attempt of synchronization through the second server. In case the synchronization occurs successfully, the CPU waits the time for a new synchronization (*Period for SNTP Synchronization*) and will try to synchronize with this server using the primary server. In case of failure (the server does not respond in less than 5 s) the time relative to the Synchronization Period is waited and step 1 is performed again.

As the waiting time for the response of the SNTP server is 5 s, the user must pay attention to lower than 10 s values for the Synchronization Period. In case the primary server does not respond, the time for the synchronization will be the minimum of 5 s (waiting for the primary server response and the synchronization attempt with secondary server). In case neither the primary server nor the secondary one responds, the synchronization time will be 10 s minimum (waiting for the two servers response and the new connection with first server attempt).

Depending on the SNTP server's subnet, the client will use the Ethernet interface that is in the corresponding subnet to make the synchronization requests. If there is no interface configured on the same subnet as the server, the request can be made by any interface that can find a route to the server.

ATTENTION

The SNTP Service depends on the user application only for its configuration. Therefore, this service will be executed even when the CPU is in *STOP* or *BREAKPOINT* modes, as long as there is an application in the CPU with the SNTP client enabled and correctly configured.

5.2.3.3. Daylight Saving Time (DST)

The DST configuration must be done indirectly through the function *SetTimeZone*, which changes the time zone applied to the RTC. In the beginning of the DST, it has to be used a function to increase the time zone in one hour. At the end of the DST, it is used to decrease it in one hour.

For further information, see the section [RTC Clock](#).

5.2.4. Internal Points

A communication point is storage on the CPU memory under form of two distinct variables. One represents the point's value (type BOOL, BYTE, WORD, etc...), while another, represents its quality (type QUALITY). Internal Points are those which the value and the quality are calculated internally by the user application, that is, they don't have an external origin like occur with points linked to IEDs (Communication drivers of type Master/Client) or to local I/O modules.

ATTENTION

Different from what happen with I/O modules declared on local bus, which have its own quality variables created by MasterTool (IOQualities GVL) and auto updated by the CPU, I/O modules declared on PROFIBUS remotes don't have. It is user responsibility to declare PROFIBUS point's quality variables, the association of these quality variables with the value variables at Internal Points tab, as well as generation and update of the quality variables value, from the existents PROFIBUS diagnostics: PROFIBUS I/O modules, PROFIBUS head and PROFIBUS Master.

This *Internal Points* configuration tab's function is to relate the variable which represents a point's value with the one which represents its quality. It must be used to relate value and quality variables internally created on the PLC program (as in a GVL), which ones typically will be posteriorly mapped to a communication driver, of type Server, for communication with the control center.

ATTENTION

If a value variable doesn't own a related quality variable, it will be reported as default a constant good quality (no significant indication) when the value variable is reported to a client or control center.

In this way, this tab purpose isn't to create or declare internal points. To do that, just declare value and/or quality variables in a GVL and map it on the communication driver.

The internal points configuration, viewed on the figure below, follow the parameters described on table below. It's possible to configure up to 5120 entries on *Internal Points* table.

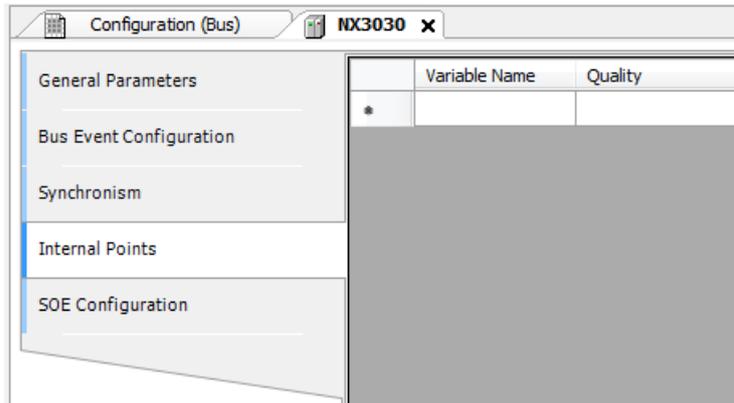


Figure 41: Internal Points Configuration Screen

Configuration	Description	Default	Options
Variable Name	Symbol variable which storage the internal point value	-	Accept variables of type BOOL, WORD, DWORD, LWORD, INT, DINT, LINT, UINT, UDINT, ULINT, REAL, LREAL or DBP. The variable can be simple, array or array's element and can be part of a struct.
Quality	Symbol variable which storage the internal point quality	-	QUALITY type variables (LibRtuStandard), which can be simple, array or array's element and can be part of a struct.

Table 44: Internal Points Configuration

The figure below show an example of two internal points configuration:

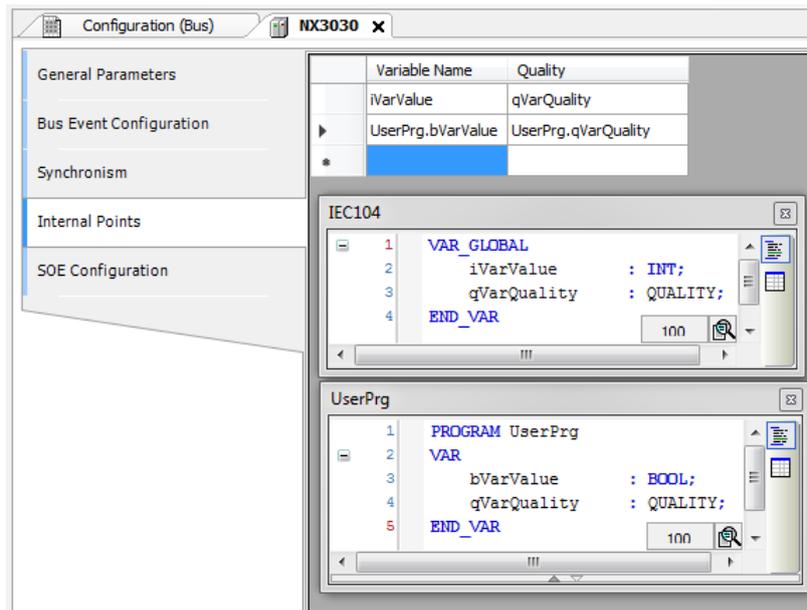


Figure 42: Internal Points Configuration Example

5.2.4.1. Quality Conversions

The internal point’s quality is a trust level information about the value stored on that point. The quality may inform, for example, that the value stored is out of range, or yet that it is valid, but low trusted.

The Standards IEC 61850, DNP3 and IEC104 have their own formats to representation of point’s quality information. The Nexto Series, by its turn, have its own quality format (but quite similar to IEC 61850) called *Internal Quality*. This format is defined by type QUALITY (library LibRtuStandard) and it is used internally to quality storage, allowing to be done conversion between protocols without information loss.

When it is done a mapping of a same communication point between two drivers, the quality conversion is automatically realized in two steps. For example: in case a communication point is mapped from a DNP3 Client driver to a IEC104 Server driver, first the quality will be converted from DNP3 format to internal format (and stored internally in the CPU), after that it will be converted from the internal format to IEC104 format.

The following tables define the protocols own formats conversion to internal format. Case it is necessary to consult the conversion between protocols, it is needed to analyze in two steps, looking each of the tables to internal format and after correlating them.

ATTENTION

In case of internal points mapped to communication drivers, it is not recommended to modify the value of quality flags that dont have a correspondent on the given protocol (i.e, flags that are not described on the following tables). This will result on generation of events equal to the previous one (but with a more recent timestamp) and, this way, depending on the configuration selected for the transmission mode of analog inputs events, it could overwrite the previous event if this one was not delivered to the control center yet.

5.2.4.1.1. Internal Quality

This is the QUALITY structure. The table shows detailed each of its components.

Bit	Name	Type	Description
0	FLAG_RESTART	BOOL	The RESTART flag indicates that the data haven’t been updated by the field since the device’s reset.

Bit	Name	Type	Description
1	FLAG_COMM_FAIL	BOOL	Indicates there is a communication failure on the way between the data origin device and the reports device.
2	FLAG_REMOTE_SUBSTITUTED	BOOL	If TRUE the data values are overwritten in the remote communication devices.
3	FLAG_LOCAL_SUBSTITUTED	BOOL	If TRUE the data value is overwritten by the device which generated this flag. This behavior might occur due to a working in diagnostic or temporary due to human intervention.
4	FLAG_FILTER	BOOL	Flag used to signalize and prevent the event communication channel overload, as oscillations (rapid changes) on the digital inputs.
5	FLAG_OVERFLOW	BOOL	This flag should indicates a quality problem, that the value, of the attribute to which the quality has been associated, is beyond representation.
6	FLAG_REFERENCE_ERROR	BOOL	This flag should identify that the value cannot be correct due to out of calibration reference.
7	FLAG_INCONSISTENT	BOOL	This flag should identify that an evaluation function has found an inconsistency.
8	FLAG_OUT_OF_RANGE	BOOL	This flag should indicates a quality problem that the attribute to which the quality has been associated is beyond the predefined values capacity.
9	FLAG_INACCURATE	BOOL	This flag should indicates that the value doesn't attend the declared precision of the source.
10	FLAG_OLD_DATA	BOOL	A value seems to be outdated. In case an update doesn't occur during a specific time period.
11	FLAG_FAILURE	BOOL	This flag should indicates that a watch function detected an internal or external failure.
12	FLAG_OPERATOR_BLOCKED	BOOL	Update blocked by operator.
13	FLAG_TEST	BOOL	This must be an additional identifier which can be used to classify a value being that a test value which won't be used to operational ends.
14-15	RESERVED	-	Reserved
16-17	VALIDITY	QUALITY_VALIDITY	<ul style="list-style-type: none"> 0 – Good (Trustfull value, means that there is no abnormal conditions) 1 – Invalid (Value doesn't match the IED's value) 2 – Reserved (Reserved) 3 – Questionable (Present value might be not the same from the IED)

Table 45: QUALITY Structure

4. INITIAL PROGRAMMING

5.2.4.1.2. IEC 60870-5-104 Conversion

The tables below presents the digital, analog, Step Position, Bitstring and counters internal point's conversion to IEC 60870-5-104 of Nexto Series available to MT8500.

Internal Points -> IEC 60870-5-104 Digital		
Internal Quality		
Flags	VALIDITY	IEC 60870-5-104 Quality
FLAG_RESTART	ANY	NOT TOPICAL
FLAG_COMM_FAIL	ANY	NOT TOPICAL
FLAG_REMOTE_SUBSTITUTED	ANY	SUBSTITUTED
FLAG_LOCAL_SUBSTITUTED	ANY	SUBSTITUTED
FLAG_FILTER	ANY	-
FLAG_OVERFLOW	ANY	-
FLAG_REFERENCE_ERROR	ANY	-
FLAG_INCONSISTENT	ANY	-
FLAG_OUT_OF_RANGE	ANY	-
FLAG_INACCURATE	ANY	-
FLAG_OLD_DATA	ANY	NOT TOPICAL
FLAG_FAILURE	ANY	INVALID
FLAG_OPERATOR_BLOCKED	ANY	BLOCKED
FLAG_TEST	ANY	-
ANY	VALIDITY_INVALID	INVALID

Table 46: Digital Points Conversion Internal to IEC 60870-5-104

Internal Points -> IEC 60870-5-104 Analog, Step Position and Bitstring		
Internal Quality		
Flags	VALIDITY	IEC 60870-5-104 Quality
FLAG_RESTART	ANY	NOT TOPICAL
FLAG_COMM_FAIL	ANY	NOT TOPICAL
FLAG_REMOTE_SUBSTITUTED	ANY	SUBSTITUTED
FLAG_LOCAL_SUBSTITUTED	ANY	SUBSTITUTED
FLAG_FILTER	ANY	-
FLAG_OVERFLOW	ANY	OVERFLOW
FLAG_REFERENCE_ERROR	ANY	INVALID
FLAG_INCONSISTENT	ANY	INVALID
FLAG_OUT_OF_RANGE	ANY	OVERFLOW
FLAG_INACCURATE	ANY	INVALID
FLAG_OLD_DATA	ANY	NOT TOPICAL
FLAG_FAILURE	ANY	INVALID
FLAG_OPERATOR_BLOCKED	ANY	BLOCKED
FLAG_TEST	ANY	-
ANY	VALIDITY_INVALID	INVALID

Table 47: Analog, Step Position and Bitstring Points Conversion Internal to IEC 60870-5-104

Internal Points -> IEC 60870-5-104 Counters		
Internal Quality		
Flags	VALIDITY	IEC 60870-5-104 Quality
FLAG_RESTART	ANY	-
FLAG_COMM_FAIL	ANY	-
FLAG_REMOTE_SUBSTITUTED	ANY	-
FLAG_LOCAL_SUBSTITUTED	ANY	-
FLAG_FILTER	ANY	-
FLAG_OVERFLOW	ANY	OVERFLOW
FLAG_REFERENCE_ERROR	ANY	-
FLAG_INCONSISTENT	ANY	-
FLAG_OUT_OF_RANGE	ANY	-
FLAG_INACCURATE	ANY	-
FLAG_OLD_DATA	ANY	-
FLAG_FAILURE	ANY	INVALID
FLAG_OPERATOR_BLOCKED	ANY	-
FLAG_TEST	ANY	-
ANY	VALIDITY_INVALID	INVALID

Table 48: Counters Conversion Internal to IEC 60870-5-104

5.2.4.1.3. MODBUS Internal Quality

As the MODBUS standard don't specify quality types to each point, but for help on use of each point's communication diagnostic, MasterTool allows the quality variables mapping, through an internal own structure, to each MODBUS point. The table below describes the quality types that each MODBUS point can assume.

Resulting Quality	Resulting VALIDITY	Description
FLAG_RESTART	VALIDITY_INVALID	Initial value. The point was never updated.
-	VALIDITY_GOOD	Communication OK. The point is updated.
FLAG_COMM_FAIL AND FLAG_RESTART	VALIDITY_INVALID	Communication error. The point never was updated.
FLAG_COMM_FAIL AND FLAG_OLD_DATA	VALIDITY_QUESTIONABLE	An error has occurred but the point was updated and now has an old value.
FLAG_FAILURE AND FLAG_RESTART	VALIDITY_INVALID	It has received an exception response and the point kept its initial value.
FLAG_FAILURE AND FLAG_OLD_DATA	VALIDITY_QUESTIONABLE	It has received an exception response, but the point has a valid old value.
FLAG_RESTART AND FLAG_OLD_DATA	VALIDITY_QUESTIONABLE	Device stopped. The point has an old value.

Table 49: MODBUS Quality

4. INITIAL PROGRAMMING

5.2.4.1.4. Local Bus I/O Modules Quality

To help in the use of each I/O point's diagnostic, MasterTool automatically creates a quality structure to each local bus module used on the PLC project, through an own internal structure accessible by structure QUALITY, available in GVL IOQualities.

The table below describes the quality types to each input and output point.

For further information look at [GVL IOQualities](#).

Diagnostics	Resulting Quality	Resulting VALIDITY	Description
Don't care	FLAG_RESTART	VALIDITY_INVALID	The quality has this value before have been read or written for the first time.
None	-	VALIDITY_GOOD	Communication OK. The point is updated.
None	FLAG_OLD_DATA AND FLAG_FAILURE	VALIDITY_QUESTIONABLE	Non-operational module. However, the data have been read or written at least once.
bOverRange OR bUnderRange	FLAG_OUT_OF_RANGE	VALIDITY_INVALID	The value is above or below the module's input allowed range.
bInputNotEnable OR bOutputNotEnable	FLAG_OPERATOR_BLOCKED	VALIDITY_INVALID	Input/Output not enable.
bOpenLoop	FLAG_FAILURE	VALIDITY_INVALID	Open loop in input module.
bFatalError	FLAG_FAILURE	VALIDITY_INVALID	Hardware fatal failure.
bNoExternalSupply	FLAG_FAILURE	VALIDITY_INVALID	External power supply is under operational minimum limit.
bShortCircuit OR bOutputShortCircuit	FLAG_FAILURE	VALIDITY_INVALID	Output short-circuit.
bCalibrationError	FLAG_INACCURATE	VALIDITY_INVALID	Calibration error.
bColdJunctionSensorError	FLAG_INACCURATE	VALIDITY_INVALID	Cold junction sensor error.

Table 50: I/O Modules Quality

5.2.4.1.5. PROFIBUS I/O Modules Quality

Different from local bus, MasterTool doesn't automatically create the PROFIBUS modules quality structures, and neither the PLC update such structures. Therefore the creation and cyclic update of PROFIBUS modules quality is user responsibility.

To help on the development of such applications, there are following practical examples, in ST language, for the main PROFIBUS modules (DI, DO, AI, AO), based on Nexto Serie's PROFIBUS slaves (NX5110). The user should feel encouraged to make any needed adaptation and change to fit to its application.

ATTENTION

For the routines, presented in sequence, correct functioning it is necessary to enable *Status in Diagnose* in the PROFIBUS slaves.

The development of PROFIBUS I/O modules quality points update routine must began from quality variables declaration and initialization, from a GVL:

```

VAR_GLOBAL
  QUALITY_PB_NX1005_I: LibDataTypes.QUALITY:= (VALIDITY:= VALIDITY_INVALID,
    FLAGS:= (FLAG_RESTART:= TRUE));
  QUALITY_PB_NX1005_O: LibDataTypes.QUALITY:= (VALIDITY:= VALIDITY_INVALID,
    FLAGS:= (FLAG_RESTART:= TRUE));
  QUALITY_PB_NX6000: LibDataTypes.QUALITY:= (VALIDITY:= VALIDITY_INVALID,
    FLAGS:= (FLAG_RESTART:= TRUE));
  QUALITY_PB_NX6100: LibDataTypes.QUALITY:= (VALIDITY:= VALIDITY_INVALID,
    FLAGS:= (FLAG_RESTART:= TRUE));
END_VAR

```

5.2.4.1.6. PROFIBUS Digital Inputs Quality

```
// PROFIBUS digital input quality update, module NX1005

// In communication success case with PROFIBUS slave (address = 99) ...
IF DG_NX5001.tMstStatus.abvSlv_State.bSlave_99 = TRUE THEN
  // Waits the PROFIBUS slave become apt to exchange data and diagnostics
  // (It is necessary to wait, avoiding invalid quality generation)
  IF DG_NX5110.tPbusHeadA.tStatus1.bStation_Non_Existent = FALSE AND
    DG_NX5110.tPbusHeadA.tStatus1.bStation_Not_Ready = FALSE AND
    DG_NX5110.tPbusHeadA.wIdentNumber > 0 THEN
    QUALITY_PB_NX1005_I.FLAGS.FLAG_COMM_FAIL:= FALSE;
    // If there is a module present on the bus (slot = 2) and
    // if there is no modules config problem (general) and
    // if there is no config problem in that module (specific) and
    // if there is no fatal error identification by the module ...
    IF (DG_NX5110.tPbusHeadA.dwModuleNotPresent AND SHL(1, 2)) = 0 AND
      DG_NX5110.tPbusHeadA.tSummarized.bConfigMismatch = FALSE AND
      DG_NX1005_24_Vdc_8_DO_Trans_8_DI.tGeneral.bConfigMismatch = FALSE AND
      DG_NX1005_24_Vdc_8_DO_Trans_8_DI.tGeneral.bFatalError = FALSE THEN
      QUALITY_PB_NX1005_I.VALIDITY:= VALIDITY_GOOD;
      QUALITY_PB_NX1005_I.FLAGS.FLAG_RESTART:= FALSE;
      QUALITY_PB_NX1005_I.FLAGS.FLAG_FAILURE:= FALSE;
      QUALITY_PB_NX1005_I.FLAGS.FLAG_OLD_DATA:= FALSE;
    ELSE
      QUALITY_PB_NX1005_I.VALIDITY:= VALIDITY_INVALID;
      QUALITY_PB_NX1005_I.FLAGS.FLAG_FAILURE:= TRUE;
      // If the point have ever been updated once ...
      IF NOT QUALITY_PB_NX1005_I.FLAGS.FLAG_RESTART THEN
        QUALITY_PB_NX1005_I.FLAGS.FLAG_OLD_DATA:= TRUE;
      END_IF
    END_IF
  END_IF
// In PROFIBUS communication failure with the PROFIBUS slave ...
ELSE
  QUALITY_PB_NX1005_I.VALIDITY:= VALIDITY_INVALID;
  QUALITY_PB_NX1005_I.FLAGS.FLAG_COMM_FAIL:= TRUE;
  QUALITY_PB_NX1005_I.FLAGS.FLAG_FAILURE:= FALSE;
  // If the point have ever been updated once ...
  IF NOT QUALITY_PB_NX1005_I.FLAGS.FLAG_RESTART THEN
    QUALITY_PB_NX1005_I.FLAGS.FLAG_OLD_DATA:= TRUE;
  END_IF
END_IF
```

5.2.4.1.7. PROFIBUS Digital Output Quality

```
// PROFIBUS digital output quality update, module NX1005

// In communication success case with PROFIBUS slave (address = 99) ...
IF DG_NX5001.tMstStatus.abvSlv_State.bSlave_99 = TRUE THEN
  // Waits the PROFIBUS slave become apt to exchange data and diagnostics
  // (It is necessary to wait, avoiding invalid quality generation)
```

4. INITIAL PROGRAMMING

```
IF DG_NX5110.tPbusHeadA.tStatus1.bStation_Non_Existent = FALSE AND
  DG_NX5110.tPbusHeadA.tStatus1.bStation_Not_Ready = FALSE AND
  DG_NX5110.tPbusHeadA.wIdentNumber > 0 THEN
QUALITY_PB_NX1005_O.FLAGS.FLAG_COMM_FAIL:= FALSE;
// If there is a module present on the bus (slot = 2) and
// if there is no modules config problem (general) and
// if there is no config problem in that module (specific) and
// if there is no fatal error identification by the module and
// if there is no outputs short circuit indication and
// if there is no external power supply missing indication ...
IF (DG_NX5110.tPbusHeadA.dwModuleNotPresent AND SHL(1, 2)) = 0 AND
  DG_NX5110.tPbusHeadA.tSummarized.bConfigMismatch = FALSE AND
  DG_NX1005_24_Vdc_8_DO_Trans_8_DI.tGeneral.bConfigMismatch = FALSE AND
  DG_NX1005_24_Vdc_8_DO_Trans_8_DI.tGeneral.bFatalError = FALSE AND
  DG_NX1005_24_Vdc_8_DO_Trans_8_DI.tDetailed.bOutputShortCircuit = FALSE AND
  DG_NX1005_24_Vdc_8_DO_Trans_8_DI.tDetailed.bNoExternalSupply = FALSE THEN
  QUALITY_PB_NX1005_O.VALIDITY:= VALIDITY_GOOD;
  QUALITY_PB_NX1005_O.FLAGS.FLAG_RESTART:= FALSE;
  QUALITY_PB_NX1005_O.FLAGS.FLAG_FAILURE:= FALSE;
  QUALITY_PB_NX1005_O.FLAGS.FLAG_OLD_DATA:= FALSE;
ELSE
  QUALITY_PB_NX1005_O.VALIDITY:= VALIDITY_INVALID;
  QUALITY_PB_NX1005_O.FLAGS.FLAG_FAILURE:= TRUE;
  // If the point have ever been updated once ...
  IF NOT QUALITY_PB_NX1005_O.FLAGS.FLAG_RESTART THEN
    QUALITY_PB_NX1005_O.FLAGS.FLAG_OLD_DATA:= TRUE;
  END_IF
END_IF
// In PROFIBUS communication failure with the PROFIBUS slave ...
ELSE
QUALITY_PB_NX1005_O.VALIDITY:= VALIDITY_INVALID;
QUALITY_PB_NX1005_O.FLAGS.FLAG_COMM_FAIL:= TRUE;
QUALITY_PB_NX1005_O.FLAGS.FLAG_FAILURE:= FALSE;
// If the point have ever been updated once ...
IF NOT QUALITY_PB_NX1005_O.FLAGS.FLAG_RESTART THEN
  QUALITY_PB_NX1005_O.FLAGS.FLAG_OLD_DATA:= TRUE;
END_IF
END_IF
```

5.2.4.1.8. PROFIBUS Analog Inputs Quality

```
// PROFIBUS analog input quality update, module NX6000

// In communication success case with PROFIBUS slave (address = 99) ...
IF DG_NX5001.tMstStatus.abvSlv_State.bSlave_99 = TRUE THEN
// Waits the PROFIBUS slave become apt to exchange data and diagnostics
// (It is necessary to wait, avoiding invalid quality generation)
IF DG_NX5110.tPbusHeadA.tStatus1.bStation_Non_Existent = FALSE AND
  DG_NX5110.tPbusHeadA.tStatus1.bStation_Not_Ready = FALSE AND
  DG_NX5110.tPbusHeadA.wIdentNumber > 0 THEN
QUALITY_PB_NX6000.FLAGS.FLAG_COMM_FAIL:= FALSE;
```

4. INITIAL PROGRAMMING

```
// If there is a module present on the bus (slot = 3) and
// if there is no modules config problem (general) and
// if there is no config problem in that module (specific) and
// if there is no fatal error identification by the module and
// if there is no calibration error indication and
// if there is no over/under range error indication and
// if there is no error indication of input in open loop ...
IF (DG_NX5110.tPbusHeadA.dwModuleNotPresent AND SHL(1, 3)) = 0 AND
  DG_NX5110.tPbusHeadA.tSummarized.bConfigMismatch = FALSE AND
  DG_NX6000_8_AI_Voltage_Current.tGeneral.bConfigMismatch = FALSE AND
  DG_NX6000_8_AI_Voltage_Current.tGeneral.bFatalError = FALSE AND
  DG_NX6000_8_AI_Voltage_Current.tGeneral.bCalibrationError = FALSE AND
  DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bOverRange = FALSE
  AND
  DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bUnderRange = FALSE
  AND
  DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bOpenLoop = FALSE
THEN
  QUALITY_PB_NX6000.VALIDITY:= VALIDITY_GOOD;
  QUALITY_PB_NX6000.FLAGS.FLAG_RESTART:= FALSE;
  QUALITY_PB_NX6000.FLAGS.FLAG_FAILURE:= FALSE;
  QUALITY_PB_NX6000.FLAGS.FLAG_OLD_DATA:= FALSE;
  QUALITY_PB_NX6000.FLAGS.FLAG_INACCURATE:= FALSE;
  QUALITY_PB_NX6000.FLAGS.FLAG_OUT_OF_RANGE:= FALSE;
ELSE
  // Condition to turns on imprecision indication
  // (check first, because invalid validity must prevail)
  IF DG_NX6000_8_AI_Voltage_Current.tGeneral.bCalibrationError = TRUE THEN
    QUALITY_PB_NX6000.VALIDITY:= VALIDITY_QUESTIONABLE;
    QUALITY_PB_NX6000.FLAGS.FLAG_INACCURATE:= TRUE;
  ELSE
    QUALITY_PB_NX6000.FLAGS.FLAG_INACCURATE:= FALSE;
  END_IF
  // Condition to turns on out of range indication
  // (check first, because invalid validity must prevail)
  IF DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bOverRange =
  TRUE OR
  DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bUnderRange =
  TRUE THEN
    QUALITY_PB_NX6000.VALIDITY:= VALIDITY_QUESTIONABLE;
    QUALITY_PB_NX6000.FLAGS.FLAG_OUT_OF_RANGE:= TRUE;
  ELSE
    QUALITY_PB_NX6000.FLAGS.FLAG_OUT_OF_RANGE:= FALSE;
  END_IF
  // Condition to turns on general failure indication (priority)
  IF (DG_NX5110.tPbusHeadA.dwModuleNotPresent AND SHL(1, 3)) > 0 OR
    DG_NX5110.tPbusHeadA.tSummarized.bConfigMismatch = TRUE OR
    DG_NX6000_8_AI_Voltage_Current.tGeneral.bConfigMismatch = TRUE OR
    DG_NX6000_8_AI_Voltage_Current.tGeneral.bFatalError = TRUE OR
    DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bOpenLoop = TRUE
  THEN
    QUALITY_PB_NX6000.VALIDITY:= VALIDITY_INVALID;
    QUALITY_PB_NX6000.FLAGS.FLAG_FAILURE:= TRUE;
    // If the point have ever been updated once ...
    IF NOT QUALITY_PB_NX6000.FLAGS.FLAG_RESTART AND
```

4. INITIAL PROGRAMMING

```
    NOT DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bOpenLoop
  THEN
    QUALITY_PB_NX6000.FLAGS.FLAG_OLD_DATA:= TRUE;
  END_IF
  ELSE
    QUALITY_PB_NX6000.FLAGS.FLAG_RESTART:= FALSE;
    QUALITY_PB_NX6000.FLAGS.FLAG_FAILURE:= FALSE;
    QUALITY_PB_NX6000.FLAGS.FLAG_OLD_DATA:= FALSE;
  END_IF
END_IF
END_IF
// In PROFIBUS communication failure with the PROFIBUS slave ...
ELSE
  QUALITY_PB_NX6000.VALIDITY:= VALIDITY_INVALID;
  QUALITY_PB_NX6000.FLAGS.FLAG_COMM_FAIL:= TRUE;
  QUALITY_PB_NX6000.FLAGS.FLAG_FAILURE:= FALSE;
  // If the point have ever been updated once ...
  IF NOT QUALITY_PB_NX6000.FLAGS.FLAG_RESTART AND
    NOT DG_NX6000_8_AI_Voltage_Current.tDetailed.tAnalogInput_00.bOpenLoop THEN
    QUALITY_PB_NX6000.FLAGS.FLAG_OLD_DATA:= TRUE;
  END_IF
END_IF
```

5.2.4.1.9. PROFIBUS Analog Output Quality

```
// PROFIBUS analog output quality update, module NX6100

// In communication success case with PROFIBUS slave (address = 99) ...
IF DG_NX5001.tMstStatus.abvSlv_State.bSlave_99 = TRUE THEN
  // Waits the PROFIBUS slave become apt to exchange data and diagnostics
  // (It is necessary to wait, avoiding invalid quality generation)
  IF DG_NX5110.tPbusHeadA.tStatus1.bStation_Non_Existent = FALSE AND
    DG_NX5110.tPbusHeadA.tStatus1.bStation_Not_Ready = FALSE AND
    DG_NX5110.tPbusHeadA.wIdentNumber > 0 THEN
  QUALITY_PB_NX6100.FLAGS.FLAG_COMM_FAIL:= FALSE;
  // If there is a module present on the bus (slot = 4) and
  // if there is no modules config problem (general) and
  // if there is no config problem in that module (specific) and
  // if there is no fatal error identification by the module and
  // if there is no calibration error indication and
  // if there is no external power supply missing indication and
  // if there is no error indication of output in open loop and
  // if there is no outputs short circuit indication ...
  IF (DG_NX5110.tPbusHeadA.dwModuleNotPresent AND SHL(1, 4)) = 0 AND
    DG_NX5110.tPbusHeadA.tSummarized.bConfigMismatch = FALSE AND
    DG_NX6100_4_AO_Voltage_Current.tGeneral.bConfigMismatch = FALSE AND
    DG_NX6100_4_AO_Voltage_Current.tGeneral.bFatalError = FALSE AND
    DG_NX6100_4_AO_Voltage_Current.tGeneral.bCalibrationError = FALSE AND
    DG_NX6100_4_AO_Voltage_Current.tGeneral.bNoExternalSupply = FALSE AND
    DG_NX6100_4_AO_Voltage_Current.tDetailed.tAnalogOutput_00.bOpenLoop = FALSE
  AND
```

4. INITIAL PROGRAMMING

```
DG_NX6100_4_AO_Voltage_Current.tDetailed.tAnalogOutput_00.bShortCircuit =
FALSE THEN
    QUALITY_PB_NX6100.VALIDITY:= VALIDITY_GOOD;
    QUALITY_PB_NX6100.FLAGS.FLAG_RESTART:= FALSE;
    QUALITY_PB_NX6100.FLAGS.FLAG_FAILURE:= FALSE;
    QUALITY_PB_NX6100.FLAGS.FLAG_INACCURATE:= FALSE;
    QUALITY_PB_NX6100.FLAGS.FLAG_OLD_DATA:= FALSE;
ELSE
    // Condition to turns on imprecision indication
    // (check first, because invalid validity must prevail)
    IF DG_NX6100_4_AO_Voltage_Current.tGeneral.bCalibrationError = TRUE THEN
        QUALITY_PB_NX6100.VALIDITY:= VALIDITY_QUESTIONABLE;
        QUALITY_PB_NX6100.FLAGS.FLAG_INACCURATE:= TRUE;
    ELSE
        QUALITY_PB_NX6100.FLAGS.FLAG_INACCURATE:= FALSE;
    END_IF
    // Condition to turns on general failure indication (priority)
    IF (DG_NX5110.tPbusHeadA.dwModuleNotPresent AND SHL(1, 4)) > 0 OR
        DG_NX5110.tPbusHeadA.tSummarized.bConfigMismatch = TRUE OR
        DG_NX6100_4_AO_Voltage_Current.tGeneral.bConfigMismatch = TRUE OR
        DG_NX6100_4_AO_Voltage_Current.tGeneral.bFatalError = TRUE OR
        DG_NX6100_4_AO_Voltage_Current.tGeneral.bNoExternalSupply = TRUE OR
        DG_NX6100_4_AO_Voltage_Current.tDetailed.tAnalogOutput_00.bOpenLoop = TRUE
    OR
        DG_NX6100_4_AO_Voltage_Current.tDetailed.tAnalogOutput_00.bShortCircuit =
    TRUE THEN
        QUALITY_PB_NX6100.VALIDITY:= VALIDITY_INVALID;
        QUALITY_PB_NX6100.FLAGS.FLAG_FAILURE:= TRUE;
        // If the point have ever been updated once ...
        IF NOT QUALITY_PB_NX6100.FLAGS.FLAG_RESTART AND NOT
            DG_NX6100_4_AO_Voltage_Current.tDetailed.tAnalogOutput_00.bOpenLoop
        THEN
            QUALITY_PB_NX6100.FLAGS.FLAG_OLD_DATA:= TRUE;
        END_IF
    ELSE
        QUALITY_PB_NX6100.FLAGS.FLAG_RESTART:= FALSE;
        QUALITY_PB_NX6100.FLAGS.FLAG_FAILURE:= FALSE;
        QUALITY_PB_NX6100.FLAGS.FLAG_OLD_DATA:= FALSE;
    END_IF
END_IF
END_IF
// In PROFIBUS communication failure with the PROFIBUS slave ...
ELSE
    QUALITY_PB_NX6100.VALIDITY:= VALIDITY_INVALID;
    QUALITY_PB_NX6100.FLAGS.FLAG_COMM_FAIL:= TRUE;
    QUALITY_PB_NX6100.FLAGS.FLAG_FAILURE:= FALSE;
    // If the point have ever been updated once ...
    IF NOT QUALITY_PB_NX6100.FLAGS.FLAG_RESTART AND
        NOT DG_NX6100_4_AO_Voltage_Current.tDetailed.tAnalogOutput_00.bOpenLoop THEN
        QUALITY_PB_NX6100.FLAGS.FLAG_OLD_DATA:= TRUE;
    END_IF
END_IF
```

5.3. Serial Interfaces Configuration

5.3.1. COM 1

The COM 1 communication interface consists of the D+ and D- terminals, for the half-duplex RS-485 standard, allowing point-to-point or network communication in open protocols MODBUS RTU Slave or MODBUS RTU Master.

When using the MODBUS Master/Slave protocol, some of these parameters (such as *Serial Mode*, *Data Bits*, *RX Threshold*) are automatically adjusted by the MasterTool for the correct operation of this protocol.

Below, it follows the parameters that must be configured for the proper operation of the application.

Configuration	Description	Default	Options
Serial Type	Serial channel configuration.	RS-485	RS-485
Baud Rate	Serial communication port speed configuration.	115200	2400, 4800, 9600, 19200, 38400, 57600, 115200 bps
Parity	Serial port parity configuration.	None	Odd Even None
Data Bits	Sets the data bits quantity in each serial communication character.	8	7 and 8
Stop Bits	Sets the serial port stop bits.	1	1 and 2
Serial Mode	Sets the serial port operation mode.	Normal Mode	- Extended Mode: Extended operation mode which delivers information regarding the received data frame (see note on COM 1 section) - Normal Mode: Serial communication normal operation mode

Table 51: RS-485 Standard Serial Configurations

Notes:

Extended Mode: This serial communication operation mode provides information regarding the data frame received. The information available is the following:

- One byte for the received data (RX_CHAR : BYTE): Store the seven or eight bits from the data received, depending on the serial communication configuration.
- One byte for the signal errors (RX_ERROR : BYTE): It has the format described below:
 - Bit 0: 0 - the character in bits 0 to 7 is valid. 1 - the character in bits 0 to 7 is not valid (or it cannot be valid), due to problems indicated in bits 10 to 15.
 - Bit 1: Not used.
 - Bit 2: Not used.
 - Bit 3: UART interruption error. The serial input remained in logic 0 (space) for a time greater than a character (start bit + data bits + parity bit + stop bits).
 - Bit 4: UART frame error. The logic 0 (space) was read when the first stop bit was expected and it should be logic 1 (mark).
 - Bit 5: UART parity error. The parity bit read is not correct according to the calculated one.
 - Bit 6: UART overrun error. Data was lost during the FIFO UART reading. New characters were received before the later ones were removed. This error will only be indicated in the first character read after the overrun error indication. This means some old data were lost.
 - Bit 7: RX line overrun error. This character was written when the RX line was completed, overwriting the unread characters.

- Two bytes for the timestamp signal (RX_TIMESTAMP : DWORD): Indicates the silence time, within the 0 to 4.294.967.295 interval, using 1 us as base. It saturates in 4.294.967.295 us if the silence time is higher than 4.294.967.295 units. The RX_TIMESTAMP of a character measures the time from a reference which can be any of the three options below:
 - On most of the cases, the end of the later character.
 - Serial port configuration.
 - The end of serial communication using the SERIAL_TX_FB, in other words, when the last character is sent on line.

Besides measuring the silence between characters, the RX_TIMESTAMP is also important as it measures the silence time of the last character on the RX line. The silence measuring is important for the correct protocol implementation, as MODBUS RTU, for example. This protocol specifies an inter-frame greater than 3.5 characters and an inter-byte less than 1.5 characters.

Data Bits: The serial interfaces *Data Bits* configuration limits the *Stop Bits* and *Communication Parity* fields. Therefore, the stop bits number and the parity method will vary according to the data bits number.

Data Bits	Stop Bits	Parity
7	1, 2	NO PARITY, ODD, EVEN
8	1, 2	NO PARITY, ODD, EVEN

Table 52: Specific Configurations

5.3.1.1. Advanced Configurations

The advanced configurations are related to the serial communication control, in other words, when it is necessary the utilization of a more accurate data transmission and reception control.

Configuration	Description	Default	Options
UART RX Threshold	Bytes quantity which must be received for a new UART interruption to be generated. Low values make the TIMESTAMP more precise when the EXTENDED MODE is used and minimizes the overrun errors. However, values too low may cause several interruptions delaying the CPU.	8	1, 4, 8 and 14
RS-485 Termination	Enable termination RS-485 in the COM1.	Enabled	Enabled Disabled

Table 53: RS-485 Standard Serial Advanced Configurations

5.4. CAN Interface Configuration (Controller Area Network)

5.4.1. CAN

The CAN interface allows point to point or network communication with other devices that have this interface using CANopen application protocol.

The parameters of CAN interface which must be configured for the proper functioning of the application are described below:

Configuration	Description	Default	Options
Network	CAN interface ID number	0	0 (fixed)
Baud Rate	CAN bus baud rate (kbit/s). Other devices must use the same baud rate.	250	10, 20, 50, 100, 125, 250, 500, 1000

Table 54: CAN Configuration

The parameters related to CANopen protocol are described on [Protocols Configuration](#) section.

5.5. Management Tab Access

Developed to perform configuration and diagnostics access to some features. The *Management* tab of the System Web Page has its access protected by user and password, with *admin* as the default value for both fields.

On the Management tab, there are other resources such as *System*, *Network*, *SNMP*, *USB Device*, *Firewall*, *OpenVPN*, and *FTP Server*. The resources available on this tab vary according to the features available for the controller used and can only be accessed after the user has logged in, as shown in the figure below.

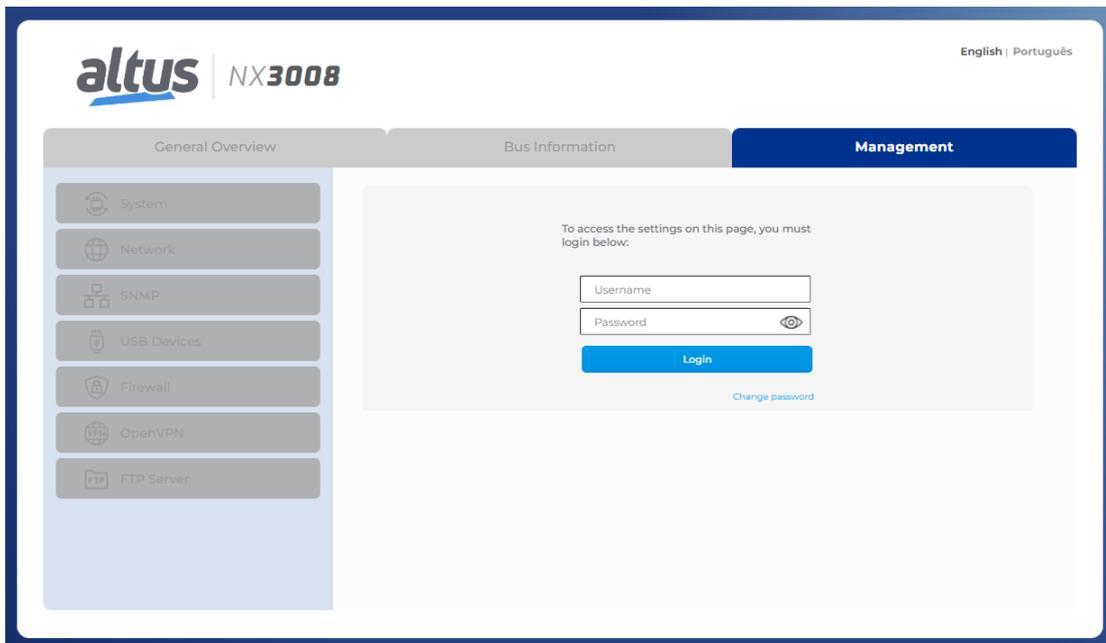


Figure 43: Management Tab Access

5.5.1. System Section

In the *System* section, you can perform a CPU firmware update. For cases in which the update is done remotely (through a radio or satellite connection, for example), the minimum speed of this link must be 128 kbps.

5.5.1.1. Clock Setting

On the System Web Page, it is possible to adjust the controller’s clock, which is found in the *System* section of the Management tab. The date and time format follows the ISO 8601 standard for date and time sampling (YYYY/MM/DD hh:mm:ss), as shown in the image below:

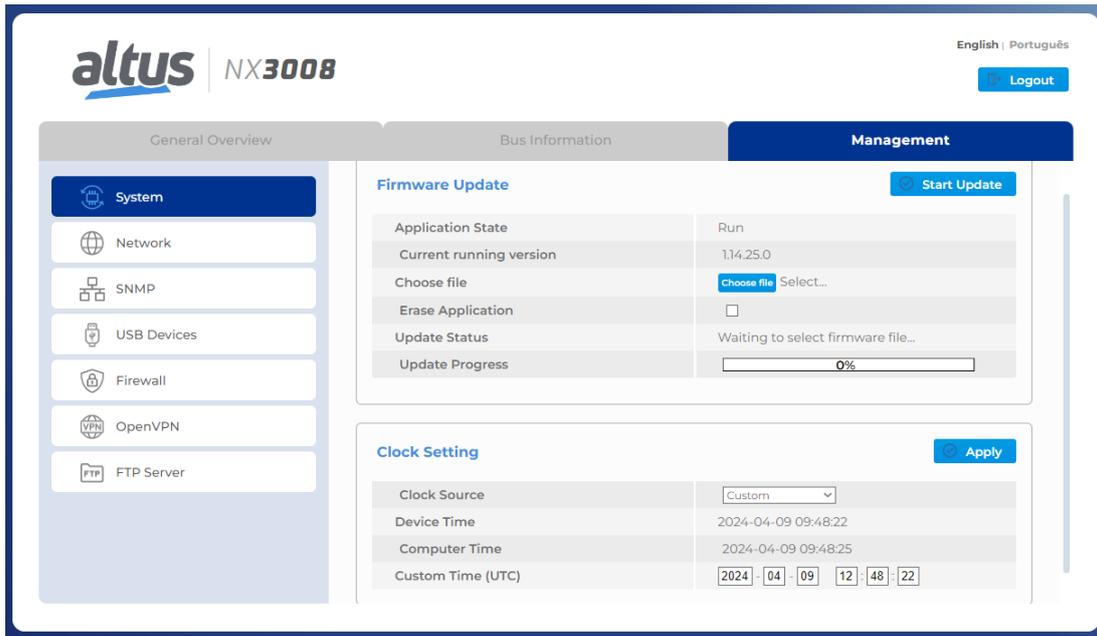


Figure 44: Clock Setting

This feature has two modes for adjusting the device’s time, which can be selected in the item “Clock Source”, providing the user with two options for synchronizing the clock.

5.5.1.1.1. *Computer Time (UTC)*

In computer time mode, user can apply the time configured on his computer in UTC for his device. To do so, select the option “Computer” in the “Clock Source” item. After clicking on the "Apply" button, it is necessary to validate the device’s credentials, then the CPU will receive the date and UTC time that are configured on the computer.

5.5.1.1.2. *Custom Time (UTC)*

In the custom time mode, the user can prepare a custom time in UTC standard to be applied to the device’s internal date and time. To do so, select the “Custom” option in the “Clock Source” item. With the mode selected, the user must configure the desired date and time in the “Custom Time (UTC)” item, which will be initialized with the browser’s local time. So, after the user clicks on the "Apply" button and validates the device’s credentials, it will have its internal time configured with the time configured in the item "Custom Time (UTC)". For configuration limits, refer to section [RTC Operating Limits](#).

5.5.2. **Network Section**

Designed to assist in the usability of the controller, the *Network* section (figure below) allows you to change network addresses and run the Network Sniffer.

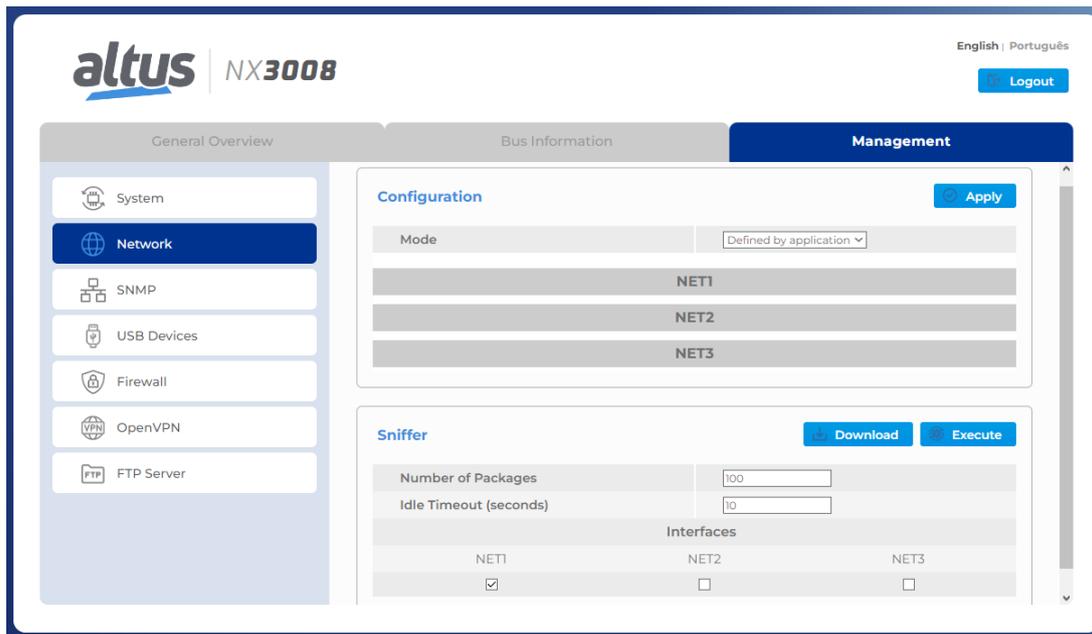


Figure 45: Network Section

5.5.2.1. Network Section Configurations

5.5.2.1.1. Defined by Application

The Mode field defines which configuration the controller should load for its interfaces. This field can be configured as *Defined By Web Page* or *Defined By Application*.

When set to *Defined by Application*, the interface table is disabled, not allowing changes, as shown in the figure below. In this mode, the settings applied to the controller are those defined by the application.

ATTENTION

The table for network configuration is displayed only when there is no application on the controller or the controller is not running. It is not possible to change the network settings while an application is running on the controller.

Below is an image with *Defined by Application* mode selected, showing the interface table disabled.

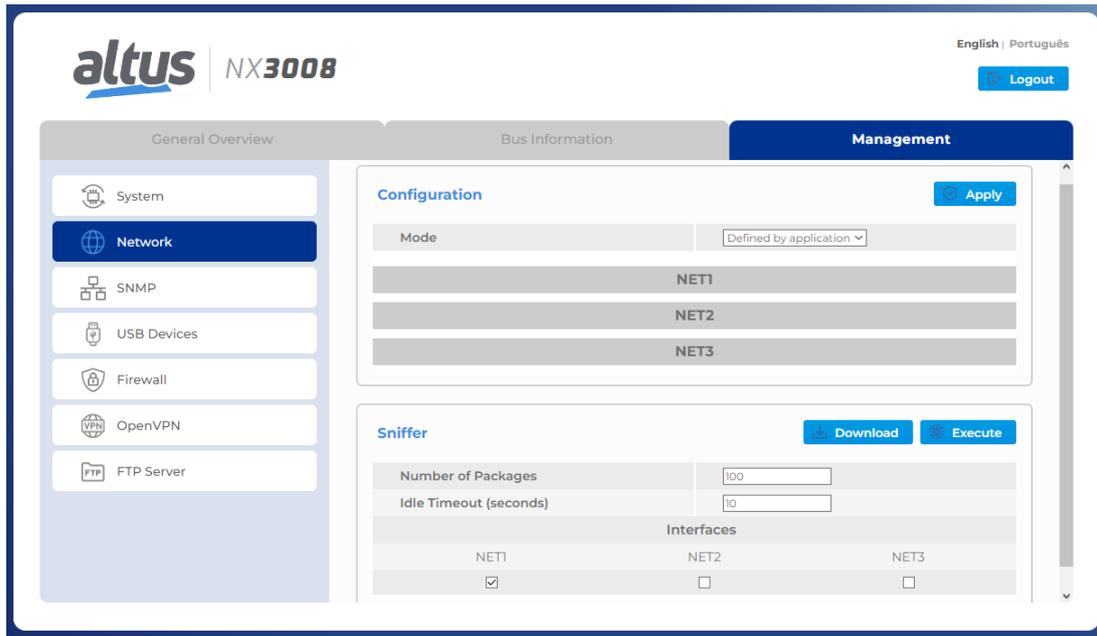


Figure 46: Interfaces Table - Application Mode

5.5.2.1.2. *Defined by web page*

For *Defined by Web Page* mode, the interface table remains enabled as shown in the figure below.

In this mode, the user can set the IP Address, Network Mask, and Gateway for each of the available Ethernet interfaces, as well as enabling and disabling NETs 2 and 3.

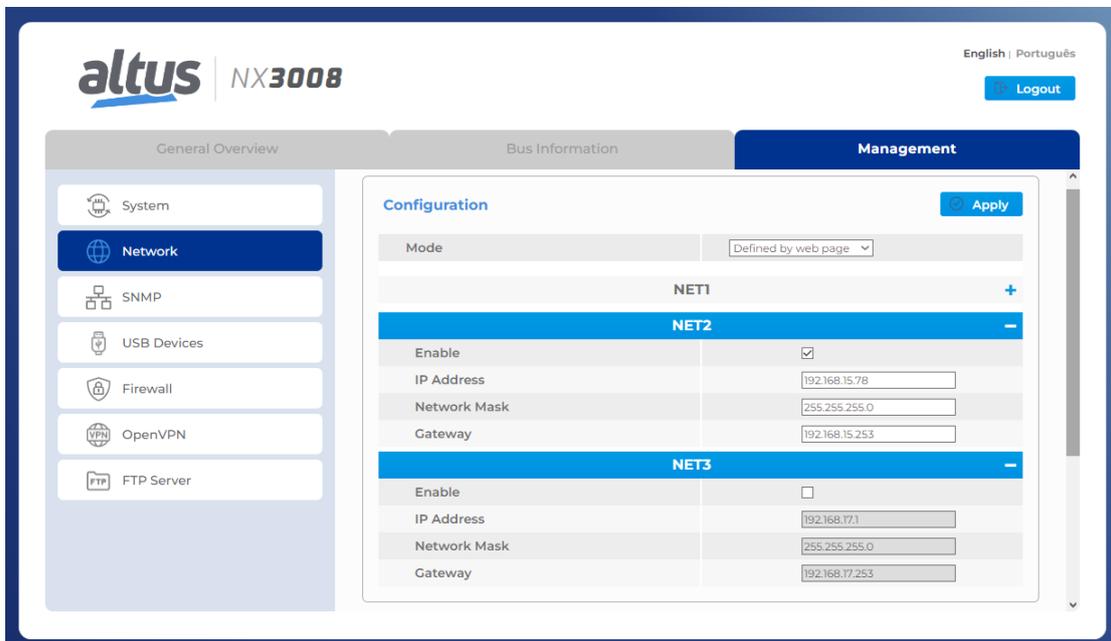


Figure 47: Interfaces Table - Web Mode

The *Enable* checkbox allows the user to enable and disable the Ethernet interfaces. This is only available to be checked or unchecked when the configuration is *Defined by web page*.

When this checkbox is unchecked, it indicates that the NET interface is disabled, i.e., it will not receive configuration and will be deactivated, as the NET 3 of the figure above. When the interface is enabled (with the checkbox checked), according to NET 2 in the figure above, the settings are available for editing.

4. INITIAL PROGRAMMING

To have the settings applied to the controller, simply click the *Apply* button. This process checks if there were any errors in the configuration made and, if so, displays a message on the browser screen indicating the error. If the settings are correct, after clicking *Apply*, a confirmation window appears in the browser to apply the new settings. By clicking *OK*, the settings are sent to the controller and applied.

ATTENTION

When making network changes in the controller, the interfaces will be restarted, which may cause a communication loss. Especially when changing the IP address value.

When applying settings using the *Defined by Application* mode, the controller will assume the configuration that was defined by the loaded application. If there is no application, the current configuration will be maintained, with only the configuration mode being changed.

Using the *Defined by Web Page* mode, the addresses indicated on the web page will be loaded.

ATTENTION

The *Defined by Web Page* mode configures the interfaces to operate in Simple Mode.

It is possible to monitor through MasterTool whether the IP address is configured from the Web Page or from the application by the *bNetDefinedByWeb* diagnostic BIT in the *Application* group, which will change to *TRUE* if the IP is configured from the Web Page and to *FALSE* if it is configured from the application.

Expression	Type	Value	Prepared value	Address	Comment
DG_NX3008	T_DIAG_NX3008_1			%QB20480	DG_NX3008 diagnostics variable
tSummarized	T_DIAG_SUMMARIZED			%QB20480	
tDetailed	T_DIAG_DETAILED			%QB20484	
Target	T_DIAG_TARGET			%QB20484	
Hardware	T_DIAG_HARDWARE			%QB20504	
Exception	T_DIAG_EXCEPTION			%QB20505	
WebVisualization	T_DIAG_WEBVISUALIZATION			%QB20508	
RetainInfo	T_DIAG_RETAIN_BASIC			%QB20509	
Reset	T_DIAG_RESET			%QB20520	
Thermometer	T_DIAG_THERMOMETER			%QB20521	
Serial	T_DIAG_SERIAL_SINGLE			%QB20530	
CAN	T_DIAG_CAN			%QB20580	
USB	T_DIAG_USB			%QB20619	
Ethernet	T_DIAG_ETHERNET			%QB20874	
UserFiles	T_DIAG_USERFILES			%QB21404	
UserLogs	T_DIAG_USERLOGS			%QB21414	
MemoryCard	T_DIAG_MEMCARD			%QB21420	
WHSB	T_DIAG_WHSB			%QB21430	
Application	T_DIAG_APP			%QB21689	
byCPUState	ENUM_APP_STATE	RUN		%QB21689	CPU operating state
bForcedIOs	BIT	FALSE		%QX21690.0	Forced IO points
bNetDefinedByWeb	BIT	TRUE		%QX21690.1	Net defined by Web
Rack	T_DIAG_RACK			%QB21691	
ApplicationInfo	T_DIAG_APP_INFO			%QB21705	
SNTP	T_DIAG_SNTP			%QB21717	
OpenVPN	T_DIAG_OPENVPN			%QB21743	
Firewall	T_DIAG_FIREWALL			%QB22159	
FTP	T_DIAG_FTP			%QB22170	

Figure 48: Diagnostics - IP defined by the Web Page

5.5.2.2. Network Sniffer

The network sniffer, shown in the figure below, can be used to observe traffic on physical interfaces, except for USB devices such as modems and wifi adapters. It has two basic settings:

Number of Packets: This is the number of packets you want to capture. The configured value of this parameter must be within the range of 100 to 25000 packets;

Idle Timeout (seconds): If there is no packet traffic on the interface after this configured timeout, the Sniffer execution is terminated. It can be configured with values between 1 and 3600 seconds.

Using the *Interfaces* table, you can select which interfaces you want the Sniffer to run on, i.e., perform network analysis. You can select all available interfaces and run them on all simultaneously. For disabled interfaces, it is not possible to run Sniffer. If the selected option is disabled, an error will be displayed in the browser.

Only a few moments after the screen opens will the *Execute* button, which starts Sniffer’s execution, become available. The *Download* button will only be unlocked if there is a Sniffer related file available for download. If the Sniffer has never been run or the file is deleted, the button will not be available.

When running the Network Sniffer, the page will disable the edit fields, the *Download* button will be locked, and the *Execute* button will become the *Stop* button, as shown in the figure below.



Figure 49: Network Sniffer Running

The *Stop* button can be used to end the sniffer execution at any time after it has been started.

For each of the interfaces on which Sniffer runs, it generates a **.pcap** file. These files are named according to the name of the controller and the interface that was analyzed, for example, **[PLC_MODEL]_capture.zip**. These files are found inside a **.zip** file, also named according to the name of the controller, for example, **[PLC_MODEL]_capture.zip**.

At the end of the sniffer execution, a message is displayed asking whether or not to automatically download the generated files. These files are stored in the *InternalMemory* folder of the *User Files Memory* and can be accessed through the controller’s programming software. The downloaded file is always in the **.zip** extension, which groups the other files.

If any problems occur related to insufficient memory due to the generation of sniffer files, it will be indicated to the user. It is recommended to try running the analyzer again with a smaller *Number of Packets* configuration.

The network sniffer can terminate its execution for three reasons: insufficient memory, idle time limit of interfaces exceeded, and manual cancellation.

5.6. USB Interface Configuration

The USB Host port present on Nexto Series controllers allows to extend the controller’s functionalities by using several types of USB dongles.

The management of USB devices is done through a dedicated section located on the *Management* tab of the controller’s System Web Page as shown below:

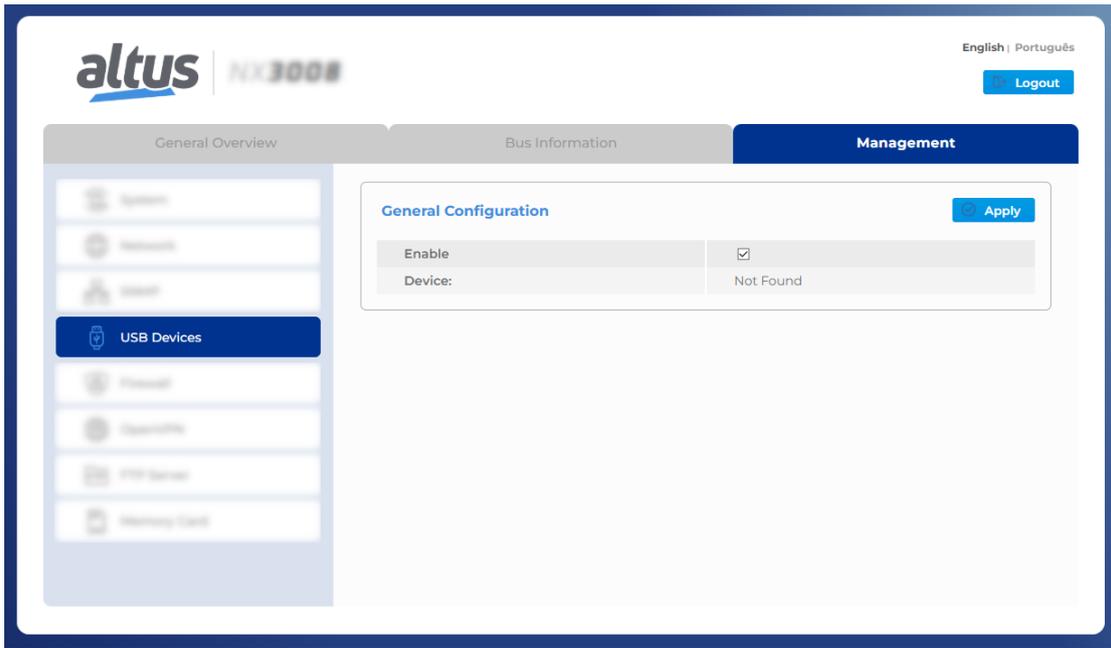


Figure 50: USB Devices Section

On this page, the USB interface’s state can be configured by marking or unmarking the checkbox and applying the configuration with the button Apply. If the USB interface is enabled, the content of this page changes dynamically according to the type of USB device that is connected. In the example above, the USB interface is enabled and there is no device connected. When USB is disabled, the content is the presented in the figure, always showing Device as "Not Found", but with the checkbox unmarked.

The following sections describe all the types of USB devices currently supported. If an unsupported device is connected, the page will inform that device is unknown:

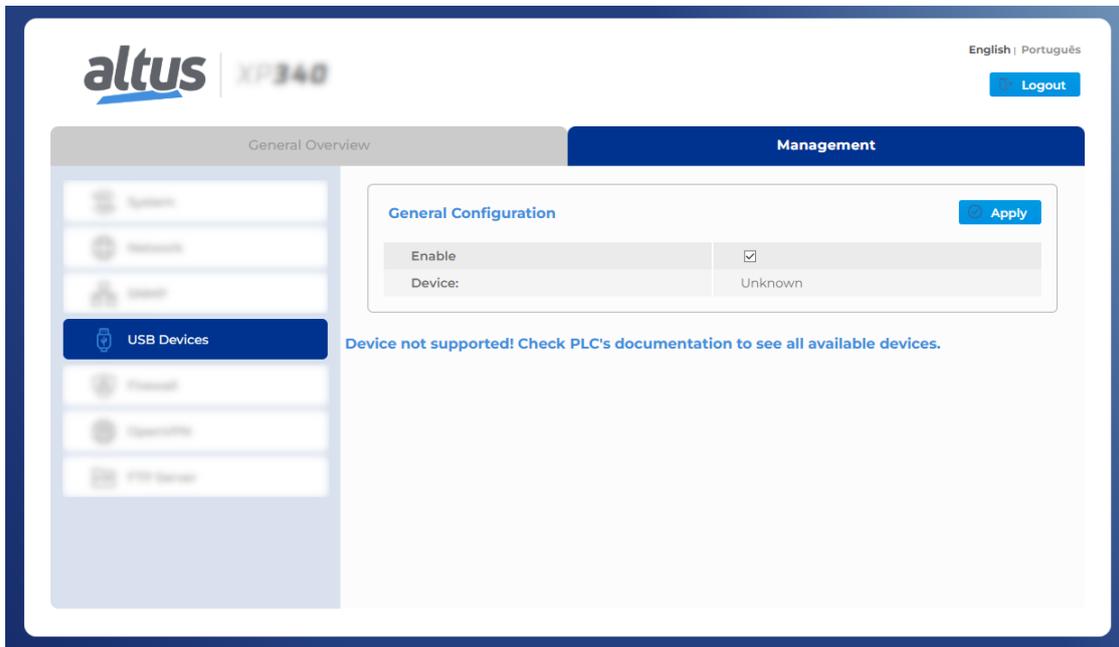


Figure 51: USB Devices - Unknown

5.6.1. Mass Storage Device

5.6.1.1. General Storage

Mass storage devices can be used to expand the controller’s flash memory to store big amount of data, like on datalogger applications, for instance. To use a USB mass storage device, simply connect it to the USB port. After a few seconds, when the device is properly detected and mounted, the USB LED will turn on and the device information will appear on section *USB Devices* located at the *Management* tab of the controller’s System Web Page as shown below:

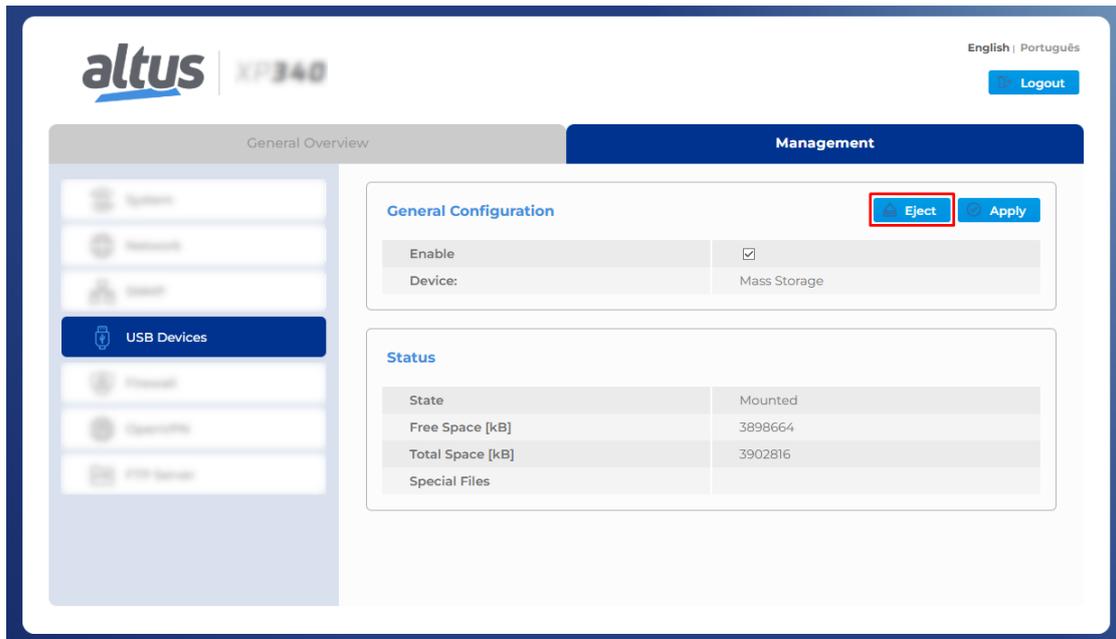


Figure 52: Mass Storage Device Information

The information shown on the status section of this page is also available in the symbolic variables diagnostics structure (see Section [Diagnostics via Variables](#)).

ATTENTION

The USB mass storage device must be formatted as a FAT32 volume. Other filesystem formats are not supported.

The device can be ejected using the command provided on the *Commands* area of this page as indicated on the picture above.

After the device is properly detected and mounted, a new folder called *Mass_Storage* will appear on the controller’s memory as shown on the picture below:

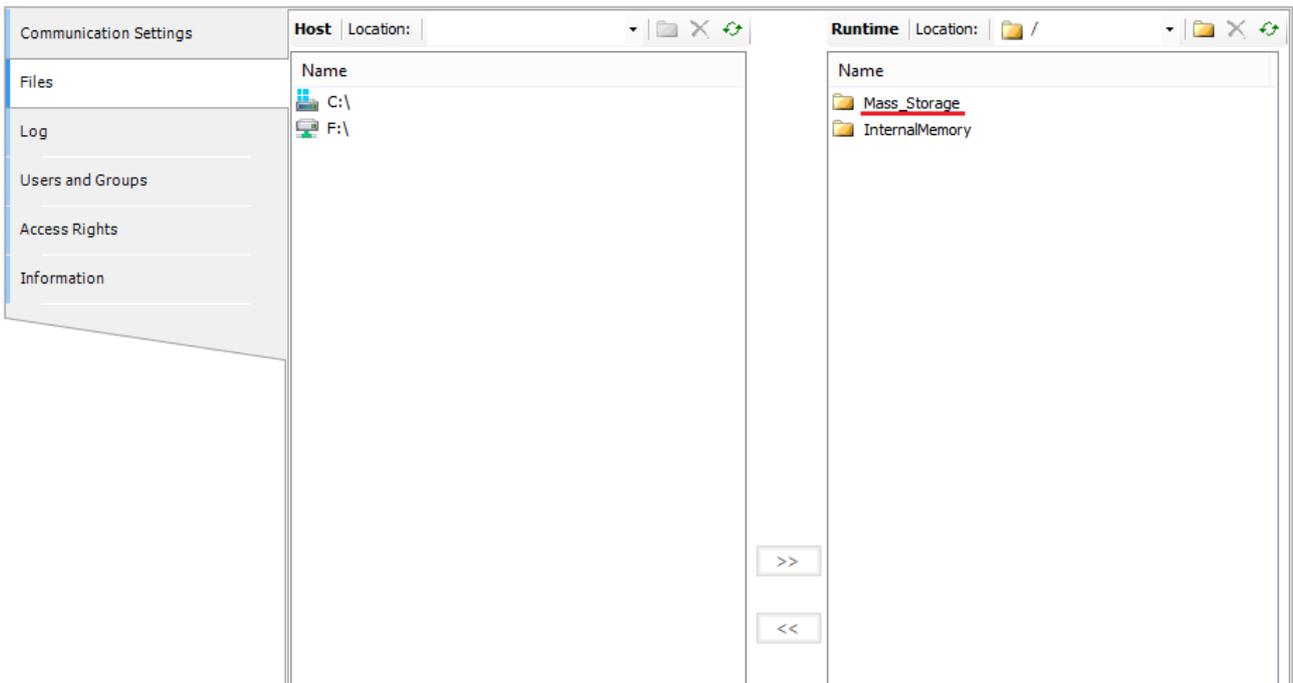


Figure 53: USB Mass Storage Folder

5.6.1.2. Application Not Loading on Startup

The USB mass storage device can be used to prevent the controller from automatically loading the application after the power on. To do that, simply place an empty text file called "dontbootapp.txt" on the root folder of mass storage device. The presence of this file is informed in the *Special Files* field on controller's System Web Page as shown below.

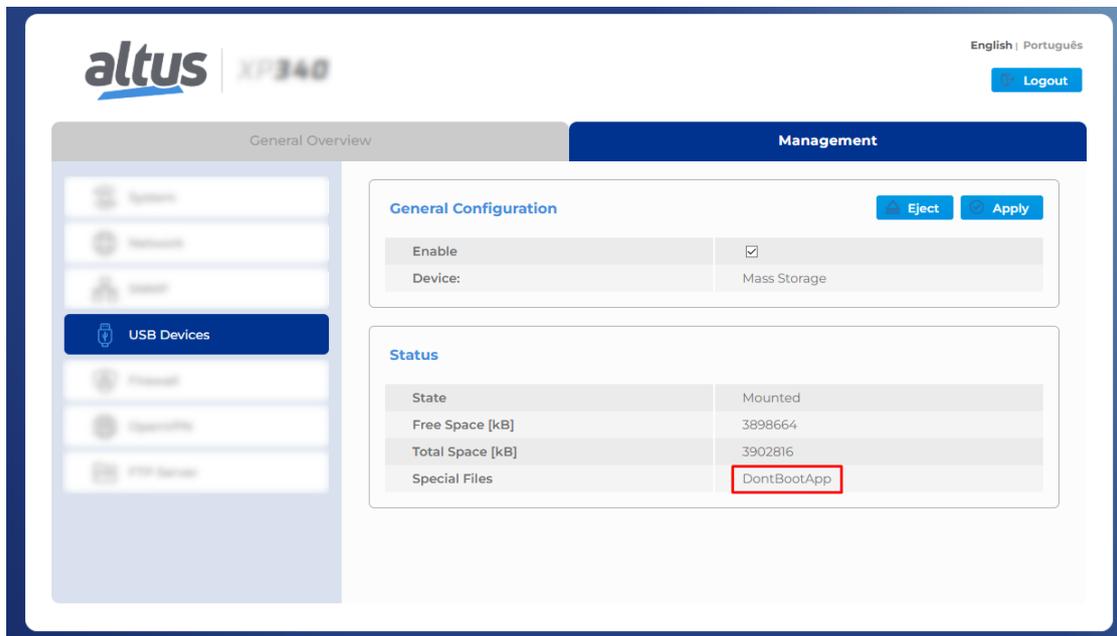


Figure 54: DontBootApp in the Mass Storage Device

5.6.1.3. Transferring an Application from a USB Device

The USB mass storage device can also be used to transfer an application to the controller. To do this, place the two files *Application.app* and *Application.crc* in the root folder of the mass storage device. If there is a WebVisu declared in the project, the folder *PLC Folder* must also be copied (these files are created using MasterTool IEC XE executing the command *Online -> Create boot application* when offline). After the power on, if the controller detects the presence of these files on the USB mass storage device, the following sequence of actions will occur:

- The controller will start copy of the application from USB device to internal memory
- After finishing the copy process, the USB device will be ejected (USB LED will turn off)
- The new application will start (RUN) automatically (if "*dontbootapp.txt*" is not present)

The presence of the application is informed in the *Special Files* field on controller’s System Web Page as shown below:

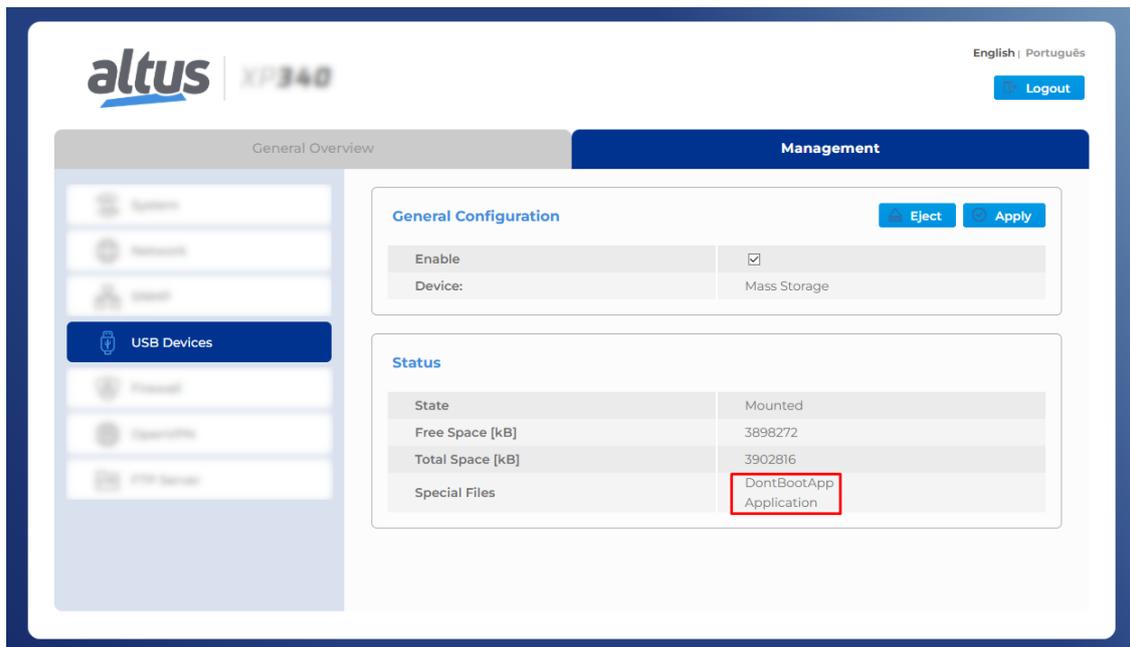


Figure 55: Application in the Mass Storage Device

Note that it is possible to have multiple *Special Files* in the same Mass Storage. In the example above, the PLC will transfer the new application to the internal memory but not load it on startup (hence, will not go to RUN).

5.6.2. USB to RS-232 Converter

The Nexto Series allows to implement a RS-232 port using a USB to Serial converter. These converters are based on an internal controller chip. The following table shows the list of supported controllers:

Controller	Manufacturer
FT232	FTDI
PL2303	Prolific

Table 55: Supported USB to RS-232 converters

This port is intended to be used exclusively with the Serial communication function blocks provided by the *NextoSerial* library, allowing to implement a point-to-point communication with equipments that use simple protocols (non time critical) like *Radio modems*, *Barcode readers*, *RFID readers*, etc... Additionally, this kind of solution has the following limitations:

- **Baud Rate:** values lower than 4800 bps are not supported
- **Data Bits:** value “5” is not supported (only 6, 7 or 8)

- **Parity:** values “mark” and “space” are not supported (only Odd, Even and None)
- **Stop Bits:** value “1.5” is not supported (only 1 or 2)

After plugging the converter into the USB port, and the device is detected and mounted correctly, the device information will appear in the *USB Devices* section, located in the *Management* tab of the controller’s System Web Page as shown below:

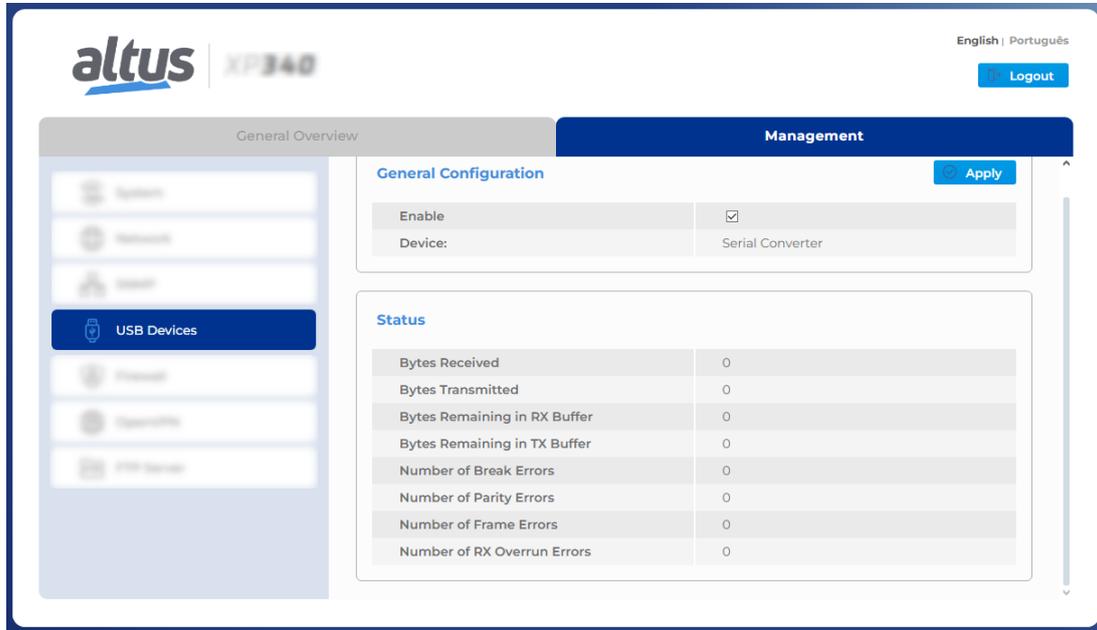


Figure 56: USB Devices - Serial Converter

The information shown on this page is also available in the symbolic variables diagnostics structure (see Section [Diagnostics via Variables](#)).

This additional serial port will be identified internally as *COM10*, and will not have a representation on the project treeview. From this point, this port can be used for communication using the *NextoSerial* functions similar to the native ports. For this kind of port, the handshake configuration is limited to *RS232_MANUAL* only (must be considered when configuring the port with *SERIAL_CFG* function).

5.6.3. Modem Devices

An USB Modem with a SIM chip can be used to connect the PLC to the internet using the cellular data network (telephone services, like sending SMS, are not implemented). This feature allows to use the NX3008 controller to implement telemetry and IoT applications. There are basically two types modems: bridge and router. The following table shows the list of supported devices.

Model	Manufacturer	Type	Remarks
E303	Huawei	Bridge	-
E3272	Huawei	Bridge	-
E3276	Huawei	Bridge	-
E8372	Huawei	Router	Redirection of the configuration web page (button <i>Open Modem Configuration</i>) is not supported for this model. In this case, the modem configuration must be done externally by plugging it directly on a PC.

Table 56: Supported USB modems

The bridge modem is a non-managed device that implements a direct connection (pass through) to the mobile data network, so all the connection requests coming from the internet will reach the controller’s operating system. For this kind of device, the configuration is performed through the controller’s system web page as described further on this section.

On the other hand, the router modem is a managed device that implements a firewall with configurable network policies. For this kind of device, all the configuration is performed through a proprietary web page that is embedded into the device. By default, the Modem blocks any kind of inbound connections (i.e, will not allow the remote access). To allow this, the user must configure the modem through the device embedded web page to open the TCP port related to the desired service (some manufacturers calls this feature as *Virtual Server* or *Port Forwarding*). The following table describes the number of the TCP port associated to the main services of the PLC.

Port	Service
80	Embedded system web page
8080	Embedded Webvisu web page
9000	Embedded Webvisu Portainer Docker
1217	MasterTool programming

Table 57: TCP ports of main PLC services

The management of the USB Modem functionality is done through the *USB Devices* section in the *Management* tab of the controller’s System Web Page. Once the Modem device is properly detected and mounted, the information will appear as shown below:

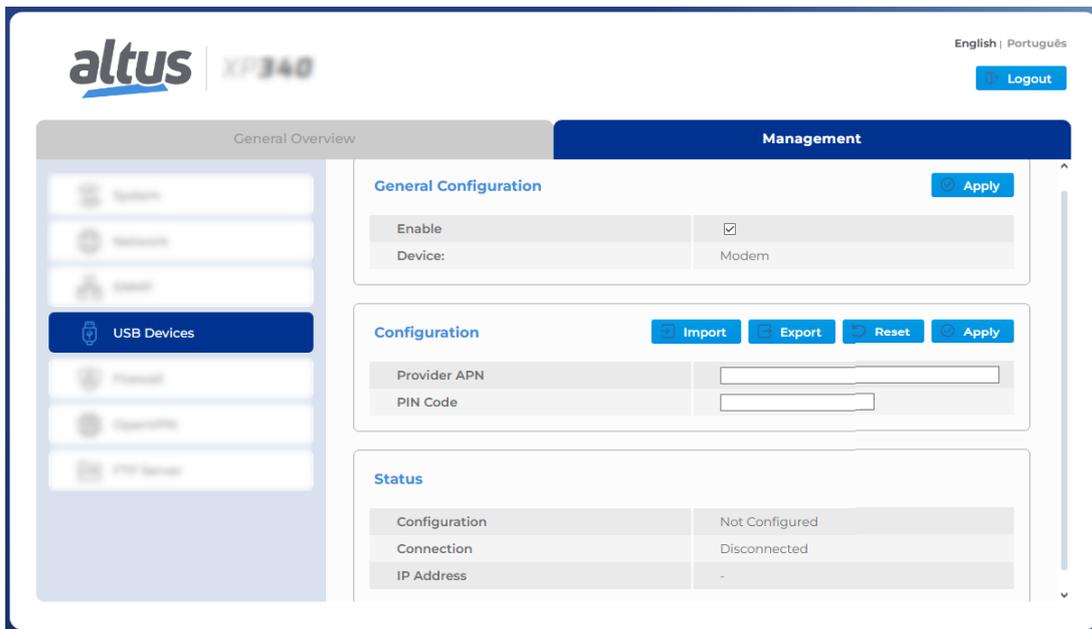


Figure 57: USB Modem Page Configuration

This area contains basically two sections: *Status* and *Configuration*.

The *Status* section is where all diagnostics related to the USB modem are displayed: configuration state (which does not depends on the device state), internet connection state and the modem IP address. These fields are updated automatically every time that a value is updated (does not require to reload the page manually). The same information is also provided on the symbolic variables diagnostics structure (see Section [Diagnostics via Variables](#)), which also contains the detailed description of the possible values for each field.

The *Configuration* section is where the user performs the modem configuration. For bridge modems, this section is used to enter the SIM chip information. For router modems, this section will show only a button called *Open Modem Configuration* that will redirect to the internal modem web page (check on the list of compatible devices if the redirection is supported, otherwise the modem must be configured externally on a PC). This section contains the following buttons:

- **Import:** loads the configuration from an external file
- **Export:** saves the current configuration on an external file
- **Reset:** erases the modem configuration from controller’s memory
- **Apply:** write the configuration on the controller’s memory

ATTENTION

The provider APN and PIN code fields are mandatory for every SIM chip. If the provider informs these parameters, they shall be used. In other hand, it's known that several SIM chips simply doesn't care for the content of these fields, using internal predefined values. In this case, these fields of the web page can be left with the default values and the connection will proceed successfully. Values like "zero" for PIN Code and "empty" for the Provider APN are not allowed.

The operation principle of USB Modem functionality is rather simple. For bridge devices, once the device is properly detected and the SIM parameters configured, the controller starts a background process, which continuously controls the modem to keep it connected to the internet. This eliminates the need of any kind of manual intervention, so if the connection is dropped for some reason (bad reception, carrier outage, etc.), the controller will try to reconnect automatically. The status of this process can be observed by the Connection *Status* field. For router modems, the device contains a similar process that runs internally (independent from the controller) that is called *Auto Connect*. It generally comes enabled by default, but can be disabled through the modem web page.

One important aspect to consider is that, if the USB Modem is configured, the controller system will set it as the default gateway for all Ethernet communication. It means that, if the controller is simultaneously connected to a local network (NET1), which has also access to the internet, all the Ethernet messages addressed to external IPs will route through the USB Modem (and not through NET1). NET1 returns as the default gateway when the USB Modem was removed.

The configuration and operation sequence can be summarized into the following steps:

- Plug the device into the USB port. After some seconds, the *USB Devices* page will show the *Device* as "Modem". If not, the device might be unsupported or defective.
- (For bridge devices) Set the SIM parameters (*Provider APN* - Access Point Name and the chip *PIN code*) as informed by the SIM chip provider. After clicking on *Apply* button, the connection process will start. Once configured, it is not necessary to set this information anymore. It will be saved on the controller's memory.
- Watch the connection status on the corresponding field. If everything goes fine, after some seconds it will inform that the modem is connected to the internet, and an IP address will appear in its field.

Once connected to the internet, this communication channel can be used for several purposes. One typical use case is to implement telemetry solution using MQTT Client Function Block to publish data. Another use case is to access the controller remotely. In this case, it is necessary to know the modem IP address on the internet. However, this address is dynamic and changes on every connection process. One way to workaround this problem is to publish the IP address (available on the modem diagnostic variables) through MQTT.

With the Modem IP address, it is possible to perform remote access to the controller's system web page to view status and diagnostics (firmware update is not supported). Also, it allows to program the controller remotely using MasterTool IEC XE. For this, the gateway must be configured with the Modem IP address like shown on the following picture:

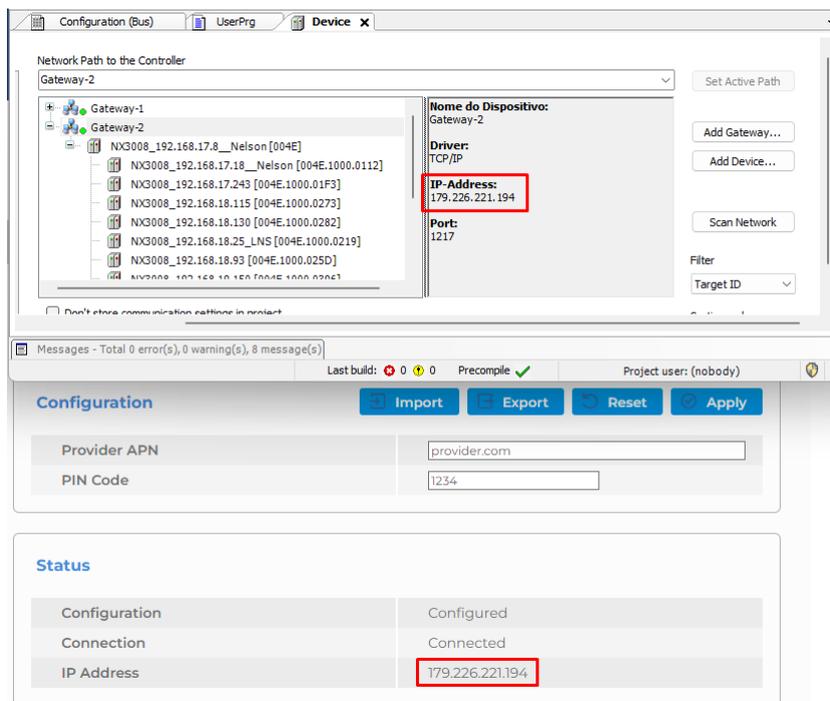


Figure 58: Configuring Gateway with Modem IP Address

ATTENTION

For bridge devices, or router devices with external access enabled (port forwarding), once connected to the internet, anyone who knows the modem IP address will be able to access the controller remotely. So, for security reasons, it is EXTREMELY important and recommended to configure the User Rights on the controller to restrict the online operations of MasterTool IEC XE with login and password.

5.6.4. WiFi Adapters

An USB WiFi adapter can be used to connect the PLC to an existing WiFi network, creating a second network adapter that can be used for programming and communication. The following table shows the list of supported chipsets.

Chipset	Manufacturer	Example of comercial products
RTL8188EU	Realtek	TP-LINK model TL-WN725N LM Technologies model LM007
RT28xx	Ralink/Mediatek	D-Link model DWA-125
AR9271	Atheros/Qualcomm	TP-LINK model TL-WN721N

Table 58: Supported chipsets for USB WiFi adapters

The management of the WiFi Adapter functionality is done through the *USB Devices* section in the *Management* tab of the controller's System Web Page. Once the WiFi adapter device is properly detected and mounted, the USB LED will turn on and the device information will appear as shown below:

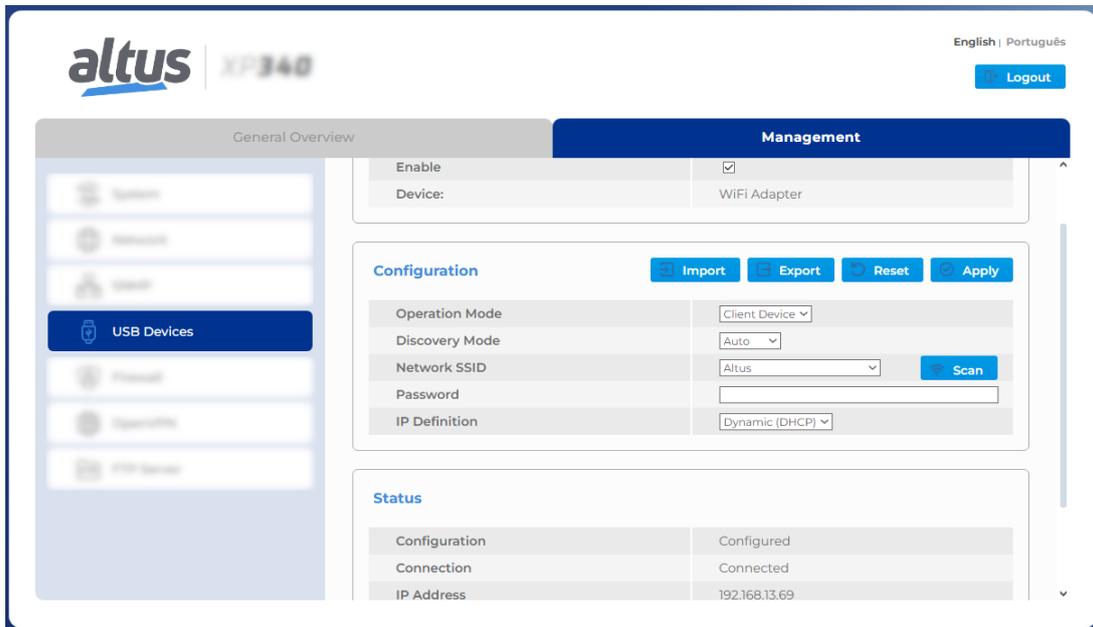


Figure 59: USB WiFi Adapter Page

This page contains basically two sections: *Status* and *Configuration*.

The *Status* section shows all diagnostics related to the WiFi adapter: configuration state, connection state, IP address, Netmask, Gateway and MAC address. These fields are updated as soon the values change. These informations are also provided in the symbolic variables diagnostics structure (see Section [Diagnostics via Variables](#)).

The *Configuration* section is composed by the following parameters:

- **Operation Mode:** defines how the WiFi adapter will operate (currently, only client mode is supported).

- **Discovery Mode:** defines what is the method to set the WiFi network. If selected as "Auto", the "Scan" button must be used to choose the wanted network. If selected as "Manual", the name of the SSID and Security Type must be entered manually.
- **Network SSID:** when discovery mode is set to "Auto", this field will show the available networks found on the scan process sorted from the best to the worst signal level (up to down). When discovery mode is set to "Manual" this field must be populated with the SSID of the wanted network.
- **Security Type:** this field is only available when the discovery mode is set to "Manual" (the "Auto" mode automatically selects the security type provided by the scanned network). This field defines the type of security used in the WiFi network, which can be "Public" or "WPA2-Personal".
- **Password:** this where you need to enter with the WiFi network password. The field will be automatically blocked if the Security Type is set as "Public" or the scanned network chosen does not use a security protocol.
- **IP Definition:** defines if the WiFi adapter will set the IP address dynamically (assigned by the network DHCP Server) or statically (where the user needs to enter the IP settings manually).
- **IP Address, Network Mask and Gateway:** only available when the IP definition is set as "Static". These fields will be used to configure the network parameters of the WiFi adapter.
- **Default Gateway:** this field defines what network interface will be used as a Gateway to access the Internet. It is possible to choose the "WiFi Adapter" or the "Local Ethernet" for this function.

ATTENTION

For proper operation, the WiFi adapter network (defined by IP and Mask) must be different from the one configured for NET1.

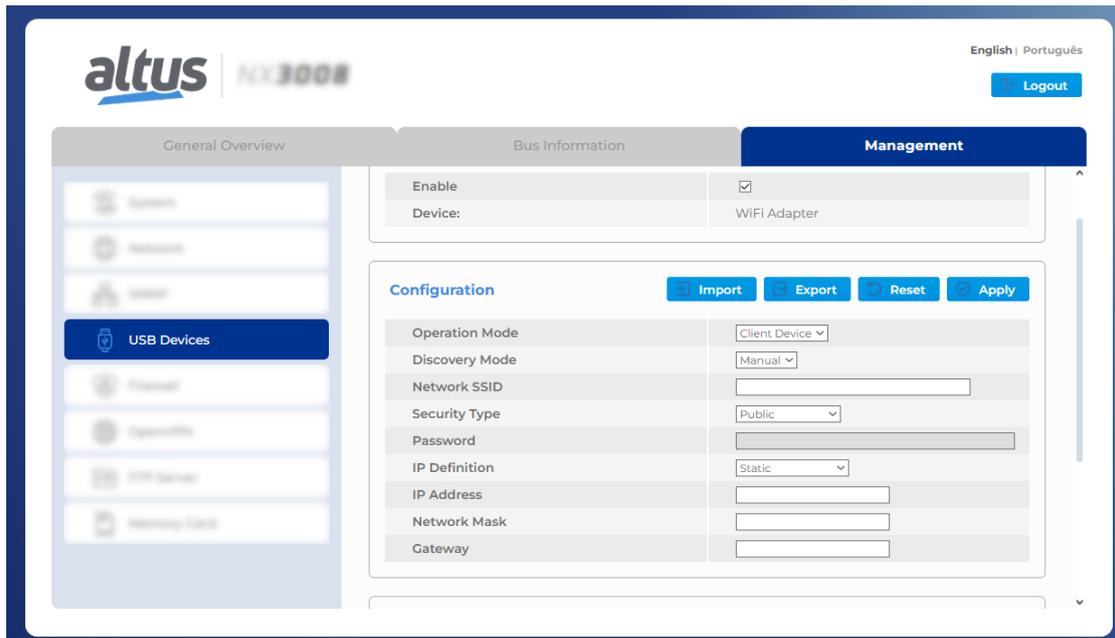


Figure 60: USB WiFi Adapter Configuration

Besides that, the *Configuration* section contains the following buttons:

- **Import:** loads a configuration file
- **Export:** download a file with the current configuration
- **Reset:** returns the configuration to the default
- **Apply:** apply the current configuration

Once the device is properly detected and the network parameters are configured, the controller will always try to keep connected to the WiFi network. The status of this process can be observed by the Connection Status field.

ATTENTION

If the *Default Gateway* was set as "WiFi Adapter", the Gateway of the NET1 diagnostics of the MasterTool will show zero (0.0.0.0). Otherwise, if it was set as "Local Ethernet", the WiFi adapter Gateway will be zero.

The configuration and operation sequence can be summarized into the following steps:

- Plug the device into the USB port. After some seconds, the *USB Devices* page will show the *Device* as "WiFi Adapter". If not, the device might be unsupported or defective.
- Set the network configuration. After clicking on Apply button, the connection process will start. Once configured, it is not necessary to set this information anymore. It will be saved on the controller's memory.
- Watch the connection status on the corresponding field. If everything goes fine, after some seconds it will inform that the adapter is connected to the WiFi network.

The following picture shows the page of a controller connected to a WiFi network:

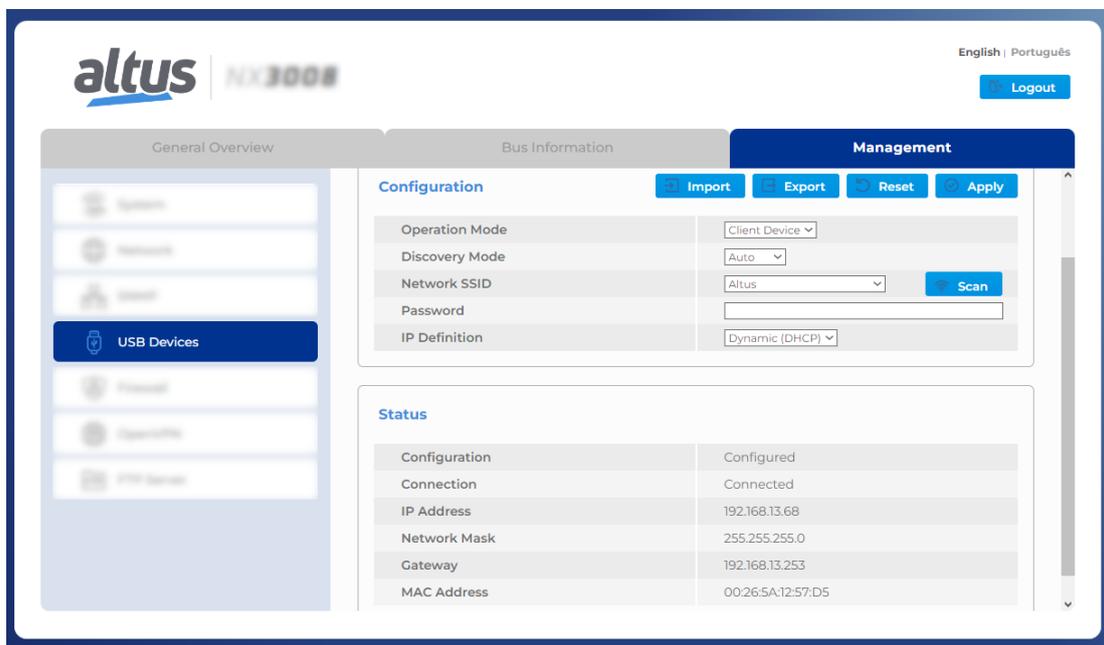


Figure 61: USB WiFi Adapter Connected to a Network

Once connected to the WiFi network, this communication channel can be used for several purposes. To program the PLC with MasterTool IEC XE, the gateway must be configured with the IP address assigned to the WiFi adapter (similar to the USB Modem, Figure 58). This IP address can also be used to access the controller's system web page, where it is possible to perform a firmware update. Additionally, this communication channel can also be used with the MQTT client Function Block to report data to an external broker on the internet (in this case, the WiFi adapter as Default Gateway).

5.6.5. USB Interface Control User Function

To facilitate the management of the USB interface, a function was developed that can be called directly by the user's application code. The **SetUSBState** function was implemented within the **NextoStandard** library. The image below shows the library information, as presented in the *Library Manager*.

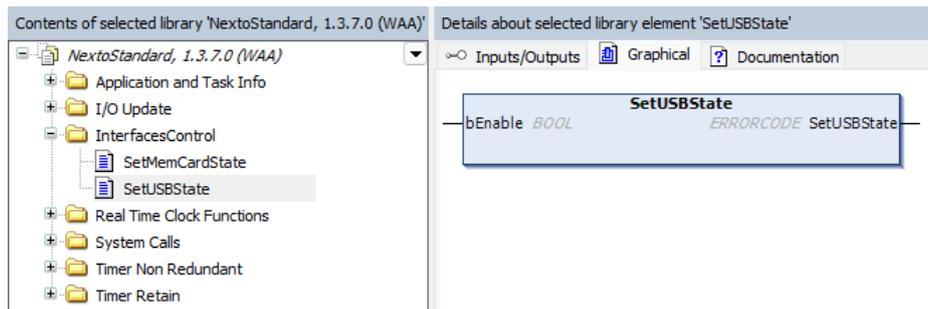


Figure 62: SetUSBState information in Library Manager

The function has an input variable of type *bool*, **bEnable**, which receives the value to enable or disable the USB interface. The function has three return values: *NoError* on success, *SetUSBStateFail* on failure, or *ImportFunctionNotFound* if the function is not supported. The image below shows a basic example of variable declaration and function call.

```
PROGRAM UserPrg
VAR
bSetUSBInterfaceState : BOOL;
stErrorCode           : NextoStandard.ERRORCODE;
END_VAR
-----
stErrorCode := NextoStandard.SetUSBState(bEnable := bSetUSBInterfaceState);
```

ATTENTION

The function executes the command to set the desired value for the USB interface. It is neither necessary nor recommended that the function be called cyclically.

5.7. Ethernet Interfaces Configuration

The NX3008 CPU has NET 1, NET 2, and NET 3. In addition of the local Ethernet interfaces, the Nexto Series also provides remote Ethernet interfaces through the inclusion of the module NX5000. NX5000 modules have only the NET 1 interface.

5.7.1. Internal Ethernet Interfaces

This interfaces are composed by a RJ45 communication connector 10Base-TE/100Base-TX/1000BASE-T standard. It allows the point to point or network communication in the following open protocols: MODBUS TCP Client, MODBUS RTU via TCP Client, MODBUS TCP Server, and MODBUS RTU via TCP Server.

The parameters which must be configured for the proper functioning of the application are described below.

5.7.1.1. NET 1

Configuration	Description	Default	Options
Obtain an IP address automatically	Enables the DHCP Client functionality on the device for automatic IP assignment	Unmarked	Marked or Unmarked
IP Address	IP address of the port on the Ethernet network	192.168.15.1	1.0.0.1 to 223.255.255.254
Subnetwork Mask	Subnet mask of the port on the Ethernet network	255.255.255.0	128.0.0.0 to 255.255.255.252
Gateway Address	Controller Gateway address of the port on the Ethernet network	192.168.15.253	0.0.0.0 to 223.255.255.254

Table 59: NET 1 Configuration

5.7.1.2. NET 2

Configuration	Description	Default	Options
IP Address	IP address of the port on the Ethernet network	192.168.16.1	1.0.0.1 to 223.255.255.254
Subnetwork Mask	Subnet mask of the port on the Ethernet network	255.255.255.0	128.0.0.0 to 255.255.255.252
Gateway Address	Gateway address of the port on the Ethernet network	192.168.16.253	0.0.0.0 to 223.255.255.254

Table 60: NET 2 Configuration

5.7.1.3. NET 3

Configuration	Description	Default	Options
IP Address	IP address of the port on the Ethernet network	192.168.17.1	1.0.0.1 to 223.255.255.254
Subnetwork Mask	Subnet mask of the port on the Ethernet network	255.255.255.0	128.0.0.0 to 255.255.255.252
Gateway Address	Gateway address of the port on the Ethernet network	192.168.17.253	0.0.0.0 to 223.255.255.254

Table 61: NET 3 Configuration

ATTENTION

It is not possible to configure more than one Ethernet interface of a CPU on the same subnet, and this type of configuration is blocked by the MasterTool tool. Therefore, each Ethernet interface must be configured on a different subnet.

5.7.1.4. Configuration of Internal Ethernet Interfaces

The Ethernet channels of the CPU can be configured in three distinct modes of operation: Single Mode, Redundant Mode, or Switch Mode. Different from other Nexto Series CPUs, the NX3008 has three Ethernet ports (NET 1, NET 2, and NET 3).

By default, the NET 1 interface cannot be configured in any mode other than simple. NET 2 has all three configuration options, and NET 3 depends on the settings of NET 2 to be set.

When NET 2 is configured as Redundant Mode or Switch Mode, the NET 2 and NET 3 interfaces operate as a redundant/switch pair, and all information is stored in the NET pair, in this case, NET 2. And in this architecture, NET 3 has all its configuration fields automatically disabled.

If NET 2 is disabled or configured as Simple Mode, the NET 3 interface, if enabled, operates as Simple Mode.

5.7.1.4.1. *Single Mode*

In this mode, the interface operates as an independent Ethernet port, with no relation to the subsequent interface.

Figure 63: Advanced Configuration of Local Ethernet Interfaces - Single Mode

5.7.1.4.2. *Redundant Mode*

In this mode, the interface forms a redundant pair with the subsequent interface, operating in an active/standby scheme. A *NIC Teaming* pair has a single IP address, associated with the interface that is currently active. Thus, a client in a SCADA or MasterTool, connected to a server on the CPU, doesn't have to worry about changing the IP address if any of the ports in the peer fail. In addition, each of the interfaces that form a redundant communication pair has separate diagnostics, to facilitate the debugging of faults that may eventually arise.

Figure 64: Advanced Configuration of Local Ethernet Interfaces - NIC Teaming Mode

When the *NIC Teaming* Mode is selected, on the same screen other parameters are automatically enabled and must be configured:

- **Period of NIC Teaming Test (ms):** Period for sending the communication test frame between the two NETs. Can be configured with values between 100 and 9900, default 500
- **Retries of NIC Teaming Test:** Maximum number of times the NET that sent the frame will wait for a response. Can be configured to values between 1 and 100, default 4
- **Switching Period (s):** Maximum time that NET Active will wait for any given packet. Can be configured with values between 1 and 25, default 10

If the response time of the *NIC Teaming* reaches *Test Period* times the *Number of Retries* and the active interface remains longer than the *Switching Period* without receiving any packets, a switchover occurs, making the previously inactive interface, active. It is important to note that there is a delay between fault detection and activation of the inactive interface due to the time required for its configuration. This delay can be up to a few tens of milliseconds.

When one of the NETs is active, it will assume the configured IP address, and the inactive NET will remain with its IP Address, Subnet Mask and Gateway Address parameters blank in the PCU diagnostics.

5.7.1.4.3. Switch Mode

In this mode, the interface forms a pair with the subsequent interface operating as an Ethernet switch, thus allowing communication over both ports. Thus, this mode allows the "cascading" of several CPUs, enabling the implementation of a ring network topology. It allows two configuration options in switch mode.

5.7.1.4.4. Switch Mode - Disabled

In this mode, the NETs 2 and 3 of the CPU act as a simple switch without any loop protection.

Enable Interface
 Obtain an IP address automatically (Single Mode)

Ethernet Port Parameters

IP Address: 192 . 168 . 15 . 1
Subnetwork Mask: 255 . 255 . 255 . 0
Gateway Address: 192 . 168 . 15 . 253

Mode

Single NIC Teaming Switch

Switch Mode Configuration

Loop Protection Mode: Disabled

Figure 65: Advanced Configuration of Local Ethernet Interfaces - Switch Mode - Disabled

5.7.1.4.5. Switch Mode - MRP

For detailed information on the configuration and operation of the MRP, see the *Configure MRP Ring with ALTUS Controller* section in the Nexto Series PROFINET Manual - MU214621.

Enable Interface

Obtain an IP address automatically (Single Mode)

Ethernet Port Parameters

IP Address

Subnetwork Mask

Gateway Address

Mode

Single NIC Teaming Switch

Switch Mode Configuration

Loop Protection Mode

Figure 66: Advanced Configuration of Local Ethernet Interfaces - Switch Mode - MRP

5.7.1.4.6. Switch Mode - RSTP

In this mode, the pair of network interfaces uses the *Rapid Spanning-Tree protocol* (RSTP) to handle network loops and communication redundancy between devices. When selected, the device forces the RSTP protocol on the bridge. However, if an STP frame is received by its ports, the *Spanning-Tree* protocol is automatically downgraded to *Spanning-Tree Protocol* (STP), thus maintaining communication with the network.

Enable Interface

Obtain an IP address automatically (Single Mode)

Ethernet Port Parameters

IP Address

Subnetwork Mask

Gateway Address

Mode

Single NIC Teaming Switch

Switch Mode Configuration

Loop Protection Mode

Bridge Priority

Max Age

Hello Time (s)

Forward Delay (s)

Tx Hold Count

Ports Path Cost

Auto Ports Path Cost

Figure 67: Advanced Configuration of Local Ethernet Interfaces - Switch Mode - RSTP

When the *Loop Protection Mode* is set to *RSTP*, other parameters are automatically enabled on the same screen and must be configured:

- **Bridge Priority:** Sets the priority of the bridge. The lower the value, the higher the priority. The default value is 32768.
- **Max Age:** The maximum value for the age of a BPDU. When operated in RSTP mode, this value is the maximum number of bridges between the Root and the Bridge that received the BPDU. However, when operated in STP mode, this is the maximum time for it to consider a BPDU frame valid. It can be configured with values between 6 and 40, the default value is 20. The value must follow this rule: $\text{Max Age} \leq 2 \times (\text{Forward Delay} - 1)$.
- **Hello Time (s):** Period for sending BPDU frames. Can be configured with values between 1 and 10, the default value is 2.

- **Forward Delay (s):** The time it takes for the *Root Port* and the *Designated Port* to transition to the *Forwarding* state when operating in STP mode. It can be configured with values between 4 and 30, the default value is 15.
- **Tx Hold Count:** Maximum limit on the number of BPDUs frames the bridge can send each hello-time. Can be set to values between 1 and 10, the default value is 6.
- **Ports Path Cost:** Sets the cost of ports to be used in the RSTP/STP network path. Can be configured with values between 1 and 20000000, the default value is 200000.
- **Auto Ports Path Cost:** When enabled, the cost of the ports is set automatically according to their connection speed, which corresponds to $(2 \times 10^{12}) / (\text{link speed})$. In this configuration, the ports can assume different costs. When disabled, both ports will assume the same cost, set in the previous parameter.

5.7.2. NX5000 Remote Ethernet Interface

5.7.2.1. NET 1

The interfaces are composed by a RJ45 communication connector 10/100Base-TX standard. It allows the point to point or network communication in the following open protocols, for example: MODBUS TCP Client, MODBUS RTU via TCP Client, MODBUS TCP Server and MODBUS RTU via TCP Server.

Below are the IP addressing parameters that must be configured for the proper functioning of the application.

Configuration	Description	Default	Options
IP Address	IP address of the port on the Ethernet network	192.168.xx.68	1.0.0.1 to 223.255.255.254
Subnetwork Mask	Subnet mask of the port on the Ethernet network	255.255.255.0	128.0.0.0 to 255.255.255.252
Gateway Address	Gateway address of the port on the Ethernet network	192.168.xx.253	0.0.0.0 to 223.255.255.254

Table 62: NX5000 Remote NET 1 Configuration

5.7.2.2. Operation Modes of the NX5000 Remote Ethernet Interface

The NX5000 modules can be inserted in the project to increase the number of Ethernet interfaces if the integrated CPU interfaces are not enough.

The Ethernet channels of the NX5000 modules can be used individually, or arranged in redundant pairs.

5.7.2.2.1. Redundant Mode

A set of two Ethernet ports forming a redundant pair has a single IP address associated with the port pair. In this way, a client such as a SCADA system or MasterTool, connected to a server on the CP, does not need to handle IP address changes in the event of a failure in any of the ports of the redundant pair.

To group two NX5000 modules as a redundant pair, the two modules must be installed in adjacent positions in the rack, and the *NIC Teaming* checkbox of the left-hand module must be selected. When this is done, parameter editing on the right-hand module is locked. The parameters edited on the left-hand module then apply to both modules.

Conversely, clearing the *NIC Teaming* checkbox of the left-hand module separates the modules, which then operate as individual, non-redundant modules.

When the *NIC Teaming* mode is selected, additional parameters are automatically enabled on the same screen and must be configured:

Figure 68: Advanced Configuration of Remote Ethernet Interface - NX5000

5.7.3. Reserved TCP/UDP Ports

The following TCP/UDP ports of the Ethernet interfaces, both integrated and remote, are used by CPU services (depending on availability according to table [Protocols](#)) and, therefore, are reserved and must not be used by the user.

Service	TCP	UDP
System Web Page	80	-
SNTP	-	123
SNMP	-	161
MODBUS TCP	502*	-
MasterTool	1217*	1740:1743
SQL Server	1433	-
MQTT	1883* / 8883*	-
EtherNet/IP	44818	2222
IEC 60870-5-104	2404*	-
IEC 61850	102*	-
DNP3	20000* / 20005*	-
OPC UA	4840	-
WEBVISU	8080	-
CODESYS ARTI	11740	-
PROFINET	-	34964
Portainer Docker	9000	-
SysLog	-	514
LibHART	1234	-

Table 63: Reserved TCP/UDP ports

* Default port, but user changeable.

5.7.4. Network Routing

For integrated Ethernet ports, the CPU operating system has a network routing mechanism that allows the communication between different networks:

1. Client protocols, when configured to communicate with a Server device located in a different network, will resolve the routing by the following priority:
 - VPN (if this feature is enabled and the network of NET interface of Client protocol is configured as a *Private Network* on the VPN Server settings)
 - USB Devices (Modem, Ethernet or Wifi)

- Another integrated NET interface configured to the same network as the destination address (in this case, the communication will route internally)

If none of these conditions occurs, the operating system will forward the communication to the Default Gateway configured on the NET interfaces, starting from the one configured on NET1 and then going through the next ones if the communication fails.

2. Server protocols will accept connections only on the interface where it is instantiated, except for MODBUS, where a new parameter (introduced on MasterTool 3.75) called *Allow Connections from Any Interface* gives the ability to receive incoming connections from other interfaces like a USB Modem or VPN.

For remote Ethernet ports (NX5000 module), the routing is more restrict and does not interact with the integrated ports:

1. Client protocols, when configured to communicate with a Server device located in a different network, will forward the communication to the Default Gateway configured on its NET interface.
2. Server protocols will accept connections only from its NET interface.

5.8. Protocols Configuration

Independently of the protocols used in each application, the Nexto Series CPUs has some maximum limits for each CPU model. There are basically two different types of communication protocols: symbolic and direct representation mappings. The maximum limit of mappings as well as the maximum protocol quantity (instances) is defined on table below:

	NX3008
Mapped Points	20480
Mappings (Per Instance / Total)	5120 / 20480
Requests	512
NETs – Client or Server Instances (Per NET / Total)	4 / 16
COM (n) – Master or Slave Instances	1
Control Centers	3

Table 64: Protocols Limits per CPU

Notes:

Mapped Points: It is the maximum number of mapped points that the CPU supports. Each mapping can contain one or more mapped points, depending on the data size. This varies depending on whether simple variables or ARRAY-type variables are used. Each simple variable, as well as each index of an ARRAY, is counted as a mapped point, even if it occupies more than one address in the driver. For example, a simple DWORD-type variable mapped in the MODBUS protocol will be counted as a single point, even though it occupies two consecutive addresses/registers in the driver.

Mappings: A “mapping” is the relationship between an internal application variable and an object of the application protocol. This field informs the maximum number of mappings supported by the CPU. It corresponds to the sum of all mappings made within the instances of communication protocols and their respective devices.

Requests: The sum of the requests of the communications protocols, declared on devices, may not exceed the maximum number of requests supported by the CPU.

NETs – Clients or Servers Instances: This field defines the maximum number of protocol instances per Ethernet interface, and also the total maximum distributed along all the Ethernet interfaces of the system.

COM (n) – Master or Slave Instances: Due to its characteristics, each serial interface supports only one communication protocol instance. Examples of instances compatible with serial interfaces: MODBUS RTU Master and MODBUS RTU Slave.

Control Centers: “Control Center” is all client device connected to the CPU through protocol IEC 60870-5-104. This field informs the maximum of client devices of control center type supported by the CPU. Correspond to the sum of all client devices of communication protocol IEC 60870-5-104 Server (does not include master or clients from MODBUS RTU Slave, MODBUS Server and DNP3 Server protocols).

The limitations of the MODBUS protocol for Direct Representation and symbolic mapping for the CPUs can be seen in Tables 65 and 66, respectively.

Limitations	MODBUS RTU Master	MODBUS RTU Slave	MODBUS Ethernet Client	MODBUS Ethernet Server
Mappings per instance	128	32	128	32
Devices per instance	64	1 ⁽¹⁾	64	64 ⁽²⁾
Mappings per device	32	32	32	32
Simultaneous requests per instance	-	-	128	64
Simultaneous requests per device	-	-	8	64

Table 65: MODBUS Protocol Limitations for Direct Representation

Notes:**Devices per instance:**

- Master or Client Protocols: number of slaves or server devices supported by each Master or Slave protocol instance.
- MODBUS RTU Slave Protocol: the limit ⁽¹⁾ informed relates to serial interfaces that do not allow a Slave to establish communication through the same serial interface, simultaneously, with more than one Master device. It's not necessary, nor is it possible to declare or configure the Master device in the instance of the MODBUS RTU slave protocol. The master device will have access to all the mappings made directly on the instance of MODBUS RTU slave protocol.
- MODBUS RTU Server Protocol: the limit ⁽²⁾ informed relates to the Ethernet interfaces, which limit the number of connections that can be established with other devices through a single Ethernet interface. It is not necessary, nor is it possible to declare or configure Clients devices in the instance of the MODBUS Server protocol. All Clients devices will have access to all the mappings made directly in the instance of the MODBUS Server protocol.

Mappings per device: The maximum number of mappings per device, despite being listed above, is also limited by the protocol maximum number of mappings. Also to be considered the maximum CPU mappings as in Table 5.8.

Simultaneous Requests per Instance: Number of requests that can be simultaneously transmitted by each Client protocol instance or that can be received simultaneously by each Server protocol instance. MODBUS RTU protocol instances, Master or Slave, do not support simultaneous requests.

Simultaneous Requests per Device: Number of requests that can be simultaneously transmitted to each MODBUS Server device, or may be received simultaneously by each MODBUS client device. MODBUS RTU devices, Master or Slave, do not support simultaneous requests.

Limitations	MODBUS RTU Master	MODBUS RTU Slave	MODBUS Ethernet Client	MODBUS Ethernet Server
Devices per instance	64	1 ⁽¹⁾	64	64 ⁽²⁾
Requests per device	32	-	32	-
Simultaneous requests per instance	-	-	128	64
Simultaneous requests per device	-	-	8	64

Table 66: MODBUS Protocol Limitations for Symbolic Mappings

Notes:**Devices per instance:**

- Master or Client Protocol: Number of slave or server devices supported by each Master or Client protocol instance.
- MODBUS RTU Slave Protocol: the limit ⁽¹⁾ informed relates to serial interfaces that do not allow a Slave to establish communication through the same serial interface, simultaneously, with more than one Master device. It's not necessary, nor is it possible to declare or configure the Master device in the instance of the MODBUS RTU slave protocol. The master device will have access to all the mappings made directly on the instance of MODBUS RTU slave protocol.
- MODBUS RTU Server Protocol: the limit ⁽²⁾ informed relates to the Ethernet interfaces, which limit the amount of connections that can be established with other devices through a single Ethernet interface. It is not necessary, nor is it possible to declare or configure Clients devices in the instance of the MODBUS Server protocol. All Clients devices will have access to all the mappings made directly in the instance of the MODBUS Server protocol.

Requests by device: Number of requests, such as reading or writing holding registers, which can be configured for each of the devices (slaves or servers) from Master or Client protocols instances. This parameter does not apply to instances of Slave or Server protocols.

Simultaneous Requests per Instance: Number of requests that can be simultaneously transmitted by each client protocol instance or that can be received simultaneously by each server protocol instance. MODBUS RTU protocol instances, Master or Slave, do not support simultaneous requests.

Simultaneous Requests per Device: Number of requests that can be simultaneously transmitted for each MODBUS server device, or may be received simultaneously from each MODBUS client device. MODBUS RTU devices, Master or Slave do not support simultaneous requests.

ATTENTION

Simultaneous requests to a variable associated to communication points, those which support the SBO operation mode (Select Before Operate), even being received from different devices are not supported. Once started the selection/operation of a point by a specific device, that must be finished before this point become able to be commanded by another device.

The protocol IEC 60870-5-104 Server limitations can be watched on table below.

Limitations	IEC 60870-5-104 Server
Devices per instance	3
Simultaneous requests per instance	3
Simultaneous requests per device	1

Table 67: Protocol IEC 60870-5-104 Server Limits

Notes:

Devices per instance: Quantity of client devices, of type control center, supported for each IEC 60870-5-104 Server protocol instance. The limit informed might be smaller because of the CPU total limits (check Table 5.8).

Simultaneous requests per instance: Quantity of requests that can be received simultaneously by each instance of Server protocol.

Simultaneous requests per device: Quantity of requests that can be received simultaneously of each IEC 60870-5-104 Client device.

5.8.1. Protocol Behavior x CPU State

The table below shows in detail the behavior of each configurable protocol in Nexto Series CPUs in every state of operation.

Protocol	Type	CPU operational state					
		STOP			RUN		
		After download, before application starts	After the application goes to STOP (PAUSE)	After an exception	Non redundant or Active	Redundant in Stand-by	After a break-point in MainPrg
MODBUS Symbol	Slave/Server	✓	✓	✓	✓	✓	✓
	Master/Client	✗	✗	✗	✓	✓	✓
MODBUS	Slave/Server	✗	✗	✗	✓	✓	✗
	Master/Client	✗	✗	✗	✓	✓	✓
SOE (DNP3)	Outstation	✓	✓	✓	✓	✗	✓
IEC 60870-5-104	Server	✗	✗	✗	✓	✗	✓
EtherCAT	Master	✓	✓	✗	✓	NA	✓
OPC DA	Server	✓	✓	✓	✓	✗	✓
OPC UA	Server	✓	✓	✓	✓	✓	✓
SNTP	Client	✓	✓	✓	✓	✓	✓
HTTP	Server	✓	✓	✓	✓	✓	✓
SNMP	Agent	✓	✓	✓	✓	✓	✓
EtherNet/IP	Scanner	✓	✓	✗	✓	NA	✗
	Adapter	✗	✓	✗	✓	NA	✗

Table 68: Protocol Behavior x CPU State

Notes:

Symbol ✓: Protocol remains active and operating normally.

Symbol ✗: Protocol is disabled.

MODBUS Symbol Slave/Server: To keep the protocol communicating when the CPU isn't in RUN or after a breakpoint, it's need to check the option "Keep the communication running on CPU stop".

5.8.2. Double Points

The input and output double digital points representation is done through a special data type called DBP (defined in the *LibDataTypes* library). This type consist basically in a structure of two BOOL type elements, called OFF and ON (equivalent to TRIP and CLOSE respectively).

In Nexto, variables of this type cannot be associated to digital input and output modules, being necessary the single digital points mapping, BOOL type, and the treatment by application to conversion in double points.

To further information about the double points mapping in the input and output digital modules check the [IEC 60870-5-104 Server](#) section.

5.8.3. CPU's Events Queue

The CPU owns an events queue of type FIFO (First In, First Out) used to store temporarily the events related to communication points until they are moved to their final destiny.

All communication points events generated in the CPU are directed and stored in CPU's queue. This queue has the following features:

- Size: 1000 events
- Retentivity : it is not retentive
- Overflow policy: keep the newest

ATTENTION

In the Nexto PLC, the events queue is stored in a non-retentive memory area (volatile). This way, the events present in CPU's queue, which haven't been transmitted yet to the control center, are going to be lost in a CPU's eventual power off.

The in and out of events in this queue follows the concept of producer/consumer. Producers are those system elements capable of generate events, adding events in the CPU's queue, while the consumers are those system elements which receive and use this events, taking them of the CPU's queue. The figure below describes this working, including the example of some events consumers and producers.

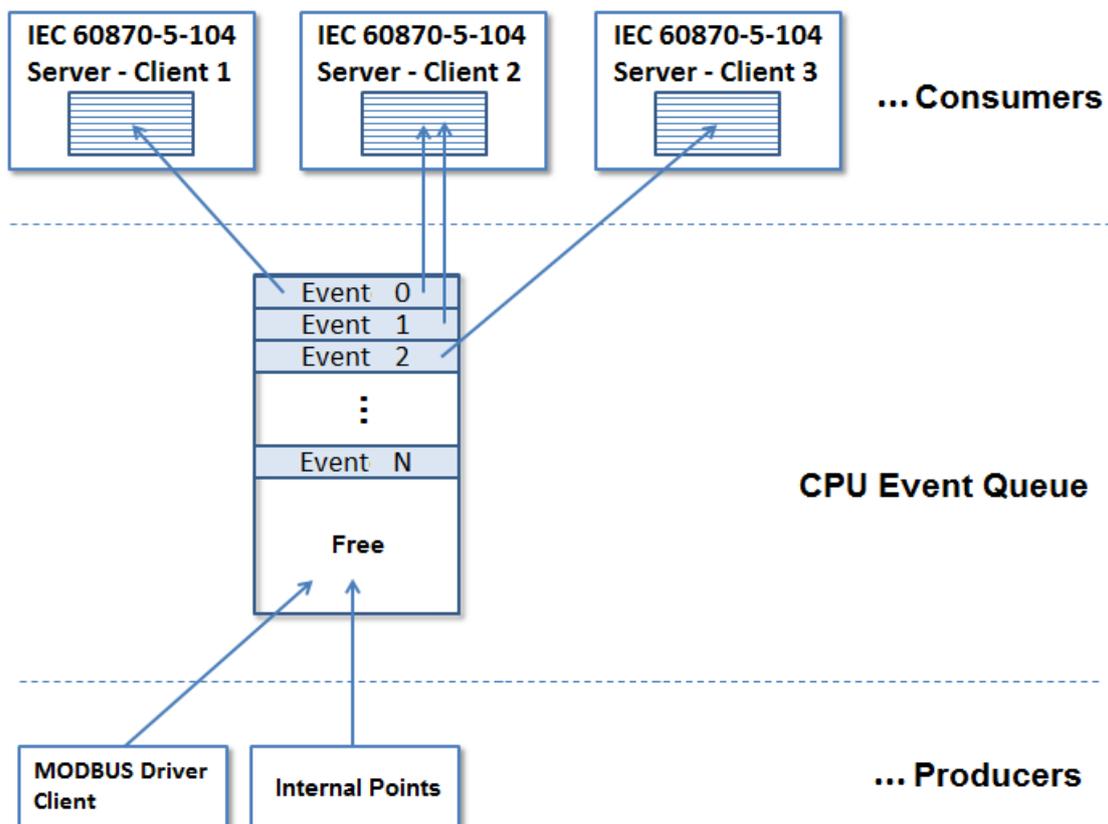


Figure 69: CPU's Event Queue

5.8.3.1. Consumers

The consumers are typically communication drivers that will communicate with SCADA or HMI. After been stored in CPU's queue, the consumers receive the events related to communication points mapped in its configuration. These events are then stored in a consumer's own events queue, which the size and working are described on the communication driver specific section.

5.8.3.2. Queue Functioning Principles

Once stored in CPU's queue, each event is transmitted to the consumer that has this communication point in its data base. On the figure above, the Event 0 is referred to a communication point mapped to two control centers IEC 60870-5-104 (Client 1 and 2). Thus the Event 1 is referred to a communication point mapped only to one control center IEC 60870-5-104 (Client 2). By its time, the Event 2 is referred to a communication point mapped to another control center IEC 60870-5-104 (Client 3).

The events remain stored in the CPU's queue until all its consumers acknowledge its receiving. The criteria used to confirm the receive is specific of each consumer. In case of the IEC 60870-5-104 Server, the acknowledge occurs when the event is transmitted to the IEC 60870-5-104 client.

In Nexto Series case, there are no diagnostics available to watch the CPU's events queue occupation, not even information about the queue overflow. However the consumers have a diagnostics group referred to its events queue. Further information can be found at the specific driver communication section.

5.8.3.2.1. Overflow Sign

The overflow sign to the consumers' events queue occurs in two situations:

- When the consumer events queue is out of space to store new events
- If the CPU aborted the event generation (because occurred to more events in a single execution cycle than the events queue total size)

5.8.3.3. Producers

The producers are typically communication drivers or PLC internal elements that are capable to generate events. The previous figure show some examples.

- **Internal Points:** This is a PLC's firmware internal element, which detects events each execution cycle (MainTask) to those communication points that don't have a defined origin and then inserts the events in the CPU's queue. The maximum number of events that can be detected in each MainTask cycle is equal to the CPU's events queue size. In case the number of generated events is bigger than this, in a single cycle, the exceeding are going to be lost.
- **MODBUS Driver (Client/Server/Master/Slave):** The variables value change caused by MODBUS read/write are detected at each MainTask cycle and then the events are inserted in CPU's queue. In Client/Master cases, are also generated quality events when there is a communication failure with the slave device.

5.8.4. Interception of Commands Coming from the Control Center

The Nexto PLC has a function block that allows selection commands and operation to the output points received by server drivers (IEC 60870-5-104 Server) been treated by the user logic. This resource allows the interlocking implementation, as well as the handling of the received command data in the user logic, or yet the command redirecting to different IEDs.

The commands interception is implemented by the *CommandReceiver* function block, defined in the *LibRtuStandard*. The input and output parameters are described on the following tables:

Parameter	Type	Description
bExec	BOOL	When TRUE, executes the command interception
bDone	BOOL	Indicates that the command output data have been already processed, releasing the function block to receive another command
dwVariableAddr	DWORD	Variable address, mapped in the server driver, which will receive the client command
eCommandResult	ENUM	Input action defined by user from the following list: SUCCESS(0) NOT_SUPPORTED(1) BLOCKED_BY_SWITCHING_HIERARCHY(2) SELECT_FAILED(3) INVALID_POSITION(4) POSITION_REACHED(5) PARAMETER_CHANGE_IN_EXECUTION(6) STEP_LIMIT(7) BLOCKED_BY_MODE(8) BLOCKED_BY_PROCESS(9) BLOCKED_BY_INTERLOCKING(10) BLOCKED_BY_SYNCHROCHECK(11) COMMAND_ALREADY_IN_EXECUTION(12) BLOCKED_BY_HEALTH (13) ONE_OF_N_CONTROL(14) ABORTION_BY_CANCEL(15) TIME_LIMIT_OVER(16) ABORTION_BY_TRIP(17) OBJECT_NOT_SELECTED(18) OBJECT_ALREADY_SELECTED(19) NO_ACCESS_AUTHORITY(20) ENDED_WITH_OVERSHOOT(21) ABORTION_DUE_TO_DEVIATION(22) ABORTION_BY_COMMUNICATION_LOSS(23) BLOCKED_BY_COMAND(24) NONE(25) INCONSISTENT_PARAMETERS(26) LOCKED_BY_OTHER_CLIENT(27) HARDWARE_ERROR(28) UNKNOWN(29)
dwTimeout	DWORD	Time-out [ms] to the treatment by user logic

Table 69: CommandReceiver Function Block Input Parameters

Notes:

bExec: When FALSE, the command just stop being intercepted for the user application, but it keeps being treated normally by the server.

bDone: After the command interception, the user is going to be responsible for treat it. At the end of the treatment, this input must be enabled for a new command can be received. Case this input is not enabled, the block is going to wait the time defined in *dwTimeout*, to then become capable of intercept new commands.

eCommandResult: Treatment results of command intercepted by user. The result returned to the client that sent the command, which must be attributed together with the input *bDone*, is converted to the protocol's format from which was received the command. In Nexto Series it is only supported the interception of commands coming from protocol IEC 60870-5-104. In protocol interception, any return different from *SUCCESS* results in a negative Acknowledge.

ATTENTION

It is not recommended the simultaneous commands interception to one same variable by two or more *CommandReceiver* function blocks. Just one of the function blocks will intercept correctly the command, being able to suffer undesirable interference from the others function blocks if addressed to the same variable.

Parameter	Type	Description
bCommandAvailable	BOOL	Indicates that a command was intercepted and the data are available to be processed
sCommand	STRUCT	This structure stores received command data, which is composed by the following fields: eCommand sSelectParameters sOperateParameters The description of each field is in this section.
eStatus	ENUM (TYPE_RESULT)	Out of function action from obtained result, according to list: OK_SUCCESS(0) ERROR_FAILED(1)

Table 70: CommandReceiver Function Block Output Parameters

Note:

eStatus: Return of a register process of a communication point command interception. When the interception is registered with success *OK_SUCCESS* is returned, else *ERROR_FAILED* is. In case interceptor register failure, commands to the determined point are not intercepted by this function block. *TYPE_RESULT* is defined in *LibDataTypes* library.

Supported commands are described on table below:

Parameter	Type	Description
eCommand	ENUM	NO_COMMAND(0) SELECT(1) OPERATE(2)

Table 71: CommandReceiver Function Block Supported Commands

The parameters that build the *sSelectParameters*, *sOperateParameters* and *sCancelParameters* structures are described on the following table:

Parameter	Type	Description
sSelectConfig	STRUCT	Received selection command configuration. This structure parameters are described on Table 73
sValue	STRUCT	Received value in a select, when is received a selection command with value. This structure parameters are described on Table 76

Table 72: Parameters sSelectParameters

Parameter	Type	Description
bSelectWithValue	BOOL	When true indicates a selection command reception with value.

Table 73: Parameters sSelectConfig

Parameter	Type	Description
sOperateConfig	STRUCT	Received selection command configuration. This structure parameters are described on Table 75
sValue	STRUCT	Field of received operation command referred value. This structure parameters are described on Table 76

Table 74: Parameters sOperateParameters

Parameter	Type	Description
bDirectOperate	BOOL	When true indicates that an operation command without select was received.
bNoAcknowledgement	BOOL	When true indicates that a command, which doesn't require the receiving acknowledge, was received.
bTimedOperate	BOOL	When true indicates that an operation command activated by time was received.
liOperateTime	LINT	Programming of the instant in which it must be runned the command. This field is valid only when <i>bTimedOperate</i> is true.
bTest	BOOL	When true indicates that the received command was sent only for test, as so the command must not be runned.

Table 75: Parameters sOperateConfig

Parameter	Type	Description
eParamType	ENUM	Informs the type of the received command: NO_COMMAND(0) SINGLE_POINT_COMMAND(1) DOUBLE_POINT_COMMAND(2) INTEGER_STATUS_COMMAND(3) ENUMERATED_STATUS_COMMAND(4) ANALOGUE_VALUE_COMMAND(5)
sSinglePoint	STRUCT	When a command is received, in received command type function, defined by eParamType, the corresponding data structure is filled. This structures parameters are described on Tables 77 to 81
sDoublePoint	STRUCT	
sIntegerStatus	STRUCT	
sEnumeratedStatus	STRUCT	
sAnalogueValue	STRUCT	

Table 76: Parameters sValue

Parameter	Type	Description
bValue	BOOL	Point operation value.
sPulseConfig	STRUCT	The pulsed command configuration parameters are stored in this structure. This structure parameters are described on Table 82.

Table 77: Parameters sSinglePoint

Parameter	Type	Description
bValue	BOOL	Point operation value.
sPulseConfig	STRUCT	The pulsed command configuration parameters are stored in this structure. This structure parameters are described on Table 82.

Table 78: Parameters sDoublePoint

Parameter	Type	Description
diValue	DINT	Point operation value.

Table 79: Parameters sIntegerStatus

Parameter	Type	Description
dwValue	DWORD	Point operation value.

Table 80: Parameters sEnumeratedStatus

Parameter	Type	Description
eType	ENUM	Informs the data type of the received analog value. INTEGER (0) FLOAT (1)
diValue	DINT	Point operation value, integer format.
fValue	REAL	Point operation value, float format.

Table 81: Parameters sAnalogueValue

Parameter	Type	Description
bPulseCommand	BOOL	When true indicates that received command is pulsed.
dwOnDuration	DWORD	This is time, in milliseconds, that the output must remain on.
dwOffDuration	DWORD	This is time, in milliseconds, that the output must remain off.
dwPulseCount	DWORD	Number of times the command must be executed.

Table 82: Parameters sPulseConfig

To intercept commands to a specific point, first it is need to load in the *dwVariableAddr* parameter the variable address correspondent to the point wanted to intercept the commands and then execute a pulse in the *bExec* parameter. Once the command

was intercepted, the function block informs that a command was intercepted through *bCommandAvailable* parameter. The intercepted command information are then filled in the *sCommand* and *eStatus* output parameters, according to the received command type. This operation depends only of the received command type, don't matter the variable's data type to which is being intercepted the command. The interception is finished and then the function block can be released to intercept a new command when *bDone* parameter is *true*. Yet must be pointed the command processing result in *eCommandResult*.

5.8.5. MODBUS RTU Master

This protocol is available for the Nexto Series CPUs in its serial channels. By selecting this option at MasterTool IEC XE, the CPU becomes MODBUS communication master, allowing the access to other devices with the same protocol, when it is in the execution mode (*Run Mode*).

There are two configuration modes for this protocol. One makes use of Direct Representation (%Q), in which the variables are defined by its address. The other, called Symbolic Mapping has the variables defined by its name.

Regardless of the configuration mode, the steps to insert a protocol instance and configure the serial interface are the same. The procedure to insert a protocol instance is found in detail in the MasterTool IEC XE User Manual - MU299609 or in the section [Inserting a Protocol Instance](#). The remaining configuration steps are described below for each mode.

- Add the MODBUS RTU Master Protocol instance to the serial channel. To execute this procedure, see [Inserting a Protocol Instance](#) section.
- Configure the serial interface, choosing the transmission speed, the parity, the channel stop bits, among others configurations by a double click on the COM 1 serial channel (or COM 2 - if available). See [Serial Interfaces Configuration](#) section.

5.8.5.1. MODBUS Master Protocol Configuration by Symbolic Mapping

To configure this protocol using symbolic mapping, you must perform the following steps:

- Configure the general parameters of the MODBUS Master protocol, like: transmission delay times and minimum inter-frame as in [Figure 70](#).
- Add and configure devices via the General Parameters tab, defining the slave address, communication time-out and number of communication retries as can be seen in [Figure 71](#).
- Add and configure the MODBUS mappings on Mappings tab as [Figure 72](#), specifying the variable name, data type, and the data initial address, the data size and range are filled automatically.
- Add and configure the MODBUS requests as presented in [Figure 73](#), specifying the function, the scan time of the request, the starting address (read/write), the data size (read/write) and generate diagnostic variables and disabling the request via the buttons at the bottom of the window.

5.8.5.1.1. MODBUS Master Protocol General Parameters – Symbolic Mapping Configuration

The general parameters, found on the MODBUS protocol initial screen (figure below), are defined as:

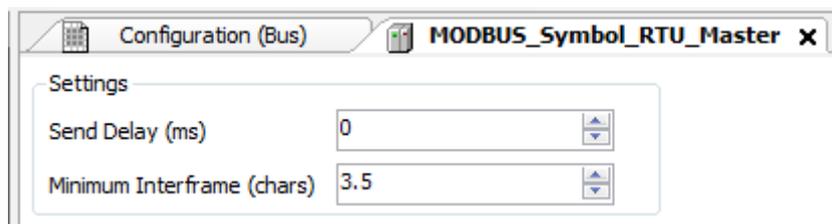


Figure 70: MODBUS RTU Master Configuration Screen

Configuration	Description	Default	Options
Send Delay (ms)	Delay for the answer transmission.	0	0 to 65535
Minimum Interframe (chars)	Minimum silence time between different frames.	3.5	3.5 to 100.0

Table 83: MODBUS RTU Master General Configurations

Notes:

Send Delay: The answer to a MODBUS protocol may cause problems in certain moments, as in the RS-485 interface or other half-duplex. Sometimes there is a delay between the slave answer time and the physical line silence (slave delay to put RTS in zero and put the RS-485 in high impedance state). To solve this problem, the master can wait the determined time in this field before sending the new request. Otherwise, the first bytes transmitted by the master could be lost.

Minimum Interframe: The MODBUS standard defines this time as 3.5 characters, but this parameter is configurable in order to attend the devices which do not follow the standard.

The MODBUS protocol diagnostics and commands configured, either by symbolic mapping or direct representation, are stored in *T_DIAG_MODBUS_RTU_MASTER_I* variables. For the direct representation mapping, they are also in 4 bytes and 8 words which are described in table below:

T_DIAG_MODBUS_RTU_MASTER_1.*	Size	Description
Diagnostic Bits:		
tDiag.bRunning	BIT	The master is running.
tDiag.bNotRunning	BIT	The master is not running (see bit: bInterruptedByCommand).
tDiag.bInterruptedByCommand	BIT	The bit bNotRunning was enabled as the master was interrupted by the user through command bits.
tDiag.bConfigFailure	BIT	Configuration failure.
tDiag.bModuleFailure	BIT	Not implemented.
Error codes:		
eErrorCode	SERIAL_STATUS (BYTE)	0: there are no errors 1: invalid serial port 2: invalid serial port mode 3: invalid baud rate 4: invalid data bits 5: invalid parity 6: invalid stop bits 7: invalid modem signal parameter 8: invalid UART RX Threshold parameter 9: invalid time-out parameter 10: busy serial port 11: UART hardware error 12: remote hardware error 20: invalid transmission buffer size 21: invalid signal modem method 22: CTS time-out = true 23: CTS time-out = false 24: transmission time-out error 30: invalid reception buffer size 31: reception time-out error 32: flow control configured differently from manual 33: invalid flow control for the configured serial port 34: data reception not allowed in normal mode 35: data reception not allowed in extended mode 36: DCD interruption not allowed 37: CTS interruption not allowed 38: DSR interruption not allowed 39: serial port not configured 50: internal error in the serial port
Command bits, automatically initialized:		
tCommand.bStop	BIT	Stop master.
tCommand.bRestart	BIT	Restart master.
tCommand.bResetCounter	BIT	Restart diagnostics statistics (counters).

T_DIAG_MODBUS_RTU_MASTER_1.*	Size	Description
Communication Statistics:		
tStat.wTXRequests	WORD	Counter of request transmitted by the master (0 to 65535).
tStat.wRXNormalResponses	WORD	Counter of normal responses received by the master (0 to 65535).
tStat.wRXExceptionResponses	WORD	Counter of responses with exception codes received by the master (0 to 65535).
tStat.wRXIllegalResponses	WORD	Counter of illegal responses received by master – invalid syntax, not enough received bytes, invalid CRC – (0 to 65535).
tStat.wRXOverrunErrors	WORD	Counter of overrun errors during reception - UART FIFO or RX line – (0 to 65535).
tStat.wRXIncompleteFrames	WORD	Counter of answers with construction errors, parity or failure during reception (0 to 65535).
tStat.wCTSTimeOutErrors	WORD	Counter of CTS time-out error, using RTS/CTS handshake, during transmission (0 to 65535).

Table 84: MODBUS RTU Master Diagnostics

Note:

Counters: All MODBUS RTU Master diagnostics counters return to zero when the limit value 65535 is exceeded.

5.8.5.1.2. *Devices Configuration – Symbolic Mapping configuration*

The devices configuration, shown on figure below, follows the following parameters:

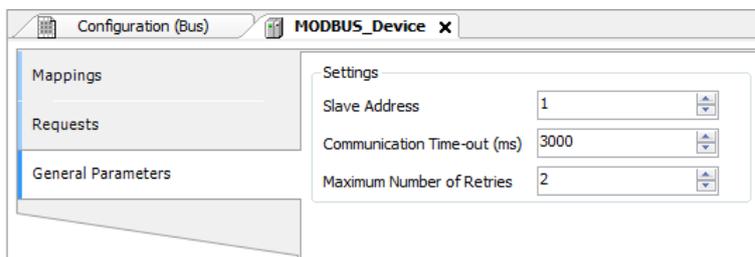


Figure 71: Device General Parameters Settings

Configuration	Description	Default	Options
Slave Address	MODBUS slave address	1	0 to 255
Communication Time-out (ms)	Defines the application level time-out	3000	10 to 65535
Maximum Number of Retries	Defines the numbers of retries before reporting a communication error	2	0 to 9

Table 85: Device Configurations

Notes:

Slave Address: According to the MODBUS standard, the valid slave addresses are from 0 to 247, where the addresses from 248 to 255 are reserved. When the master sends a writing command with the address configured as zero, it is making broadcast requests in the network.

Communication Time-out: The communication time-out is the time that the master waits for a response from the slave to the request. For a MODBUS RTU master device it must be taken into account at least the following system variables: the time it takes the slave to transmit the frame (according to the baud rate), the time the slave takes to process the request and the response sending delay if configured in the slave. It is recommended that the time-out is equal to or greater than the time to transmit the frame plus the delay of sending the response and twice the processing time of the request. For more information, see [Communication Performance](#) section.

Maximum number of retries: Sets the number of retries before reporting a communication error. For example, if the slave does not respond to a request and the master is set to send three retries, the error counter number is incremented by one unit when the execution of these three retries. After the increase of the communication error trying to process restarts and if the number of retries is reached again, new error will increment the counter.

5.8.5.1.3. Mappings Configuration – Symbolic Mapping Settings

The MODBUS relations configuration, showed on figure below, follows the parameters described on table below:

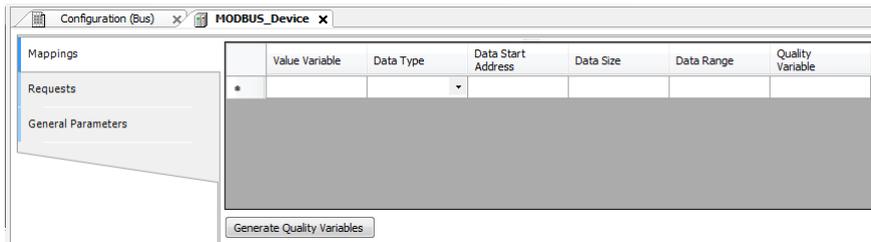


Figure 72: MODBUS Data Mappings Screen

Configuration	Description	Default	Options
Value Variable	Symbolic variable name	-	Name of a variable declared in a program or GVL
Data Type	MODBUS data type	-	Coil - Write (1 bit) Coil - Read (1 bit) Holding Register - Write (16 bits) Holding Register - Read (16 bits) Holding Register – Mask AND (16 bits) Holding Register – Mask OR (16 bits) Input Register (16 bits) Input Status (1 bit)
Data Start Address	Initial address of the MODBUS data	-	1 to 65536
Data Size	Size of the MODBUS data	-	1 to 65536
Data Range	The address range of configured data	-	-

Table 86: MODBUS Mappings Settings

Notes:

Value Variable: this field is used to specify a symbolic variable in MODBUS relation.

Data type: this field is used to specify the data type used in the MODBUS relation.

Data Type	Size [bits]	Description
Coil - Write	1	Writing digital output.
Coil - Read	1	Reading digital output.
Holding Register - Write	16	Writing analog output.
Holding Register - Read	16	Reading analog output.
Holding Register - Mask AND	16	Analog output which can be read or written with AND mask.
Holding Register - Mask OR	16	Analog output which can be read or written with OR mask.
Input Register	16	Analog input which can be only read.
Input Status	1	Digital input which can be only read.

Table 87: Data Types Supported in MODBUS

4. INITIAL PROGRAMMING

Data Start Address: Data initial address of a MODBUS mapping.

Data Size: The size value specifies the maximum amount of data that a MODBUS interface can access, from the initial address. Thus, to read a continuous address range, it is necessary that all addresses are declared in a single interface. This field varies with the MODBUS data type configured.

Data Range: This field shows to the user the memory address range used by the MODBUS interface.

5.8.5.1.4. Requests Configuration – Symbolic Mapping Settings

The configuration of the MODBUS requests, viewed in figure below, follow the parameters described in table below:

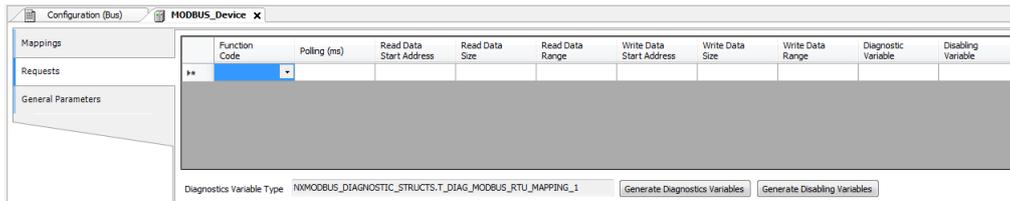


Figure 73: Data Requests Screen MODBUS Master

Configuration	Description	Default Value	Options
Function Code	MODBUS function type	-	01 – Read Coils 02 – Read Input Status 03 – Read Holding Registers 04 – Read Input Registers 05 – Write Single Coil 06 – Write Single Register 15 – Write Multiple Coils 16 – Write Multiple Registers 22 – Mask Write Register 23 – Read/Write Multiple Registers
Polling (ms)	Communication period (ms)	100	0 to 3600000
Read Data Start Address	Initial address of the MODBUS read data	-	1 to 65536
Read Data Size	Size of MODBUS Read data	-	Depends on the function used
Read Data Range	MODBUS Read data address range	-	0 to 2147483646
Write Data Start Address	Initial address of the MODBUS write data	-	1 to 65536
Write Data Size	Size of MODBUS Write data	-	Depends on the function used
Write Data Range	MODBUS Write data address range	-	0 to 2147483647
Diagnostic Variable	Diagnostic variable name	-	Name of a variable declared in a program or GVL
Disabling Variable	Variable used to disable MODBUS relation	-	Field for symbolic variable used to disable, individually, MODBUS requests configured. This variable must be of type BOOL. The variable can be simple or array element and can be in structures.

Table 88: MODBUS Relations Configuration

Notes:

Setting: the number of factory default settings and the values for the column Options may vary according to the data type and MODBUS function (FC).

Function Code: MODBUS (FC) functions available are the following:

Code		Description
DEC	HEX	
1	0x01	Read Coils (FC 01)
2	0x02	Read Input Status (FC 02)
3	0x03	Read Holding Registers (FC 03)
4	0x04	Read Input Registers (FC 04)
5	0x05	Write Single Coil (FC 05)
6	0x06	Write Single Holding Register (FC 06)
15	0x0F	Write Multiple Coils (FC 15)
16	0x10	Write Multiple Holding Registers (FC 16)
22	0x16	Mask Write Holding Register (FC 22)
23	0x17	Read/Write Multiple Holding Registers (FC 23)

Table 89: MODBUS Functions Supported by Nexto CPUs

Polling: this parameter indicates how often the communication set for this request must be performed. By the end of a communication will be awaited a time equal to the value configured in the field polling and after that, a new communication will be executed.

Read Data Start Address: field for the initial address of the MODBUS read data.

Read Data Size: the minimum value for the read data size is 1 and the maximum value depends on the MODBUS function (FC) used as below:

- Read Coils (FC 01): 2000
- Read Input Status (FC 02): 2000
- Read Holding Registers (FC 03): 125
- Read Input Registers (FC 04): 125
- Read/Write Multiple Registers (FC 23): 121

Read Data Range: this field shows the MODBUS read data range configured for each request. The initial address, along with the read data size will result in the range of read data for each request.

Write Data Start Address: field for the initial address of the MODBUS write data.

Write Data Size: the minimum value for the write data size is 1 and the maximum value depends on the MODBUS function (FC) used as below:

- Write Single Coil (FC 05): 1
- Write Single Register (FC 06): 1
- Write Multiple Coils (FC 15): 1968
- Write Multiple Registers (FC 16): 123
- Mask Write Register (FC 22): 1
- Read/Write Multiple Registers (FC 23): 121

Write Data Range: this field shows the MODBUS write data range configured for each request. The initial address, along with the read data size will result in the range of write data for each request.

Diagnostic Variable: The MODBUS request diagnostics configured by symbolic mapping or by direct representation, are stored in variables of type *T_DIAG_MODBUS_RTU_MAPPING_1* for Master devices and *T_DIAG_MODBUS_ETH_CLIENT_1* for Client devices and the mapping by direct representation are in 4-byte and 2-word, which are described in Table 90.

<i>T_DIAG_MODBUS_RTU_MAPPING_1.*</i>	Size	Description
Communication Status Bits:		
byStatus.bCommIdle	BIT	Communication idle (waiting to be executed).
byStatus.bCommExecuting	BIT	Active communication.
byStatus.bCommPostponed	BIT	Communication deferred, because the maximum number of concurrent requests was reached. Deferred communications will be carried out in the same sequence in which they were ordered to avoid indeterminacy. The time spent in this State is not counted for the purposes of time-out. The bCommIdle and bCommExecuting bits are false when the bCommPostponed bit is true.
byStatus.bCommDisabled	BIT	Communication disabled. The bCommIdle bit is restarted in this condition.

T_DIAG_MODBUS_RTU_MAPPING_1.*	Size	Description
byStatus.bCommOk	BIT	Communication terminated previously was held successfully.
byStatus.bCommError	BIT	Communication terminated previously had an error. Check error code.
Last error code (enabled when bCommError = true):		
eLastErrorCode	MASTER_ERROR_CODE (BYTE)	Informs the possible cause of the last error in the MODBUS mapping. Consult Table 113 for further details.
Last exception code received by master:		
eLastExceptionCode	MODBUS_EXCEPTION (BYTE)	NO_EXCEPTION (0) FUNCTION_NOT_SUPPORTED (1) MAPPING_NOT_FOUND (2) ILLEGAL_VALUE (3) ACCESS_DENIED (128)* MAPPING_DISABLED (129)* IGNORE_FRAME (255)*
Communication statistics:		
wCommCounter	WORD	Communications counter terminated, with or without errors. The user can test when communication has finished testing the variation of this counter. When the value 65535 is reached, the counter returns to zero.
wCommErrorCounter	WORD	Communications counter terminated with errors. When the value 65535 is reached, the counter returns to zero.

Table 90: MODBUS RTU Relations Diagnostics

Notes:

Exception Codes: The exception codes presented in this field are values returned by the slave. The definitions of the exception codes 128, 129 and 255 presented in the table are valid only when using Altus slaves. Slaves from other manufacturers might use other definitions for each code.

Disabling Variable: variable of Boolean type used to disable, individually, MODBUS requests configured on request tab via button at the bottom of the window. The request is disabled when the variable, corresponding to the request, is equal to 1, otherwise the request is enabled.

Last Error Code: The codes for the possible situations that cause an error in the MODBUS communication can be consulted below:

Code	Enumerable	Description
1	ERR_EXCEPTION	Reply is in an exception code (see eLastExceptionCode = Exception Code).
2	ERR_CRC	Reply with invalid CRC.
3	ERR_ADDRESS	MODBUS address not found. The address that replied the request was different than expected.
4	ERR_FUNCTION	Invalid function code. The reply's function code was different than expected.
5	ERR_FRAME_DATA_COUNT	The amount of data in the reply was different than expected.
7	ERR_NOT_ECHO	The reply is not an echo of the request (FC 05 and 06).
8	ERR_REFERENCE_NUMBER	Invalid reference number (FC 15 and 16).
9	ERR_INVALID_FRAME_SIZE	Reply shorter than expected.
20	ERR_CONNECTION	Error while establishing connection.
21	ERR_SEND	Error during transmission stage.
22	ERR_RECEIVE	Error during reception stage.
40	ERR_CONNECTION_TIMEOUT	Application level time-out during connection.
41	ERR_SEND_TIMEOUT	Application level time-out during transmission.
42	ERR_RECEIVE_TIMEOUT	Application level time-out while waiting for reply.
43	ERR_CTS_OFF_TIMEOUT	Time-out while waiting CTS = false in transmission.
44	ERR_CTS_ON_TIMEOUT	Time-out while waiting CTS = true in transmission.
128	NO_ERROR	No error since startup.

Table 91: MODBUS Relations Error Codes

ATTENTION

Differently from other application tasks, when a deprecation mark in the MainTask is reached, the task of a Master MODBUS RTU instance and any other MODBUS task will stop running at the moment that it tries to perform a writing in a memory area. It occurs in order to keep the consistency of the memory areas data while a MainTask is not running.

5.8.5.2. MODBUS Master Protocol Configuration for Direct Representation (%Q)

To configure this protocol using direct representation (%Q), the following steps must be performed:

- Configure the general parameters of the MODBUS protocol, such as: communication times and direct representation variables (%Q) to receive diagnostics.
- Add and configure devices by setting address, direct representation variables (%Q) to disable the relations, communication time-outs, etc.
- Add and configure MODBUS relations, specifying the data type and MODBUS function, time-outs, direct representation variables (%Q) to receive diagnostics of the relation and other to receive/write the data, amount of data to be transmitted and relation polling.

The descriptions of each configuration are listed below in this section.

5.8.5.2.1. General Parameters of MODBUS Master Protocol - setting by Direct Representation(%Q)

The General parameters, found on the home screen of MODBUS protocol configuration (figure below), are defined as:

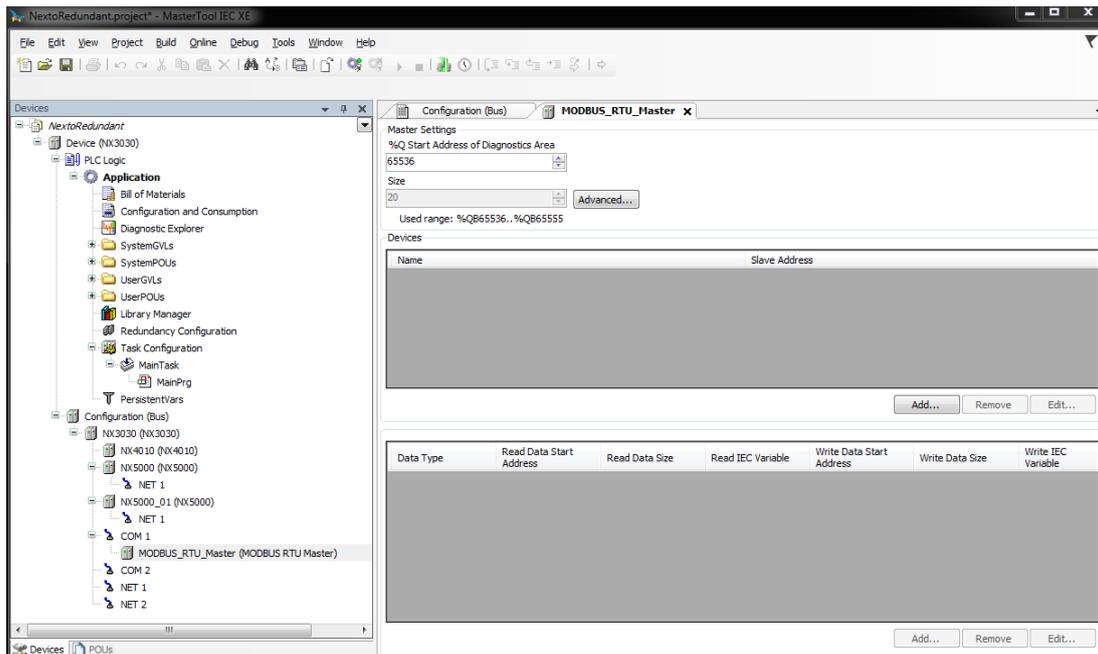


Figure 74: MODBUS RTU Master Setup Screen

Direct representation variables (%Q) for the protocol diagnostic:

Configuration	Description	Default Value	Options
%Q Start Address of Diagnostics Area	Initial address of the diagnostic variables	-	0 to 2147483628
Size	Size of diagnostics area	20	Disabled for editing

Table 92: MODBUS RTU Master Configuration

Notes:

Initial Address of Diagnostics in %Q: this field is limited by the size of outputs variables (%Q) addressable memory of each CPU, which can be found in section [Memory](#).

Default Value: the factory default value cannot be set to the *%Q Start Address of Diagnostics Area* field, because the creation of a Protocol instance may be held at any time on application development. The MasterTool IEC XE software itself allocate a value, from the range of output variables of direct representation (%Q), not used yet.

The diagnostics and MODBUS protocol commands are described in Table 84.

The communication times of the MODBUS Master protocol, found on the button *Advanced...* in the configuration screen are divided into *Send Delay* and *Minimum Interframe*, further details are described in section [MODBUS Master Protocol General Parameters – Symbolic Mapping Configuration](#).

5.8.5.2.2. *Devices Configuration – Configuration for Direct Representation (%Q)*

The configuration of the devices, viewed in figure below, comprises the following parameters:

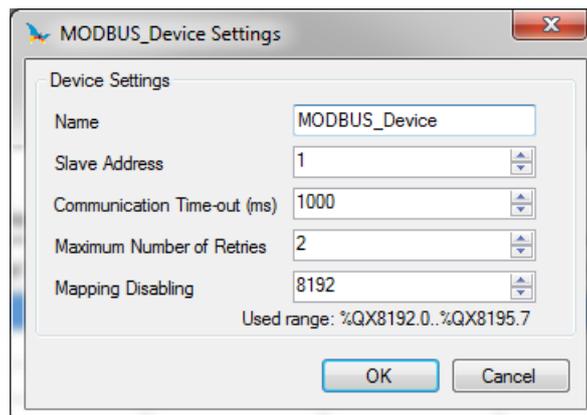


Figure 75: Device Configuration

Configuration	Description	Default Value	Options
Name	Name of the instance	MODBUS_Device	Identifier, according to IEC 61131-3
Slave Address	The MODBUS slave address	1	0 to 255
Communication Time-out (ms)	Sets the time-out of the application level	1000	10 to 65535
Maximum Number of Retries	Sets the number of retries before reporting a communication error	2	0 to 9
Mapping Disabling	Initial address used to disable MODBUS relations	-	0 to 2147483644

Table 93: Device Configuration - MODBUS Master

Notes:

Instance Name: this field is the identifier of the device, which is checked according to IEC 61131-3, i.e. does not allow spaces, special characters and start with numeral character. It's limited in 24 characters.

Mapping Disabling: composed of 32 bits, used to disable, individually, the 32 MODBUS relations configured in *Device Mappings* space. The relation is disabled when the bit, corresponding to relation, is equal to 1, otherwise, the mapping is enabled. This field is limited by the size of outputs variables (%Q) addressable memory of each CPU, which can be found in section [Memory](#).

Default Value: the factory default value cannot be set to the *Mapping Disabling* field, because the creation of a Protocol instance may be held at any time on application development. The MasterTool IEC XE software itself allocate a value, from the range of output variables of direct representation (%Q), not used yet.

For further details on the *Slave Address*, *Communication Time-out* and *Maximum Number of Retries* parameters see notes in section [Devices Configuration – Symbolic Mapping configuration](#).

5.8.5.2.3. *Mappings Configuration – Configuration for Direct Representation (%Q)*

The MODBUS relations settings, viewed in the figures below, follow the parameters described in table below:

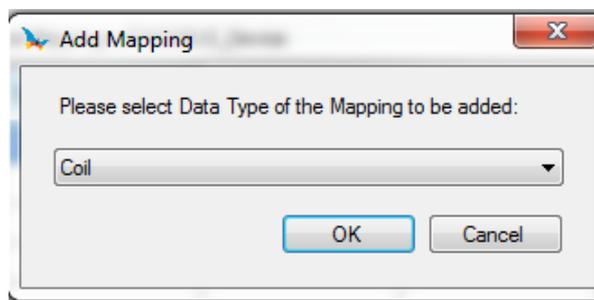


Figure 76: MODBUS Data Type

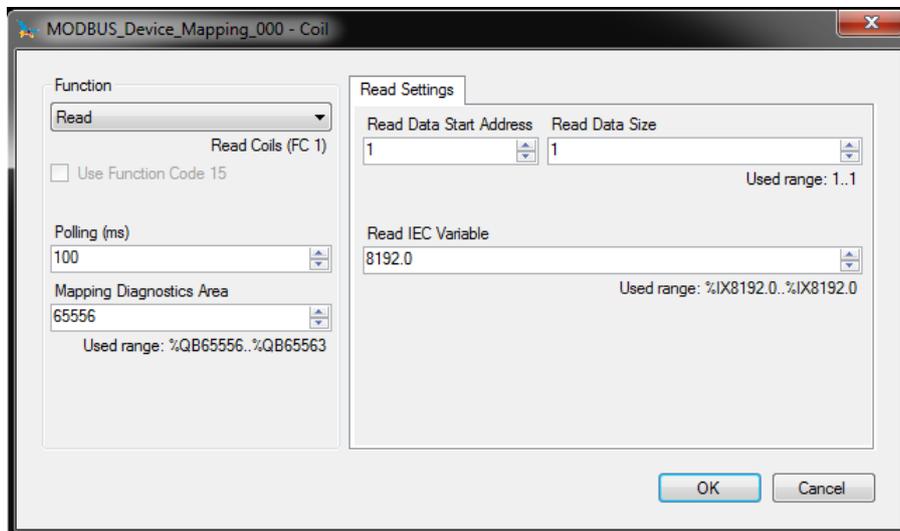


Figure 77: MODBUS Function

In table below, the number of factory default settings and the values for the column Options, may vary according to the data type and MODBUS function (FC).

Configuration	Description	Default Value	Options
Function	MODBUS function type	Read	Read Write Read/Write Mask Write
Polling (ms)	Communication period (ms)	100	0 to 3600000

Configuration	Description	Default Value	Options
Mapping Diagnostics Area	Initial address of the MODBUS relation diagnostics (%Q)	-	0 to 2147483640
Read Data Start Address	Initial address of the MODBUS read data	1	1 to 65536
Read Data Size	Number of MODBUS read data	-	Depends on the function used
Read IEC Variable	Initial address of the read variables (%I)	-	0 to 2147483646
Write Data Start Address	Initial address of the MODBUS write data	1	1 to 65536
Write Data Size	Number of MODBUS write data	-	Depends on the function used
Write IEC Variable	Initial address of the write variables (%Q)	-	0 to 2147483647
Mask Write IEC Variables	Initial address of the variables for the write mask (%Q)	-	0 to 2147483644

Table 94: Device Mapping

Notes:

Function: the available data types are detailed in the Table 113 and MODBUS functions (FC) are available in the Table 111.

Polling: this parameter indicates how often the communication set for this relation must be executed. At the end of communication will be awaited a time equal to the configured polling and after, will be performed a new communication as soon as possible.

Mapping Diagnostics Area: this field is limited by the size of output variables addressable memory (%Q) at CPU, which can be found in the section [Memory](#). The configured MODBUS relations diagnostics are described in Table 90.

Read/Write Data Size: details of the data size supported by each function are described in the notes of the section [Requests Configuration – Symbolic Mapping Settings](#).

ATTENTION

When accessing the communication data memory is between devices with different endianness (Little-Endian and Big-Endian), inversion of the read/write data may occur. In this case, the user must adjust the data in the application.

Read IEC Variable: if the MODBUS data type is *Coil* or *Input Status* (bit), the initial address of the IEC reading variables will have the format %IX10.1, for example. However, if the MODBUS data type is *Holding Register* or *Input Register* (16 bits), the initial address of the IEC reading variables will be %IW. This field is limited by the size of input variables addressable memory (%I) at CPU, which can be found in the section [Memory](#).

Write IEC Variable: if the MODBUS data type is *Coil*, the initial address of the IEC writing variables will have the format %QX10.1, for example. However, if the MODBUS data type is *Holding Register* (16 bits), the initial address of the IEC writing variables will be %QW. This field is limited by the size of output variables addressable memory (%Q) at CPU, which can be found in the section [Memory](#).

Write Mask: the function *Mask Write* (FC 22), employs a logic between the value already written and the two words that are configured in this field using %QW(0) for the AND mask and %QW(2) for the OR mask; allowing the user to handle the word. This field is limited by the size of output variables addressable memory (%Q) of each CPU, which can be found in the section [Memory](#).

Default Value: the factory default value cannot be set for the *Mapping Diagnostics Area*, *Read IEC Variable*, *Write IEC Variable* and *Mask Write IEC Variables* fields, since the creation of a relation can be performed at any time on application development. The MasterTool IEC XE software itself allocate a value from the range of direct representation output variables (%Q), still unused. Factory default cannot be set to the *Read/Write Data Size* fields, as they will vary according to the MODBUS data type selected.

ATTENTION

Unlike other tasks of an application, when a mark is reached at MainTask debugging, the MODBUS RTU Master instance task or any other MODBUS task will stop being executed at the moment it tries to write in the memory area. This occurs in order to maintain data consistency of memory areas while MainTask is not running.

5.8.6. MODBUS RTU Slave

This protocol is available for the Nexto Series on its serial channels. At selecting this option in MasterTool IEC XE, the CPU becomes a MODBUS communication slave, allowing the connection with MODBUS RTU master devices.

There are two ways to configure this protocol. The first one makes use of direct representation (%Q), in which the variables are defined by your address. The second one, through symbolic mapping, where the variables are defined by your name.

Independent of the configuration mode, the steps to insert an instance of the protocol and configure the serial interface are equal. The procedure to insert an instance of the protocol is found in detail in the MasterTool IEC XE User Manual - MU299609. The remaining configuration steps are described below for each mode:

- Add the MODBUS RTU Slave Protocol instance to the serial channel COM 1 or COM 2 (or both, in cases of two communication networks). To execute this procedure see [Inserting a Protocol Instance](#) section.
- Configure the serial interface, choosing the communication speed, the RTS/CTS signals behavior, the parity, the stop bits channel, among others. See [Serial Interfaces Configuration](#) section.

5.8.6.1. MODBUS Slave Protocol Configuration via Symbolic Mapping

To configure this protocol using symbolic mapping, you must perform the following steps:

- Configure the MODBUS slave protocol general parameters, as: slave address and communication times (available at the Slave advanced configurations button).
- Add and configure MODBUS relations, specifying the variable name, MODBUS data type and data initial address. Automatically, the data size and range will be filled, in accordance to the variable type declared.

5.8.6.1.1. MODBUS Slave Protocol General Parameters – Configuration via Symbolic Mapping

The general parameters, found on the MODBUS protocol initial screen (figure below), are defined as.

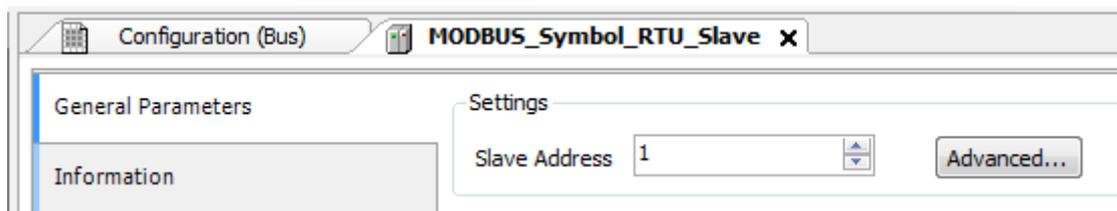


Figure 78: MODBUS RTU Slave Configuration Screen

Configuration	Description	Default	Options
Slave Address	MODBUS slave address	1	1 to 255

Table 95: Slave Configurations

The MODBUS slave protocol communication times, found in the *Advanced...* button on the configuration screen, are divided in: *Task Cycle*, *Send Delay* and *Minimum Interframe* as shown in figure below and in table below.

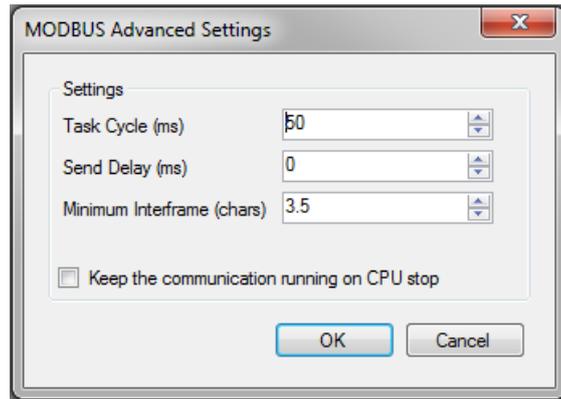


Figure 79: Modbus Slave Advanced Configurations

Configuration	Description	Default	Options
Task Cycle (ms)	Time for the instance execution within the cycle, without considering its own execution time	50	20 to 100
Send Delay (ms)	Delay for the transmission response	0	0 to 65535
Minimum Interframe (chars)	Minimum silence time between different frames	3.5	3.5 to 100.0
Keep the communication running on CPU stop	Enable the MODBUS Symbol Slave to run while the CPU is in STOP or standing in a breakpoint	Unchecked	Checked or unchecked

Table 96: Modbus Slave Advanced Configurations

Notes:

Task Cycle: the user will have to be careful when changing this parameter as it interferes directly in the answer time, data volume for scan and mainly in the CPU resources balance between communications and other tasks.

Send Delay: the answer to a MODBUS protocol may cause problems in certain moments, as in the RS-485 interface or other half-duplex. Sometimes there is a delay between the time of the request from the master and the silence on the physical line (slave delay to put RTS in zero and put the RS-485 in high impedance state). To solve this problem, the master can wait the determined time in this field before sending the new request. On the opposite case, the first bytes transmitted by the master could be lost.

Minimum Interframe: the MODBUS standard defines this time as 3.5 characters, but this parameter is configurable in order to attend the devices which don't follow the standard.

The MODBUS Slave protocol diagnostics and commands configured, either by symbolic mapping or direct representation, are stored in *T_DIAG_MODBUS_RTU_SLAVE_1* variables. For the direct representation mapping, they are also in 4 bytes and 8 words which are described in table below:

T_DIAG_MODBUS_RTU_SLAVE_1.*	Size	Description
Diagnostic Bits:		
tDiag.bRunning	BIT	The slave is in execution mode.
tDiag.bNotRunning	BIT	The slave is not in execution (see bit: bInterruptedByCommand).
tDiag.bInterruptedByCommand	BIT	The bit bNotRunning was enabled as the slave was interrupted by the user through command bits.
tDiag.bConfigFailure	BIT	Configuration failure.
tDiag.bModuleFailure	BIT	Not implemented.
Error codes:		
		0: there are no errors 1: invalid serial port 2: invalid serial port mode 3: invalid baud rate 4: invalid data bits 5: invalid parity

T_DIAG_MODBUS_RTU_SLAVE_1.*	Size	Description
eErrorCode	SERIAL_STATUS (BYTE)	6: invalid stop bits 7: invalid modem signal parameter 8: invalid UART RX Threshold parameter 9: invalid time-out parameter 10: busy serial port 11: UART hardware error 12: remote hardware error 20: invalid transmission buffer size 21: invalid signal modem method 22: CTS time-out = true 23: CTS time-out = false 24: transmission time-out error 30: invalid reception buffer size 31: reception time-out error 32: flow control configured differently from manual 33: invalid flow control for the configured serial port 34: data reception not allowed in normal mode 35: data reception not allowed in extended mode 36: DCD interruption not allowed 37: CTS interruption not allowed 38: DSR interruption not allowed 39: serial port not configured 50: internal error in the serial port
Command bits, automatically initialized:		
tCommand.bStop	BIT	Stop slave.
tCommand.bRestart	BIT	Restart slave.
tCommand.bResetCounter	BIT	Restart diagnostics statistics (counters).
Communication Statistics:		
tStat.wRXRequests	WORD	Counter of normal requests received by the slave and answered normally. In case of a broadcast command, this counter is incremented, but it is not transmitted (0 to 65535).
tStat.wTXExceptionResponses	WORD	Counter of normal requests received by the slave and answered with exception code. In case of a broadcast command, this counter is incremented, but it isn't transmitted (0 to 65535).
tStat.wRXFrames	WORD	Counter of frames received by the slave. It's considered a frame something which is processed and it is followed by a Minimum Interframe Silence, in other words, an illegal message is also computed (0 to 65535).
tStat.wRXIllegalRequests	WORD	Illegal request counter. These are frames which start with address 0 (broadcast) or with the MODBUS slave address, but aren't legal requests – invalid syntax, smaller frames, invalid CRC – (0 to 65535).
tStat.wRXOverrunErrors	WORD	Counter of frames with overrun errors during reception – UART FIFO or RX line – (0 to 65535).
tStat.wRXIncompleteFrames	WORD	Counter of frames with construction errors, parity or failure during reception (0 to 65535).
tStat.wCTSTimeOutErrors	WORD	Counter of CTS time-out error, using the RTS/CTS handshake, during the transmission (0 to 65535).

Table 97: MODBUS RTU Slave Diagnostic

Note:

Counters: all MODBUS RTU Slave diagnostics counters return to zero when the limit value 65535 is exceeded.

5.8.6.1.2. Configuration of the Relations – Symbolic Mapping Setting

The MODBUS relations configuration, showed on figure below, follows the parameters described on table below:

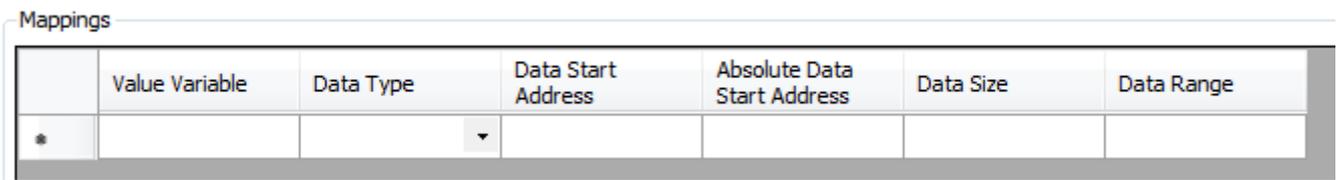


Figure 80: MODBUS Data Mappings Screen

Configuration	Description	Default	Options
Value Variable	Symbolic variable name	-	Name of a variable declared in a program or GVL
Data Type	MODBUS data type	-	Coil Input Status Holding Register Input Register
Data Start Address	MODBUS data initial address	-	1 to 65536
Absolute Data Start Address	Absolute initial address of MODBUS data according to its type	-	-
Data Size	MODBUS data size	-	1 to 65536
Data Range	Data address range configured	-	-

Table 98: MODBUS Mappings Configurations

Notes:

Value Variable: this field is used to specify a symbolic variable in MODBUS relation.

Data Type: this field is used to specify the data type used in the MODBUS relation.

Data Type	Size [bits]	Description
Coil	1	Digital output that can be read or written.
Input Status	1	Digital input (read only).
Holding Register	16	Analog output that can be read or written.
Input Register	16	Analog input (read only).

Table 99: MODBUS data types supported by Nexto CPUs

Data Start Address: data initial address of the MODBUS relation.

Data Size: the Data Size value sets the maximum amount of data that a MODBUS relation can access from the initial address. Thus, in order to read a continuous range of addresses, it is necessary that all addresses are declared in a single relation. This field varies according to the configured type of MODBUS data.

Data Range: this field shows the user the memory address range used by the MODBUS relation.

ATTENTION

Differently from other application tasks, when a deuration mark in the MainTask is reached, the task of a MODBUS RTU Slave instance and any other MODBUS task will stop running at the moment that it tries to perform a writing in a memory area. It occurs in order to keep the consistency of the memory areas data while a MainTask is not running.

5.8.6.2. MODBUS Slave Protocol Configuration via Direct Representation (%Q)

To configure this protocol using Direct Representation (%Q), you must perform the following steps:

- Configure the general parameters of MODBUS slave protocol, such as: communication times, address and direct representation variables (%Q) to receive diagnostics and control relations.
- Add and configure MODBUS relations, specifying the MODBUS data type, direct representation variables (%Q) to receive/write the data and amount of data to communicate.

The descriptions of each setting are listed below, in this section.

5.8.6.2.1. General Parameters of MODBUS Slave Protocol – Configuration via Direct Representation (%Q)

The general parameters, found on the home screen of MODBUS protocol configuration (figure below), are defined as:

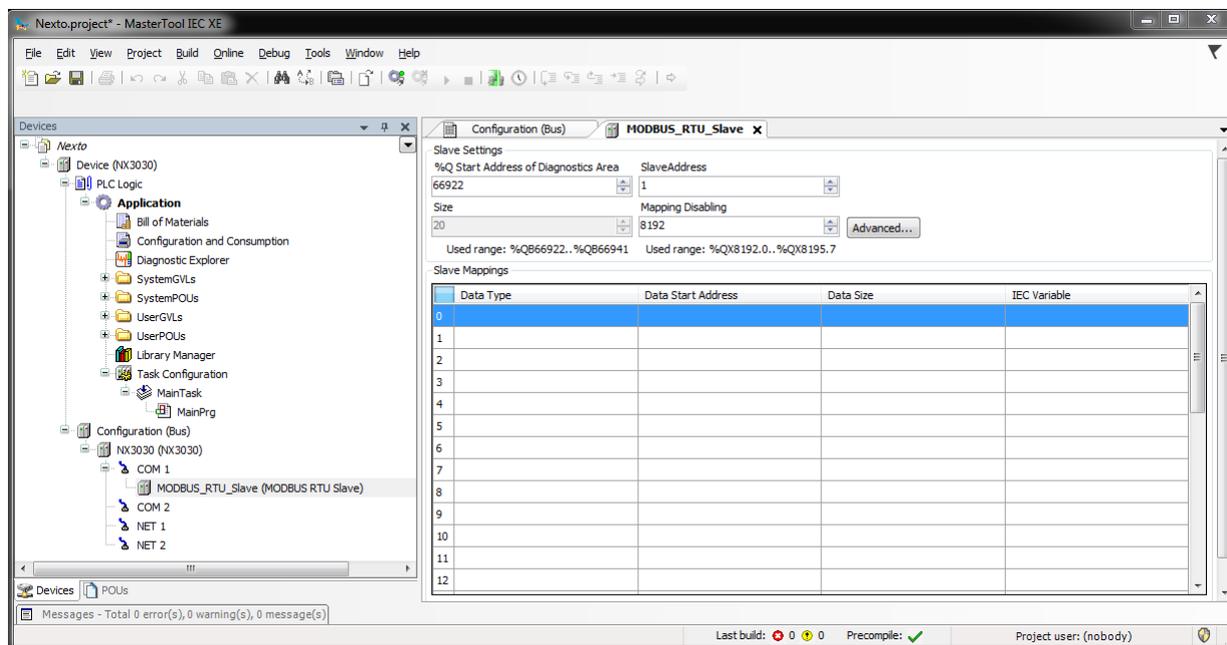


Figure 81: MODBUS RTU Slave Configuration Screen by Direct Representation

Address and direct representation variables (%Q) to control relations and diagnostics:

Configuration	Description	Default Value	Options
%Q Start Address of Diagnostics Area	Initial address of the diagnostic variables	-	0 to 2147483628
Size	Size of diagnostics area	-	Disabled for editing
Slave Address	MODBUS slave address	1	1 to 255
Mapping Disabling	Initial address used to disable MODBUS relations	-	0 to 2147483644

Table 100: Address and Direct Representation Variables Settings

Notes:

%Q Start Address of Diagnostics Area: this field is limited by the size of output variables addressable memory (%Q) of each CPU, which can be found in section [Memory](#).

Slave Address: it is important to note that the Slave accepts requests broadcast, when the master sends a command with the address set to zero. Moreover, in accordance with standard MODBUS, the valid address range for slaves is 1 to 247. The addresses 248 to 255 are reserved.

Mapping Disabling: composed of 32 bits, used to disable, individually, the 32 MODBUS relations configured in *Slave Mappings* space. The relation is disabled when the corresponding bit is equal to 1, otherwise, the mapping is enabled. This field is limited by the size of output variables addressable memory (%Q) of each CPU, which can be found on [Memory](#) section.

Default Value: the factory default value cannot be set for the *%Q Start Address of Diagnostics Area* and *Mapping Disabling* fields, since the creation of a relation can be performed at any time on application development. The MasterTool IEC XE software itself allocate a value from the range of direct representation output variables (%Q), still unused.

The MODBUS Slave by Direct Representation protocol stops communicating while the CPU is in STOP or stopped at a breakpoint.

The MODBUS protocol diagnostics and commands are described in the [Table 97](#).

The communication times of the MODBUS Slave protocol, found on the button *Advanced...* of the configuration screen, are described in [Table 96](#).

5.8.6.2.2. Mappings Configuration – Configuration via Direct Representation (%Q)

The MODBUS relations settings, viewed in the figures below, follow the parameters described in table below:

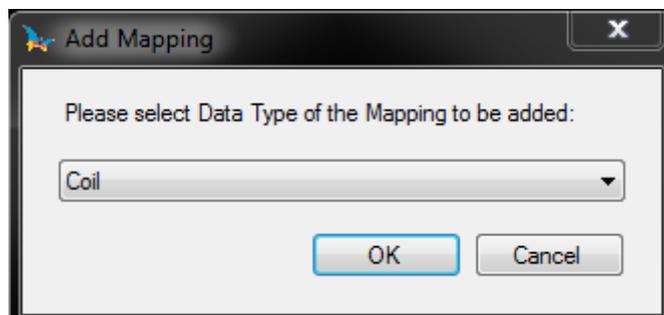


Figure 82: Adding MODBUS Relations

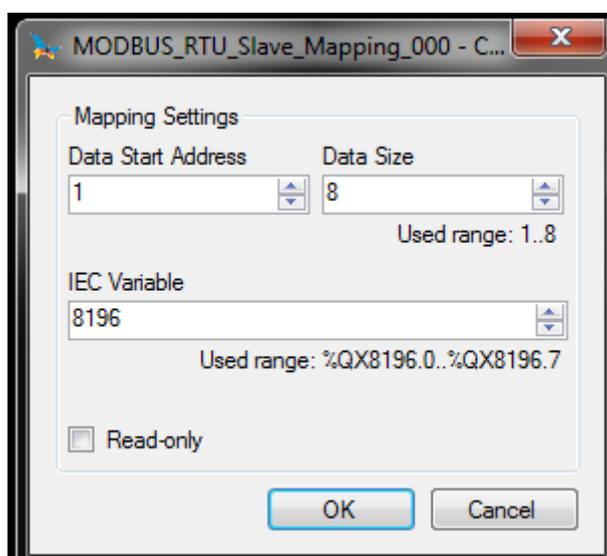


Figure 83: Configuring the MODBUS Relation

Configuration	Description	Default Value	Options
Data Type	MODBUS data type	Coil	Coil (1 bit) Holding Register (16 bits) Input Register (16 bits) Input Status (1 bit)
Data Start Address	Initial address of the MODBUS data	1	1 to 65536
Data Size	Number of MODBUS data	-	1 to 65536
IEC Variable	Initial address of variables (%Q)	-	0 to 2147483647
Read-only	Only allows reading	Disabled	Enabled or disabled

Table 101: Slave Mappings

Notes:

Options: the values written in the column *Options* may vary according with the configured MODBUS data.

Data Size: the value of *Data Size* defines the maximum amount of data that a MODBUS relation can access, from the initial address. Thus, to read a continuous address range, it is necessary that all addresses are declared in a single interface. This field varies with the MODBUS data type configured, i.e. when selected *Coil* or *Input Status*, the *Data Size* field must be a multiple of eight. Also, the maximum amount must not exceed the size of output addressable memory and not assign the same values used in the application.

ATTENTION

When accessing the communication data memory is between devices with different endianness (Little-Endian and Big-Endian), inversion of the read/write data may occur. In this case, the user must adjust the data in the application.

IEC Variable: in case the MODBUS data type is *Coil* or *Input Status* (bit), the IEC variables initial address will be in the format *%QX10.I*. However, if the MODBUS data type is *Holding Register* or *Input Register* (16 bits), the IEC variables initial address will be in the format *%QW*. This field is limited by the memory size of the addressable output variables (*%Q*) from each CPU, which can be seen on [Memory](#) section.

Read-only: when enabled, it only allows the communication master to read the variable data. It does not allow the writing. This option is valid for the writing functions only.

Default Value: the default value cannot be defined for the *IEC Variable* field since the creation of a relation can be performed at any time on application development. The MasterTool IEC XE software itself allocate a value from the range of direct representation output variables (*%Q*), still unused. The default cannot be defined for the *Data Size* field as it will vary according to selected MODBUS data type.

In the previously defined relations, the maximum MODBUS data size can be 65535 (maximum value configured in the *Data Size* field). However, the request which arrives in the MODBUS RTU Slave must address a subgroup of this mapping and this group must have, at most, the data size depending on the function code which is defined below:

- Read Coils (FC 1): 2000
- Read Input Status (FC 2): 2000
- Read Holding Registers (FC 3): 125
- Read Input Registers (FC 4): 125
- Write Single Coil (FC 5): 1
- Write Single Holding register (FC 6): 1
- Force Multiple Coils (FC 15): 1968
- Write Holding Registers (FC 16): 123
- Mask Write Register (FC 22): 1
- Read/Write Holding Registers (FC 23):
 - Read: 121
 - Write: 121

ATTENTION

Differently from other application tasks, when a deuration mark in the MainTask is reached, the task of a Slave MODBUS RTU instance and any other MODBUS task will stop running at the moment that it tries to perform a writing in a memory area. It occurs in order to keep the consistency of the memory areas data while a MainTask is not running.

5.8.7. MODBUS Ethernet

The multi-master communication allows the Nexto CPUs to read or write MODBUS variables in other controllers or HMIs compatible with the MODBUS TCP protocol or MODBUS RTU via TCP. The Nexto CPU can, at the same time, be client and server in the same communication network, or even have more instances associated to the Ethernet interface. It does not matter if they are MODBUS TCP or MODBUS RTU via TCP, as described on [Table 5.8](#).

The figure below represents some of the communication possibilities using the MODBUS TCP protocol simultaneously with the MODBUS RTU via TCP protocol.

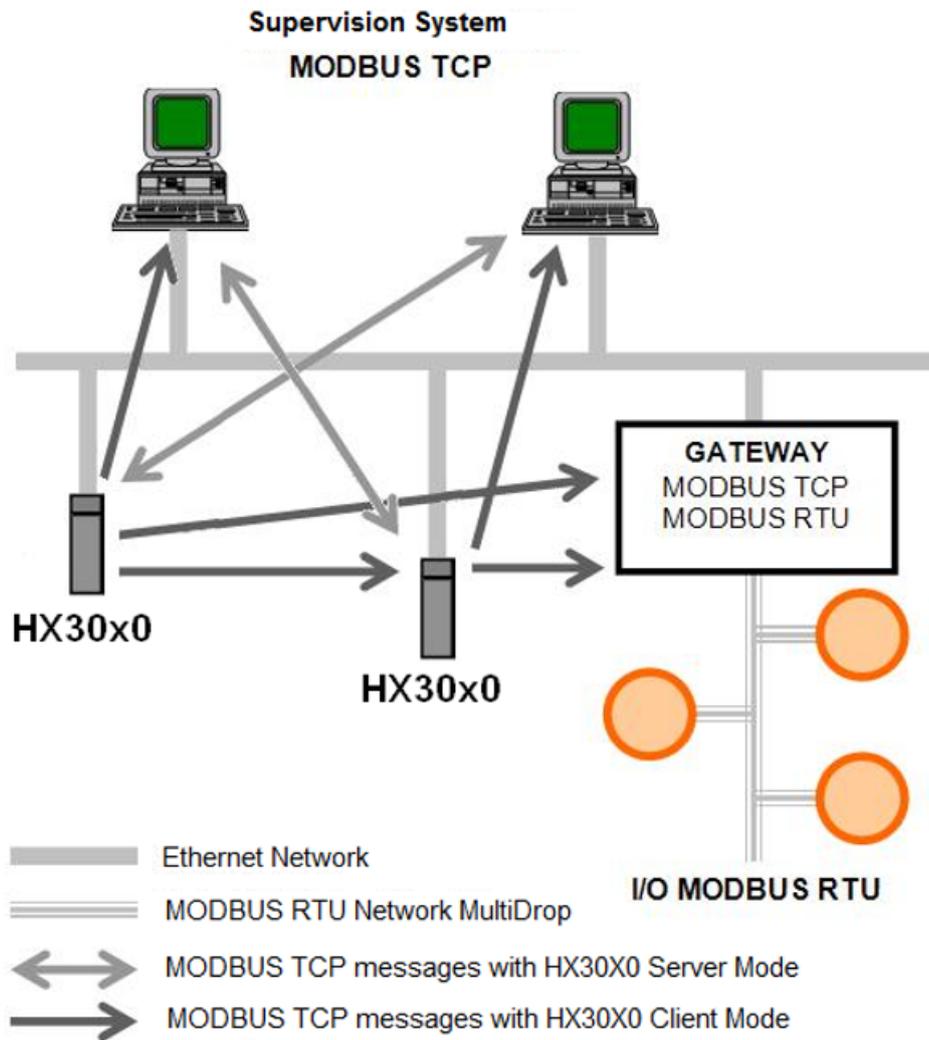


Figure 84: MODBUS TCP Communication Network

The association of MODBUS variables with CPU symbolic variables is made by the user through relations definition via MasterTool IEC XE configuration tool. It's possible to configure up to 32 relations for the server mode and up to 128 relations for the client mode. The relations in client mode, on the other hand, must respect the data maximum size of a MODBUS function: 125 registers (input registers or holding registers) or 2000 bits (coils or input status). This information is detailed in the description of each protocol.

All relations, in client mode or server mode, can be disabled through direct representation variables (%Q) identified as Disabling Variables by MasterTool IEC XE. The disabling may occur through general bits which affect all relations of an operation mode, or through specific bits, affecting specific relations.

For the server mode relations, IP addresses clusters can be defined with writing and reading allowance, called filters. This is made through the definition of an IP network address and of a subnet mask, resulting in a group of client IPs which can read and write in the relation variables. Reading/writing functions are filtered, in other words, they cannot be requested by any client, independent from the IP address. This information is detailed in the MODBUS Ethernet Server protocol.

When the MODBUS TCP protocol is used in the client mode, it's possible to use the multiple requests feature, with the same TCP connection to accelerate the communication with the servers. When this feature isn't desired or isn't supported by the server, it can be disabled (relation level action). It is important to emphasize that the maximum number of TCP connections between the client and server is 63. If some parameters are changed, inactive communications can be closed, which allows the opening of new connections.

The tables below bring, respectively, the complete list of data and MODBUS functions supported by the Nexto CPUs.

Data Type	Size [bits]	Description
Coil	1	Digital output that can be read or written.
Input Status	1	Digital input (read only).
Holding Register	16	Analog output that can be read or written.
Input Register	16	Analog input (read only).

Table 102: MODBUS data types supported by Nexto CPUs

Code		Description
DEC	HEX	
1	0x01	Read Coils (FC 01)
2	0x02	Read Input Status (FC 02)
3	0x03	Read Holding Registers (FC 03)
4	0x04	Read Input Registers (FC 04)
5	0x05	Write Single Coil (FC 05)
6	0x06	Write Single Holding Register (FC 06)
15	0x0F	Write Multiple Coils (FC 15)
16	0x10	Write Multiple Holding Registers (FC 16)
22	0x16	Mask Write Holding Register (FC 22)
23	0x17	Read/Write Multiple Holding Registers (FC 23)

Table 103: MODBUS Functions Supported by Nexto CPUs

Independent of the configuration mode, the steps to insert an instance of the protocol and configure the Ethernet interface are equal. The remaining configuration steps are described below for each modality.

- Add one or more instances of the MODBUS Ethernet client or server protocol to Ethernet channel. To perform this procedure, refer to the section [Inserting a Protocol Instance](#).
- Configure the Ethernet interface. To perform this procedure, see section [Ethernet Interfaces Configuration](#).

5.8.8. MODBUS Ethernet Client

This protocol is available for all Nexto Series CPUs on its Ethernet channels. When selecting this option at MasterTool IEC XE, the CPU becomes a MODBUS communication client, allowing the access to other devices with the same protocol, when it's in execution mode (*Run Mode*).

There are two ways to configure this protocol. The first one makes use of *direct representation (%Q)*, in which the variables are defined by your address. The second one, through *symbolic mapping*, where the variables are defined by your name.

The procedure to insert an instance of the protocol is found in detail in the MasterTool IEC XE User Manual – MU299609 or on [Inserting a Protocol Instance](#) section.

5.8.8.1. MODBUS Ethernet Client Configuration via Symbolic Mapping

To configure this protocol using *Symbolic Mapping*, it's necessary to execute the following steps:

- Configure the general parameters of MODBUS protocol client, with the Transmission Control Protocol (TCP) or RTU via TCP.
- Add and configure devices by setting IP address, port, address of the slave and time-out of communication (available on the Advanced Settings button of the device).
- Add and configure the MODBUS mappings, specifying the variable name, data type, data initial address, data size and variable that will receive the quality data.
- Add and configure the MODBUS request, specifying the desired function, the scan time of the request, the initial address (read/write), the size of the data (read/write), the variable that will receive the data quality and the variable responsible for disabling the request.

5.8.8.1.1. MODBUS Client Protocol General Parameters – Configuration via Symbolic Mapping

The general parameters, found on the MODBUS protocol configuration initial screen (figure below), are defined as:

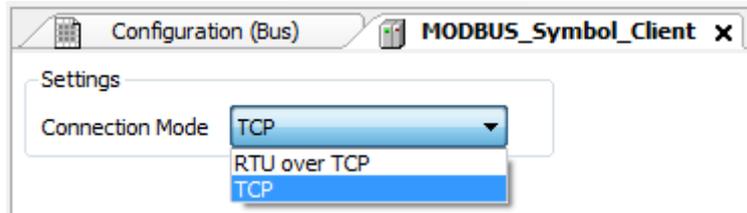


Figure 85: MODBUS Client General Parameters Configuration Screen

Configuration	Description	Default	Options
Connection Mode	Protocol selection	TCP	RTU via TCP TCP

Table 104: MODBUS Client General Configurations

The MODBUS Client protocol diagnostics and commands configured, either by symbolic mapping or direct representation, are stored in *T_DIAG_MODBUS_ETH_CLIENT_1* variables. For the direct representation mapping, they are also in 4 bytes and 8 words which are described in table below:

T_DIAG_MODBUS_ETH_CLIENT_1.*	Size	Description
Diagnostic Bits:		
tDiag.bRunning	BIT	The client is in execution mode.
tDiag.bNotRunning	BIT	The client is not in execution mode (see bit bInterruptedByCommand).
tDiag.bInterruptedByCommand	BIT	The bit bNotRunning was enabled, as the client was interrupted by the user through command bits.
tDiag.bConfigFailure	BIT	Configuration failure.
tDiag.bModuleFailure	BIT	Indicates if there is failure in the module or the module is not present.
tDiag.bAllDevicesCommFailure	BIT	Indicates that all devices configured in the Client are in failure.
Command bits, automatically initialized:		
tCommand.bStop	BIT	Stop client.
tCommand.bRestart	BIT	Restart client.
tCommand.bResetCounter	BIT	Restart the diagnostic statistics (counters).
Communication Statistics:		
tStat.wTXRequests	WORD	Counter of number of requests transmitted by the client (0 to 65535).
tStat.wRXNormalResponses	WORD	Counter of normal answers received by the client (0 to 65535).
tStat.wRXExceptionResponses	WORD	Counter of answers with exception code (0 to 65535).
tStat.wRXIllegalResponses	WORD	Counter of illegal answers received by the client – invalid syntax, invalid CRC or not enough bytes received (0 to 65535).

Table 105: MODBUS Client Protocol Diagnostics

Note:

Counters: all MODBUS TCP Client diagnostics counters return to zero when the limit value 65535 is exceeded.

5.8.8.1.2. Device Configuration – Configuration via Symbolic Mapping

The devices configuration, shown on figure below, follows the following parameters:

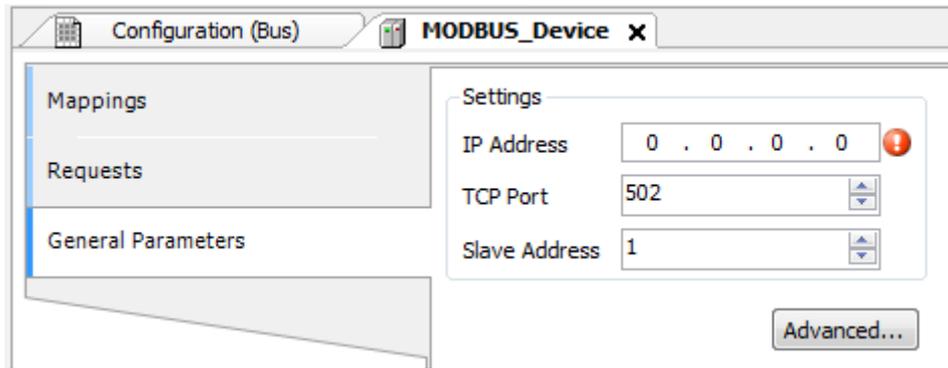


Figure 86: Device General Parameters Settings

Configuration	Description	Default	Options
IP Address	Server IP address	0.0.0.0	1.0.0.1 to 223.255.255.254
TCP Port	TCP port	502	2 to 65534
Slave Address	MODBUS Slave address	1	0 to 255

Table 106: MODBUS Client General Configurations

Notes:

IP Address: IP address of Modbus Server Device.

TCP Port: if there are multiple instances of the protocol added in a single Ethernet interface, different TCP ports must be selected for each instance. Some TCP ports, among the possibilities mentioned above, are reserved and therefore cannot be used. See table [Reserved TCP/UDP ports](#).

Slave address: according to the MODBUS standard, the valid address range for slaves is 0 to 247, where addresses 248 to 255 are reserved. When the master sends a command of writing with the address set to zero, it is performing broadcast requests on the network.

The parameters in the advanced settings of the MODBUS Client device, found on the button *Advanced...* in the *General Parameters* tab are divided into: *Maximum Simultaneous Requests*, *Communication Time-out*, *Mode of Connection Time-out* and *Inactive Time*.

Configuration	Description	Default	Options
Maximum Simultaneous Request	Number of simultaneous request the client can ask from the server	1	1 to 8
Communication Time-out (ms)	Application level time-out in ms	3000	10 to 65535
Mode	Defines when the connection with the server finished by the client	Connecting stays open while a time-out does not occur.	Connecting stays open while a time-out does not occur. Connection is closed at the end of each communication. Connection is closed after an inactive time of (s): 10 to 3600.
Inactive Time (s)	Inactivity time	10	10 to 3600

Table 107: MODBUS Client Advanced Configurations

Notes:

Maximum Simultaneous Requests: it is used with a high scan cycle. This parameter is fixed in 1 (not editable) when the configured protocol is MODBUS RTU over TCP.

Communication Time-out: the Communication time-out is the time that the client will wait for a server response to the request. For a MODBUS Client device, two variables of the system must be considered: the time the server takes to process a request and the response sending delay in case it is set in the server. It is recommended that the time-out is equal or higher than twice the sum of these parameters. For further information, check [Communication Performance](#) section.

Mode: defines when the connection with the server is finished by the client. Below follows the available options:

- **Connecting stays open while a time-out does not occur:** This option presents the same behavior of Client, close the connection due non response of a request by the Server before reaching the Communication Time-out.
- **Connection is closed at the end of each communication:** The connection is closed by the Client after finish each request.
- **Connection is closed after an Inactive Time:** The connection will be closed by the Client if it reach the Inactive Time without performing a request to the Server.

Inactive Time: inactivity connection time.

5.8.8.1.3. Mappings Configuration – Configuration via Symbolic Mapping

The MODBUS relations configuration, showed on figure below, follows the parameters described on table below:

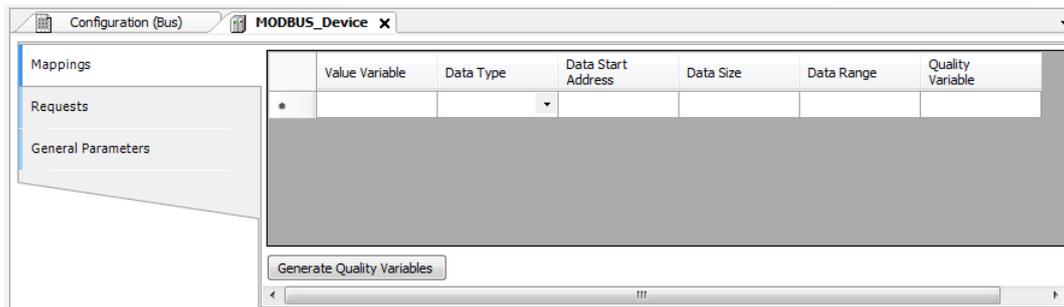


Figure 87: MODBUS Data Type

Configuration	Description	Default	Options
Value Variable	Symbolic variable name	-	Name of a variable declared in a program or GVL
Data Type	MODBUS data type	-	Coil - Write (1 bit) Coil - Read (1 bit) Holding Register - Write (16 bits) Holding Register - Read (16 bits) Holding Register – Mask AND (16 bits) Holding Register – Mask OR (16 bits) Input Register (16 bits) Input Status (1 bit)
Data Start Address	Initial address of the MODBUS data	-	1 to 65536
Data Size	Size of the MODBUS data	-	1 to 65536
Data Range	The address range of configured data	-	-

Table 108: MODBUS Mappings Settings

Notes:

Value Variable: this field is used to specify a symbolic variable in MODBUS relation.

Data type: this field is used to specify the data type used in the MODBUS relation.

Data Type	Size [bits]	Description
Coil - Write	1	Writing digital output.
Coil - Read	1	Reading digital output.
Holding Register - Write	16	Writing analog output.
Holding Register - Read	16	Reading analog output.

Data Type	Size [bits]	Description
Holding Register - Mask AND	16	Analog output which can be read or written with AND mask.
Holding Register - Mask OR	16	Analog output which can be read or written with OR mask.
Input Register	16	Analog input which can be only read.
Input Status	1	Digital input which can be only read.

Table 109: Data Types Supported in MODBUS

Data Start Address: Data initial address of a MODBUS mapping.

Data Size: The size value specifies the maximum amount of data that a MODBUS interface can access, from the initial address. Thus, to read a continuous address range, it is necessary that all addresses are declared in a single interface. This field varies with the MODBUS data type configured.

Data Range: This field shows to the user the memory address range used by the MODBUS interface.

5.8.8.1.4. Requests Configuration – Configuration via Symbolic Mapping

The configuration of the MODBUS requests, viewed in figure below, follow the parameters described in table below:

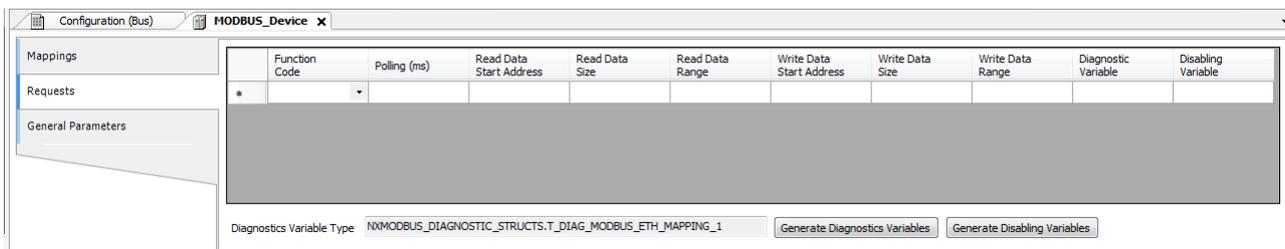


Figure 88: MODBUS Data Request Screen

Configuration	Description	Default Value	Options
Function Code	MODBUS function type	-	01 – Read Coils 02 – Read Input Status 03 – Read Holding Registers 04 – Read Input Registers 05 – Write Single Coil 06 – Write Single Register 15 – Write Multiple Coils 16 – Write Multiple Registers 22 – Mask Write Register 23 – Read/Write Multiple Registers
Polling (ms)	Communication period (ms)	100	0 to 3600000
Read Data Start Address	Initial address of the MODBUS read data	-	1 to 65536
Read Data Size	Size of MODBUS Read data	-	Depends on the function used
Read Data Range	MODBUS Read data address range	-	0 to 2147483646
Write Data Start Address	Initial address of the MODBUS write data	-	1 to 65536
Write Data Size	Size of MODBUS Write data	-	Depends on the function used
Write Data Range	MODBUS Write data address range	-	0 to 2147483647
Diagnostic Variable	Diagnostic variable name	-	Name of a variable declared in a program or GVL

Configuration	Description	Default Value	Options
Disabling Variable	Variable used to disable MODBUS relation	-	Field for symbolic variable used to disable, individually, MODBUS requests configured. This variable must be of type BOOL. The variable can be simple or array element and can be in structures.

Table 110: MODBUS Relations Configuration

Notes:

Setting: the number of factory default settings and the values for the column Options may vary according to the data type and MODBUS function (FC).

Function Code: MODBUS (FC) functions available are the following:

Code		Description
DEC	HEX	
1	0x01	Read Coils (FC 01)
2	0x02	Read Input Status (FC 02)
3	0x03	Read Holding Registers (FC 03)
4	0x04	Read Input Registers (FC 04)
5	0x05	Write Single Coil (FC 05)
6	0x06	Write Single Holding Register (FC 06)
15	0x0F	Write Multiple Coils (FC 15)
16	0x10	Write Multiple Holding Registers (FC 16)
22	0x16	Mask Write Holding Register (FC 22)
23	0x17	Read/Write Multiple Holding Registers (FC 23)

Table 111: MODBUS Functions Supported by Nexto CPUs

Polling: this parameter indicates how often the communication set for this request must be performed. By the end of a communication will be awaited a time equal to the value configured in the field polling and after that, a new communication will be executed.

Read Data Start Address: field for the initial address of the MODBUS read data.

Read Data Size: the minimum value for the read data size is 1 and the maximum value depends on the MODBUS function (FC) used as below:

- Read Coils (FC 01): 2000
- Read Input Status (FC 02): 2000
- Read Holding Registers (FC 03): 125
- Read Input Registers (FC 04): 125
- Read/Write Multiple Registers (FC 23): 121

Read Data Range: this field shows the MODBUS read data range configured for each request. The initial address, along with the read data size will result in the range of read data for each request.

Write Data Start Address: field for the initial address of the MODBUS write data.

Write Data Size: the minimum value for the write data size is 1 and the maximum value depends on the MODBUS function (FC) used as below:

- Write Single Coil (FC 05): 1
- Write Single Register (FC 06): 1
- Write Multiple Coils (FC 15): 1968
- Write Multiple Registers (FC 16): 123
- Mask Write Register (FC 22): 1
- Read/Write Multiple Registers (FC 23): 121

Write Data Range: this field shows the MODBUS write data range configured for each request. The initial address, along with the read data size will result in the range of write data for each request.

Diagnostic Variable: The MODBUS request diagnostics configured by symbolic mapping or by direct representation, are stored in variables of type *T_DIAG_MODBUS_RTU_MAPPING_1* for Master devices and *T_DIAG_MODBUS_ETH_CLIENT_1* for Client devices and the mapping by direct representation are in 4-byte and 2-word, which are described in Table 90.

T_DIAG_MODBUS_ETH_MAPPING_1.*	Size	Description
Communication Status Bits:		
byStatus.bCommIdle	BIT	Communication idle (waiting to be executed).
byStatus.bCommExecuting	BIT	Active communication.
byStatus.bCommPostponed	BIT	Communication deferred, because the maximum number of concurrent requests was reached. Deferred communications will be carried out in the same sequence in which they were ordered to avoid indeterminacy. The time spent in this State is not counted for the purposes of time-out. The bCommIdle and bCommExecuting bits are false when the bCommPostponed bit is true.
byStatus.bCommDisabled	BIT	Communication disabled. The bCommIdle bit is restarted in this condition.
byStatus.bCommOk	BIT	Communication terminated previously was held successfully.
byStatus.bCommError	BIT	Communication terminated previously had an error. Check error code.
byStatus.bCommAborted	BIT	Previously terminated communication was interrupted due to connection failure.
Last error code (enabled when bCommError = true):		
eLastErrorCode	MASTER_ERROR_CODE (BYTE)	Informs the possible cause of the last error in the MODBUS mapping. Consult Table 113 for further details.
Last exception code received by master:		
eLastExceptionCode	MODBUS_EXCEPTION (BYTE)	NO_EXCEPTION (0) FUNCTION_NOT_SUPPORTED (1) MAPPING_NOT_FOUND (2) ILLEGAL_VALUE (3) ACCESS_DENIED (128)* MAPPING_DISABLED (129)* IGNORE_FRAME (255)*
Communication statistics:		
wCommCounter	WORD	Communications counter terminated, with or without errors. The user can test when communication has finished testing the variation of this counter. When the value 65535 is reached, the counter returns to zero.
wCommErrorCounter	WORD	Communications counter terminated with errors. When the value 65535 is reached, the counter returns to zero.

Table 112: MODBUS Client Relations Diagnostics

Notes:

Exception Codes: the exception codes show in this field is the server returned values. The definitions of the exception codes 128, 129 and 255 are valid only with Altus slaves. For slaves from other manufacturers these exception codes can have different meanings.

Disabling Variable: field for the variable used to disable MODBUS requests individually configured within requests. The request is disabled when the variable, corresponding to the request, is equal to 1, otherwise the request is enabled.

Last Error Code: The codes for the possible situations that cause an error in the MODBUS communication can be consulted below:

Code	Enumerable	Description
1	ERR_EXCEPTION	Reply is in an exception code (see eLastExceptionCode = Exception Code).
2	ERR_CRC	Reply with invalid CRC.
3	ERR_ADDRESS	MODBUS address not found. The address that replied the request was different than expected.
4	ERR_FUNCTION	Invalid function code. The reply's function code was different than expected.
5	ERR_FRAME_DATA_COUNT	The amount of data in the reply was different than expected.
7	ERR_NOT_ECHO	The reply is not an echo of the request (FC 05 and 06).
8	ERR_REFERENCE_NUMBER	Invalid reference number (FC 15 and 16).
9	ERR_INVALID_FRAME_SIZE	Reply shorter than expected.
20	ERR_CONNECTION	Error while establishing connection.
21	ERR_SEND	Error during transmission stage.
22	ERR_RECEIVE	Error during reception stage.
40	ERR_CONNECTION_TIMEOUT	Application level time-out during connection.
41	ERR_SEND_TIMEOUT	Application level time-out during transmission.
42	ERR_RECEIVE_TIMEOUT	Application level time-out while waiting for reply.
43	ERR_CTS_OFF_TIMEOUT	Time-out while waiting CTS = false in transmission.
44	ERR_CTS_ON_TIMEOUT	Time-out while waiting CTS = true in transmission.
128	NO_ERROR	No error since startup.

Table 113: MODBUS Relations Error Codes

ATTENTION

Unlike other tasks of an application, when a mark is reached at MainTask debugging, the MODBUS Ethernet Client instance task or any other MODBUS task will stop being executed at the moment it tries to write in the memory area. This occurs in order to maintain data consistency of memory areas while MainTask is not running.

5.8.8.2. MODBUS Ethernet Client configuration via Direct Representation (%Q)

To configure this protocol using direct representation (%Q), the following steps must be performed:

- Configure the general parameters of the MODBUS protocol, such as: communication times and direct representation variables (%Q) to receive diagnostics.
- Add and configure devices by setting address, direct representation variables (%Q) to disable the relations, communication time-outs, etc.
- Add and configure MODBUS relations, specifying the data type and MODBUS function, time-outs, direct representation variables (%Q) to receive diagnostics of the relation and other to receive/write the data, amount of data to be transmitted and relation polling.

The descriptions of each configuration are listed below in this section.

5.8.8.2.1. General parameters of MODBUS Protocol Client - configuration for Direct Representation (%Q)

The General parameters, found on the home screen of MODBUS protocol configuration (figure below), are defined as:

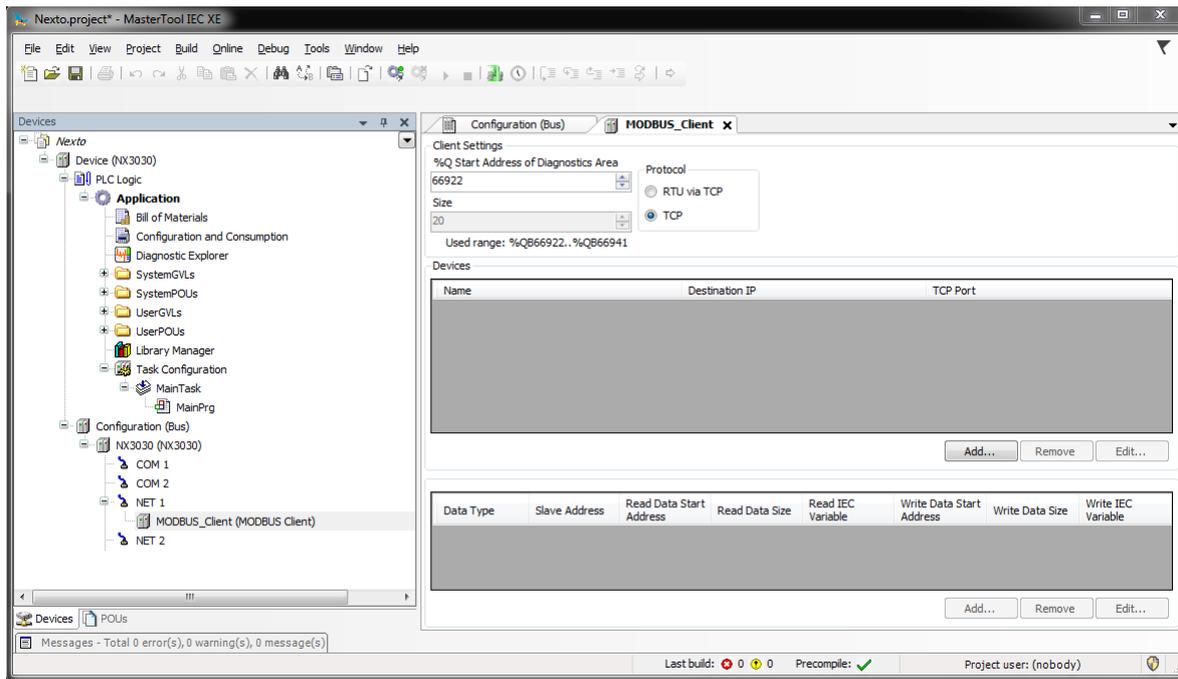


Figure 89: MODBUS Client Setup Screen

Protocol selection and direct representation variables (%Q) for diagnostics:

Setting	Description	Default Value	Options
%Q Start Address of Diagnostics Area	Initial address of the diagnostic variables	-	0 to 2147483628
Size	Size of diagnostics	20	Disabled for editing
Protocol	Protocol selection	TCP	RTU via TCP TCP

Table 114: MODBUS Client settings

Notes:

%Q Start Address of Diagnostics Area: this field is limited by the size of output variables addressable memory (%Q) at CPU, which can be found in section [Memory](#).

Default Value: the default value cannot be defined for the *%Q Start Address of Diagnostics Area* field since the creation of a protocol instance can be made at any moment within the application development. The MasterTool IEC XE software itself allocate a value from the range of direct representation output variables (%Q), still unused.

The diagnostics and MODBUS commands are described in [Table 105](#).

5.8.8.2.2. *Device Configuration – Configuration via Direct Representation (%Q)*

The configuration of the devices, viewed in figure below, comprises the following parameters:

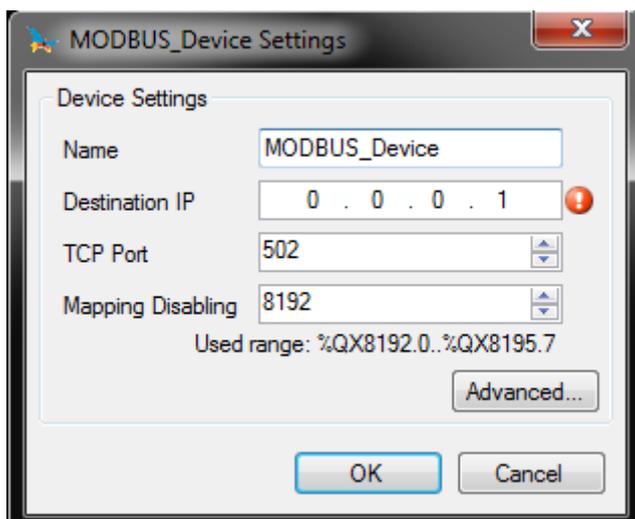


Figure 90: Configuring MODBUS Client

Configuration	Description	Factory default	Options
Name	Name of the instance	MODBUS_Device	Identifier, according to IEC 61131-3
Destination IP	IP address of the server	0. 0. 0.1	1.0.0.1 to 223.255.255.255
TCP Port	TCP Port	502	2 to 65534
Mapping Disabling	Initial address used to disable MODBUS relations	-	Any address of the %Q area, limited by the CPU model

Table 115: Configuration of Client Devices

Notes:

Instance Name: this field is the identifier of the device, which is checked according to IEC 61131-3, i.e. it does not allow spaces, special characters and starting with numeral character. It is limited to 24 characters.

TCP Port: if there are multiple instances of the protocol added in a single Ethernet interface, different TCP ports must be selected for each instance. Some TCP ports, among the possibilities mentioned above, are reserved and therefore cannot be used. See table [Reserved TCP/UDP ports](#).

Mapping Disabling: composed of 32 bits, it is used to disable, individually, the 32 MODBUS relations configured in *Device Mappings* space. The relation is disabled when the corresponding bit is equal to 1, otherwise, the mapping is enabled. This field is limited by the size of output variables addressable memory (%Q) at CPU, which can be found in section [Memory](#).

Default Value: factory default cannot be set for the *Mapping Disabling* field, since the creation of a protocol instance can be made at any moment within the application development. The MasterTool IEC XE software itself allocate a value from the range of direct representation output variables (%Q), still unused.

Communication Time-out: the settings present on the button *Advanced...* on the TCP connection, are described in the notes of the section [Device Configuration – Configuration via Symbolic Mapping](#).

5.8.8.2.3. *Mapping Configuration – Configuration via Direct Representation (%Q)*

The MODBUS relations settings, viewed in the figures below, follow the parameters described in table below:

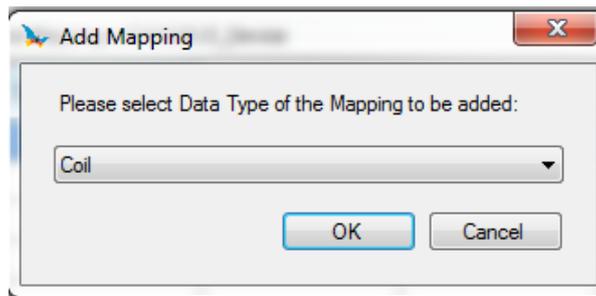


Figure 91: MODBUS Data Type

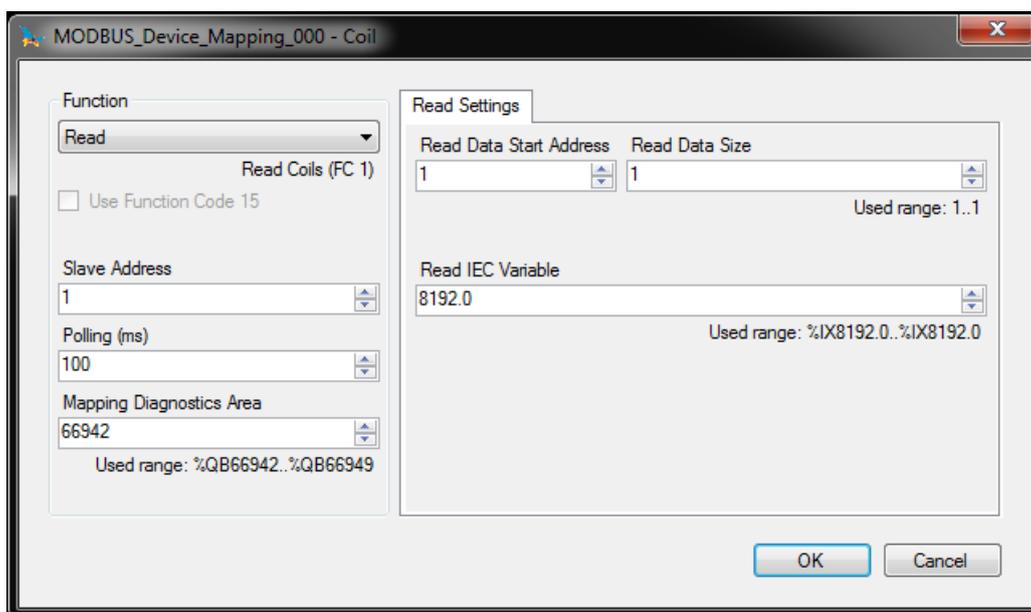


Figure 92: MODBUS Function

In table below, the number of factory default settings and the values for the column Options, may vary according to the data type and MODBUS function (FC).

Configuration	Description	Default Value	Options
Function	MODBUS function type	Read	Read Write Read/Write Mask Write
Slave Address	MODBUS slave address	1	0 to 255
Polling (ms)	Period of communication (ms)	100	0 to 3600000
Mapping Diagnostics Area	Starting address of MODBUS interface diagnostics	-	0 to 2147483640
Read Data Start Address	Starting address of the read MODBUS data	1	1 to 65536
Read Data Size	Number of read MODBUS data	-	Depends on the function used
Read IEC Variable	Starting address of the read variables (%I)	-	0 to 2147483647
Write Data Start Address	Starting address of MODBUS writing data	1	1 to 65536
Write Data Size	Number of MODBUS writing data	-	Depends on the function used
Write IEC Variable	Starting address of the write variables (%Q)	-	0 to 2147483647

Configuration	Description	Default Value	Options
Mask Write IEC Variables	Starting address of variables for write mask (%Q)	-	0 to 2147483644

Table 116: Device Mapping

Notes:

Device Mappings Table: the number of settings and values described in the column Options may vary according to the data type and MODBUS function.

Slave Address: typically, the address 0 is used when the server is a MODBUS RTU or MODBUS RTU via TCP Gateway, and the same broadcasts the request to all network devices. When the address 0 is used, the client doesn't wait for a response and its use serves only to written commands. Moreover, in accordance with MODBUS standard, the valid address range for slaves is 0 to 247, and addresses 248 to 255 are reserved.

Polling: this parameter indicates how often the communication set for this relation must be executed. At the end of communication will be awaited a time equal to the configured polling and after, will be performed a new communication as soon as possible.

Mapping Diagnostic Area: this field is limited by the size of output variables addressable memory (%Q) at CPU, which can be found in the section [Memory](#). The configured MODBUS relations diagnostics are described in Table 90.

Size of the Read and Write Data: details of the size of the data supported by each function are described in the notes of [Requests Configuration – Symbolic Mapping Settings](#) section.

ATTENTION

When accessing the communication data memory is between devices with different endianness (Little-Endian and Big-Endian), inversion of the read/write data may occur. In this case, the user must adjust the data in the application.

Read IEC Variable: in case the MODBUS data type is *Coil* or *Input Status* (bit), the IEC variables initial address will be in the format %IX10.1. However, if the MODBUS data type is *Holding Register* or *Input Register* (16 bits), the IEC variables initial address will be in the format %IW. This field is limited by the memory size of the addressable input variables (%I) from each CPU, which can be seen on [Memory](#) section.

Write IEC Variable: in case the MODBUS data type is *Coil* (bit), the IEC variables initial address will be in the format %QX10.1. However, if the MODBUS data type is *Holding Register* (16 bits), the IEC variables initial address will be in the format %QW. This field is limited by the memory size of the addressable output variables (%Q) from each CPU, which can be seen on [Memory](#) section.

Write Mask of IEC Variables: the *Mask Write Register* function (FC 22) employs a logic between the value already written and the two words that are configured in this field using %QW(0) for the AND mask and %QW(2) for the OR mask; allowing the user to handle the word. This field is limited by the size of output variables addressable memory (%Q) of each CPU, which can be found in the section [Memory](#).

Default Value: the factory default value cannot be set for the *Mapping Diagnostics Area*, *Read IEC Variable*, *Write IEC Variable* and *Mask Write IEC Variables* fields, since the creation of a relation can be performed at any time on application development. The MasterTool IEC XE software itself allocate a value from the range of direct representation output variables (%Q), still unused. Factory default cannot be set to the *Read/Write Data Size* fields, as they will vary according to the MODBUS data type selected.

ATTENTION

Unlike other tasks of an application, when a mark is reached at MainTask debugging, the MODBUS Ethernet Client instance task or any other MODBUS task will stop being executed at the moment it tries to write in the memory area. This occurs in order to maintain data consistency of memory areas while MainTask is not running.

5.8.8.3. MODBUS Client Relation Start in Acyclic Form

To start a MODBUS Client relation in acyclic form, it is suggested the following method which can be implemented in a simple way in the user application program:

- Define the maximum polling time for the relations;
- Keep the relation normally disabled;
- Enable the relation at the moment the execution is desired;
- Wait for the confirmation of the relation execution finishing and, at this moment, disable it again.

5.8.9. MODBUS Ethernet Server

This protocol is available for all Nexto Series CPUs on its Ethernet channels. When selecting this option at MasterTool IEC XE, the CPU becomes a MODBUS communication server, allowing the connection with MODBUS client devices. This protocol is only available when the CPU is in execution mode (*Run Mode*).

There are two ways to configure this protocol. The first one makes use of *direct representation (%Q)*, in which the variables are defined by your address. The second one, through *symbolic mapping*, where the variables are defined by your name.

The procedure to insert an instance of the protocol is found in detail in the MasterTool IEC XE User Manual – MU299609.

5.8.9.1. MODBUS Server Ethernet Protocol Configuration for Symbolic Mapping

To configure this protocol using *Symbolic Mappings*, it is necessary to execute the following steps:

- Configure the MODBUS server protocol general parameters, as: TCP port, protocol selection, IP filters for Reading and Writing (available at the Filters Configuration button) and communication times (available at the Server Advanced Configurations button).
- Add and configure MODBUS mappings, specifying the variable name, data type, data initial address and data size.

The description of each configuration is related ahead in this section.

5.8.9.1.1. MODBUS Server Protocol General Parameters – Configuration via Symbolic Mapping

The general parameters, found on the MODBUS protocol initial screen (figure below), are defined as.

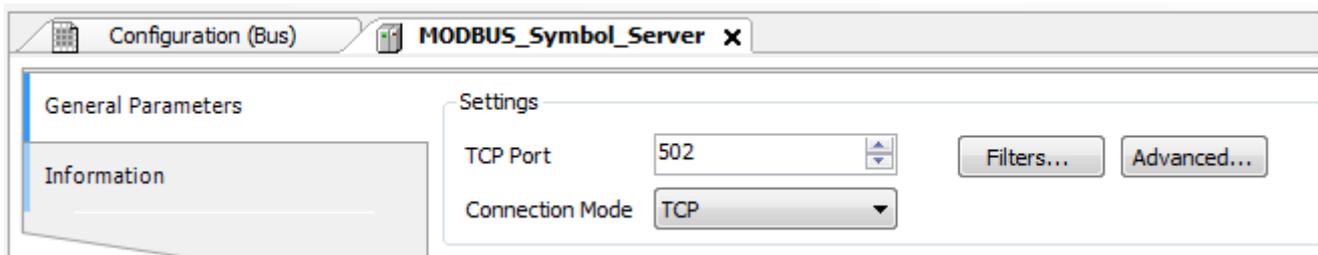


Figure 93: MODBUS Server General Parameters Configuration Screen

Configuration	Description	Default	Options
TCP Port	TCP port	502	2 to 65534
Connection Mode	Protocol selection	TCP	RTU via TCP TCP

Table 117: MODBUS Server General Configurations

Notes:

TCP Port: if there are multiple instances of the protocol added in a single Ethernet interface, different TCP ports must be selected for each instance. Some TCP ports, among the possibilities mentioned above, are reserved and therefore cannot be used. See table [Reserved TCP/UDP ports](#).

The settings present on the *Filters...* button, described in table below, are relative to the TCP communication filters:

Configuration	Description	Default Value	Options
Write Filter IP Address	Specifies a range of IPs with write access in the variables declared in the MODBUS interface.	0.0.0.0	0.0.0.0 to 255.255.255.255
Write Filter Mask	Specifies the subnet mask in conjunction with the IP filter parameter for writing.	0.0.0.0	0.0.0.0 to 255.255.255.255

Configuration	Description	Default Value	Options
Read Filter IP Address	Specifies a range of IPs with read access in the variables declared in the MODBUS interface.	0.0.0.0	0.0.0.0 to 255.255.255.255
Read Filter Mask	Specifies the subnet mask in conjunction with the IP filter parameter for reading.	0.0.0.0	0.0.0.0 to 255.255.255.255

Table 118: IP Filters

Note:

Filters: filters are used to establish a range of IP addresses that have write or read access to MODBUS relations, being individually configured. The permission criteria is accomplished through a logical AND operation between the Write Filter Mask and the IP address of the client. If the result is the same as the Write Filter IP Address, the client is entitled to write. For example, if the Write Filter IP Address = 192.168.15.0 and the Write Filter Mask = 255.255.255.0, then only customers with IP address = 192.168.15.x shall be entitled. The same procedure is applied in the Read Filter parameters to define the read rights.

The communication times of the MODBUS server protocol, found on the *Advanced...* button of the configuration screen, are divided into: *Task Cycle* and *Connection Inactivity Time-out*.

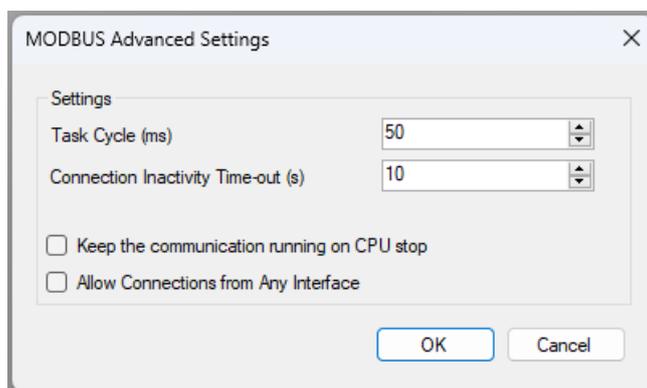


Figure 94: MODBUS Server Advanced Settings Configuration Screen

Configuration	Description	Default Value	Options
Task Cycle (ms)	Time for the instance execution within the cycle, without considering its own execution time	50	5 to 100
Connection Inactivity Time-out (s)	Maximum idle time between client and server before the connection is closed by the server	10	1 to 3600
Keep the communication running on CPU stop.	Enable the MODBUS Slave to run while the CPU is in STOP or after a breakpoint	Unmarked	Marked or Unmarked
Allow Connections from Any Interface	Enables connections through any network interface, including VPN	Unmarked	Marked or Unmarked

Table 119: MODBUS Server Advanced Configurations

Notes:

Task Cycle: the user has to be careful when changing this parameter as it interferes directly in the answer time, data volume for scanning and mainly in the CPU resources balance between communications and other tasks.

Connection Inactivity Time-out: this parameter was created in order to avoid that the maximum quantity of TCP connections is reached, imagining that inactive connections remain open on account of the most different problems. It indicates how long a connection (client or server) can remain open without being used (without exchanging communication messages). If the specified time is not reached, the connection is closed releasing an input in the connection table.

Allow Connections from Any Interface: When enabled, the MODBUS server will accept connections from any available interface on the device, including VPN interfaces. When disabled, it will only accept connections on the interface where it is instantiated. When enabling this option, ensure that no other protocol in the project uses the same port as the MODBUS server to avoid communication conflicts.

5.8.9.1.2. MODBUS Server Diagnostics – Configuration via Symbolic Mapping

The diagnostics and commands of the MODBUS server protocol configured, either by symbolic mapping or by direct representation, are stored in variables of type *T_DIAG_MODBUS_ETH_SERVER_1* and the mapping by direct representation are in 4-byte and 8-word, which are described in table below:

T_DIAG_MODBUS_ETH_SERVER_1.*	Size	Description
Diagnostic Bits:		
tDiag.bRunning	BIT	The server is running.
tDiag.bNotRunning	BIT	The server is not running (see bit bInterruptedByCommand).
tDiag.bInterruptedByCommand	BIT	The bit bNotRunning was enabled, because the server was interrupted by the user through the command bit.
tDiag.bConfigFailure	BIT	Configuration failure.
tDiag.bModuleFailure	BIT	Indicates if there is failure in the module or the module is not present.
Command bits, automatically initialized:		
tCommand.bStop	BIT	Stop the server.
tCommand.bRestart	BIT	Restart the server.
tCommand.bResetCounter	BIT	Reset diagnostics statistics (counters).
Communication Statistics:		
tStat.wActiveConnections	WORD	Number of established connections between client and server (0 to 64).
tStat.wTimeoutClosedConnections	WORD	Connections counter, between the client and server, interrupted after a period of inactivity - time-out (0 to 65535).
tStat.wClientClosedConnections	WORD	Connections counter interrupted due to customer request (0 to 65535).
tStat.wRXFrames	WORD	Ethernet frames counter received by the server. An Ethernet frame can contain more than one request (0 to 65535).
tStat.wRXRequests	WORD	Requests received by the server counter and answered normally (0 to 65535).
tStat.wTXExceptionResponses	WORD	Requests received by the server counter and answered with exception codes (0 to 65535).
tStat.wRXIllegalRequests	WORD	Illegal requests counter (0 to 65535).

Table 120: MODBUS Server Diagnostics

Note:

Counters: all counters of the MODBUS Ethernet Server Diagnostics return to zero when the limit value 65535 is exceeded.

bModuleFailure: Diagnosis implemented only for symbolic MODBUS.

5.8.9.1.3. Mapping Configuration – Configuration via Symbolic Mapping

The MODBUS relations configuration, showed on figure below, follows the parameters described on table below:

Mappings

	Value Variable	Data Type	Data Start Address	Absolute Data Start Address	Data Size	Data Range
*						

Figure 95: MODBUS Server Data Mappings Screen

Configuration	Description	Default Value	Options
Value Variable	Symbolic variable name	-	Name of a variable declared in a program or GVL
Data Type	MODBUS data type	-	Coil Input Status Holding Register Input Register
Data Start Address	Starting address of the MODBUS data	-	1 to 65536
Absolute Data Start Address	Start address of absolute data of Modbus as its type	-	-
Data Size	Size of the MODBUS data	-	1 to 65536
Data Range	Data range address configured	-	-

Table 121: MODBUS Ethernet Mappings Configuration

Notes:

Value Variable: this field is used to specify a symbolic variable in MODBUS relation.

Data Type: this field is used to specify the data type used in the MODBUS relation.

Data Start Address: data initial address of the MODBUS relation.

Absolute Data Start Address: absolute start address of the MODBUS data according to their type. For example, the Holding Register with address 5 has absolute address 400005. This field is read only and is available to assist in Client/Master MODBUS configuration that will communicate with this device. The values depend on the base address (offset) of each data type and allowed MODBUS address for each data type.

Data Size: the Data Size value sets the maximum amount of data that a MODBUS relation can access from the initial address. Thus, in order to read a continuous range of addresses, it is necessary that all addresses are declared in a single relation. This field varies according to the configured type of MODBUS data.

Data Range: is a read-only field and reports on the range of addresses that is being used by this mapping. It is formed by the sum of the fields *Data Start Address* and *Data Size*. There can be no range overlays with others mappings of the same *Data Type*.

ATTENTION

Unlike other tasks of an application, when a mark is reached at MainTask debugging, the MODBUS Ethernet Server instance task or any other MODBUS task will stop being executed at the moment it tries to write in the memory area. This occurs in order to maintain data consistency of memory areas while MainTask is not running.

5.8.9.2. MODBUS Server Ethernet Protocol Configuration via Direct Representation (%Q)

To configure this protocol using *Direct Representation (%Q)*, the user must perform the following steps:

- Configure the general parameters of MODBUS Server Protocol, such as: communication times, address and direct representation variables (%Q) to receive the diagnostics and control relation.
- Add and configure MODBUS relations, specifying the MODBUS data type, direct representation variables (%Q) to receive/write the data and amount of data to be reported.

The descriptions of each configuration are listed below in this section.

5.8.9.2.1. General Parameters of MODBUS Server Protocol – Configuration via Direct Representation (%Q)

The general parameters, found on the home screen of MODBUS protocol configuration (figure below), are defined as:

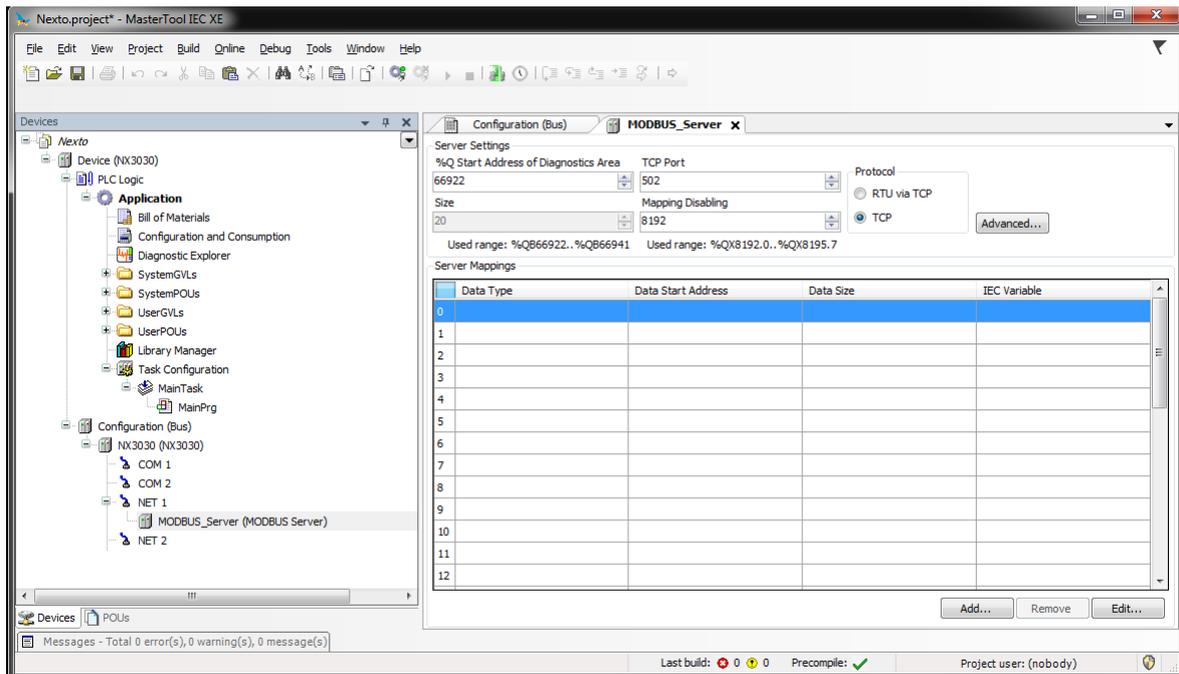


Figure 96: MODBUS Server Setup Screen

TCP port, protocol and direct representation variables (%Q) to control relations and diagnostics:

Configuration	Description	Default Value	Options
%Q Start Address of Diagnostics Area	Starting address of the diagnostic variables	-	0 to 2147483628
Size	Size of diagnostics	20	Disabled for editing
TCP Port	TCP Port	502	2 to 65534
Mapping Disabling	Starting address used to disable MODBUS relations	-	0 to 2147483644
Protocol	Protocol selection	TCP	RTU via TCP TCP

Table 122: Settings to control relations and diagnostics

Notes:

%Q Start Address of Diagnostics Area: this field is limited by the size of output variables addressable memory (%Q) at CPU, which can be found in section [Memory](#).

TCP Port: if there are multiple instances of the protocol added in a single Ethernet interface, different TCP ports must be selected for each instance. Some TCP ports, among the possibilities mentioned above, are reserved and therefore cannot be used. See table [Reserved TCP/UDP ports](#).

Mapping Disabling: composed of 32 bits, used to disable, individually, the 32 MODBUS relations configured in *Server Mappings* space. The relation is disabled when the corresponding bit is equal to 1, otherwise, the mapping is enabled. This field is limited by the size of output variables addressable memory (%Q) of each CPU, which can be found on [Memory](#) section.

Default Value: the factory default value cannot be set to the *%Q Start Address of Diagnostics Area* and *Mapping Disabling* fields, because the creation of a Protocol instance may be held at any time on application development. The MasterTool IEC XE software itself allocate a value, from the range of output variables of direct representation (%Q), not used yet.

The communication times of the MODBUS Server protocol, found on the *Advanced...* button of the configuration screen, are divided into: *Task Cycle (ms)* and *Connection Inactivity Time-out (s)*. Further details are described in [MODBUS Server Protocol General Parameters – Configuration via Symbolic Mapping](#) section.

The diagnostics and MODBUS commands are described in [Table 120](#).

5.8.9.2.2. *Mapping Configuration – Configuration via Direct Representation (%Q)*

The MODBUS relations settings, viewed in the figures below, follow the parameters described in table below:

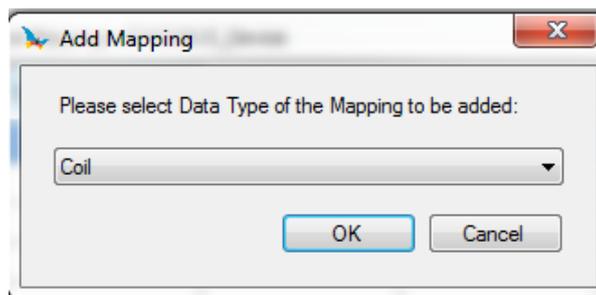


Figure 97: MODBUS Data Type

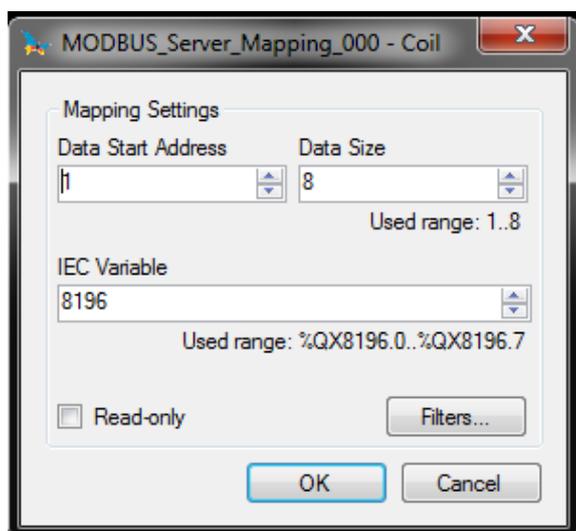


Figure 98: MODBUS Server Function

Configuration	Description	Default	Options
Data Type	MODBUS data type	Coil	Coil (1 bit) Holding Register (16 bits) Input Status (1 bit) Input Register (16 bits)
Data Start Address	MODBUS data initial address	1	1 to 65536
Data Size	MODBUS data quantity	8	1 to 65536 (Holding Register and Input Register) 8 to 65536 (Coil and Input Status)
IEC Variable	Variables initial address (%Q)	-	0 to 2147483647
Read-only	Allow reading only	Disabled	Enabled or Disabled

Table 123: Server Mappings

Notes:

Options: the values written in the column *Options* may vary according with the configured MODBUS data.

Data Size: the *Data Size* value sets the maximum amount of data that a MODBUS relation can access from the initial address. Thus, to read a continuous range of addresses, it is necessary that all addresses are declared in a single relation. This field varies according to the set MODBUS data type, that is, when selected *Coil* or *Input Status*, the field *Data Size* must be a number multiple of 8. It is also important to take care so the maximum value is not greater than the addressable output memory size and the attributed values aren't the same already used during the application.

ATTENTION

When accessing the communication data memory is between devices with different endianness (Little-Endian and Big-Endian), inversion of the read/write data may occur. In this case, the user must adjust the data in the application.

IEC Variable: in case the MODBUS data type is *Coil* or *Input Status* (bit), the IEC variables initial address will be in the format for example *%QX10.1*. However, if the MODBUS data type is *Holding Register* or *Input Register* (16 bits), the IEC variables initial address will be in the format *%QW*. This field is limited by the memory size of the addressable output variables (%Q) from each CPU, which can be seen on the [Memory](#) section.

Read-only: when enabled, it only allows the communication master to read the variable data. It does not allow the writing. This option is valid for the writing functions only.

Default: the default cannot be defined for the *IEC Variable* field as the creation of a protocol instance can be made at any moment within the application development, making the MasterTool IEC XE software allocate a value itself from the direct representation output variables range (%Q) still not used. The default cannot be defined for the *Data Size* field as it will vary according to selected MODBUS data type.

The settings present on the *Filters...* button, described in table below, are relative to the TCP communication filters:

Configuration	Description	Default Value	Options
Write Filter IP Address	Specifies a range of IPs with write access in the variables declared in the MODBUS interface.	0.0.0.0	0.0.0.0 to 255.255.255.255
Write Filter Mask	Specifies the subnet mask in conjunction with the IP filter parameter for writing.	0.0.0.0	0.0.0.0 to 255.255.255.255
Read Filter IP Address	Specifies a range of IPs with read access in the variables declared in the MODBUS interface.	0.0.0.0	0.0.0.0 to 255.255.255.255
Read Filter Mask	Specifies the subnet mask in conjunction with the IP filter parameter for reading.	0.0.0.0	0.0.0.0 to 255.255.255.255

Table 124: IP Filters

Note:

Filters: filters are used to establish a range of IP addresses that have write or read access to MODBUS relations, being individually configured. The permission criteria is accomplished through a logical AND operation between the Write Filter Mask and the IP address of the client. If the result is the same as the Write Filter IP Address, the client is entitled to write. For example, if the Write Filter IP Address = 192.168.15.0 and the Write Filter Mask = 255.255.255.0, then only customers with IP address = 192.168.15.x shall be entitled. The same procedure is applied in the Read Filter parameters to define the read rights.

In the previously defined relations, the maximum MODBUS data size can be 65536 (maximum value configured in the *Data Size* field). However, the request which arrives in the MODBUS Ethernet Server must address a subgroup of this mapping and this group must have, at most, the data size depending on the function code which is defined below:

- Read Coils (FC 1): 2000
- Read Input Status (FC 2): 2000
- Read Holding Registers (FC 3): 125
- Read Input Registers (FC 4): 125
- Write Single Coil (FC 5): 1
- Write Single Holding register (FC 6): 1
- Force Multiple Coils (FC 15): 1968
- Write Holding Registers (FC 16): 123
- Mask Write Register (FC 22): 1
- Read/Write Holding Registers (FC 23):
 - Read: 121
 - Write: 121

ATTENTION

Differently from other application tasks, when a depuration mark in the MainTask is reached, the task of an Ethernet MODBUS Server instance and any other MODBUS task will stop running at the moment that it tries to perform a writing in a memory area. It occurs in order to keep the consistency of the memory areas data while a MainTask is not running.

5.8.10. OPC DA Server

It's possible to communicate with the Nexto Series CPUs using the OPC DA (*Open Platform Communications Data Access*) technology. This open communication platform was developed to be the standard in industrial communications. Based on client/server architecture, it offers several advantages in project development and communication with automation systems.

A very common analogy to describe the OPC DA technology is of a printer. When correctly connected, the computer needs a driver to interface with the equipment. Similarly, the OPC helps with the interface between the supervision system and the field data on the PLC.

When it comes to project development, to configure the communication and exchange information between the systems is extremely simple using OPC DA technology. Using other drivers, based on addresses, it's necessary to create tables to relate tags from the supervision system with variables from the programmable controller. When the data areas are changed during the project, it's necessary to remap the variables and create new tables with the relations between the information on the PLC with the Supervisory Control And Data Acquisition system (SCADA).

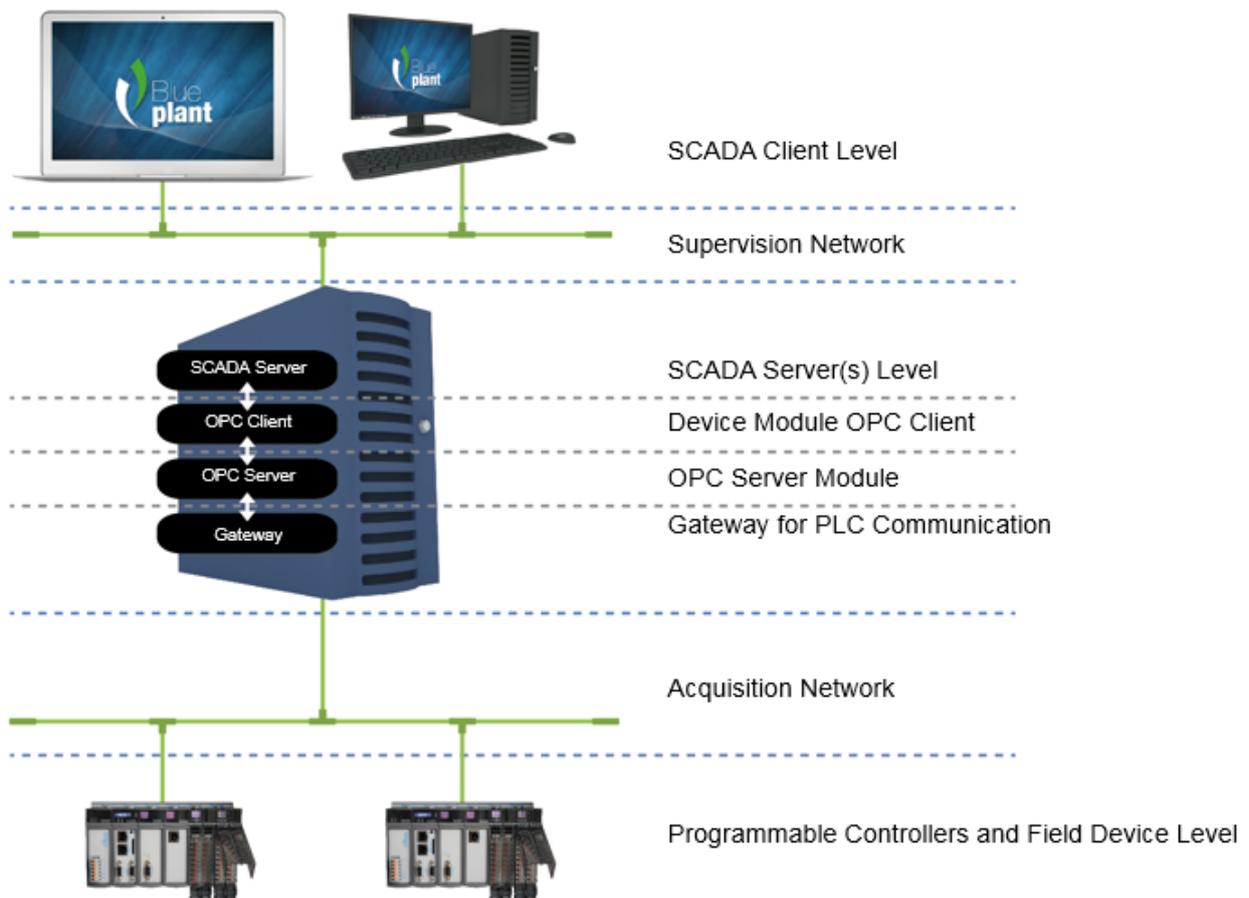


Figure 99: OPC DA Architecture

The figure above shows an architecture to communicate a SCADA system and PLCs in automation projects. All the roles present on a communication are explicit on this figure regardless of the equipment in which it's executed, since they can be done in the same equipment or in various ones. Each of the roles of this architecture are described on table below.

Role	Description
Programmable Controllers and Field Devices Level	The field devices and the PLCs are where the operation state and plant control information are stored. The SCADA system access the information on these devices and store on the SCADA server, so that the SCADA clients can consult it during the plant operation.
Acquisition Network	The acquisition network is where the requests for data collected by field devices travel, to request the data collected from the field devices.
Gateway for PLC Communication	A gateway enables the communication between the OPC DA Server and Nexto Series PLCs. A gateway in the same subnet of the PLC is always necessary, as described in chapter Communication Settings of MasterTool IEC XE User Manual – MU299609.
OPC Server Module	The OPC DA Server is a Module responsible of receiving the OPC DA requests and translate them to the communication with the field devices.
Device Module OPC Client	The OPC Client Device module is responsible for the requests to the OPC DA Server using the OPC DA protocol. The collected data is stored on the SCADA Server database.
SCADA Server Level	The SCADA Server is responsible for connecting to the various communication devices and store the data collected by them on a database, so that it can be consulted by the SCADA Clients.
Supervision Network	The supervision network is the network through which the SCADA Clients are connected to the SCADA Servers. In a topology in which there aren't multiple Client or where the Server and the Client are installed on the same equipment, this kind of network doesn't exist.
SCADA Client Level	The SCADA Clients are responsible for requesting to the SCADA Servers the necessary data to be shown in a screen where the operation of a plant is being executed. Through then it is possible to execute readings and writings on data stored on the SCADA Server database.

Table 125: Roles Description on an OPC DA Server Architecture

The relation between the tags on the supervision system and the process data on the controller variables is totally transparent. This means that, if there's an alteration on the data areas through the development of the project, it isn't necessary to rework the relations between the information on the PLC and the SCADA, just use the new variable provided by the PLC on the systems that request this data.

The use of OPC offers more productivity and connectivity with SCADA systems. It contributes with the reduction of applications development time and with the maintenance costs. It even makes possible the insertion of new data on the communication in a simplified form and with greater flexibility and interoperability between the automation system, due to the fact that it's an open standard.

The installation of the OPC DA Server is done altogether with MasterTool IEC XE installation, and its settings are done inside the tool. It's worth notice that the OPC is available only with the integrated Ethernet interface of the Nexto CPUs. The Ethernet expansion modules do not support this functionality.

5.8.10.1. Creating a Project for OPC DA Communication

Unlike the communication with drivers such as MODBUS and PROFIBUS DP, to set an OPC DA communication it's only necessary to correctly set the node and indicate which variables will be used in the communication. There are two ways to indicate which variables of the project will be available in the OPC DA Server. In both cases it's necessary to add the object *Symbol Configuration* to the application, in case it isn't present. To add it, right-click over the object *Application* and select the option.

ATTENTION

The variables shown in the objects *IoConfig_Globals*, *IoConfig_Application_Mappings* and *IoConfig_Global_Mappings* are used internally for I/O control and shouldn't be used by the user.

ATTENTION

In addition to the variables declared at SFC language POU's, some implicitly created variables are also shown. To each step created, a type *IecSfc.SFCStepType* variable is created, where the step states can be monitored, namely whether it is active or not and the time that it's active as in norm IEC 61131-1. To each transition, a BOOL type variable is created that defines if the transition is true or false. These variables are shown in the object *Symbol Configuration* that can be provided access to the OPC Client.

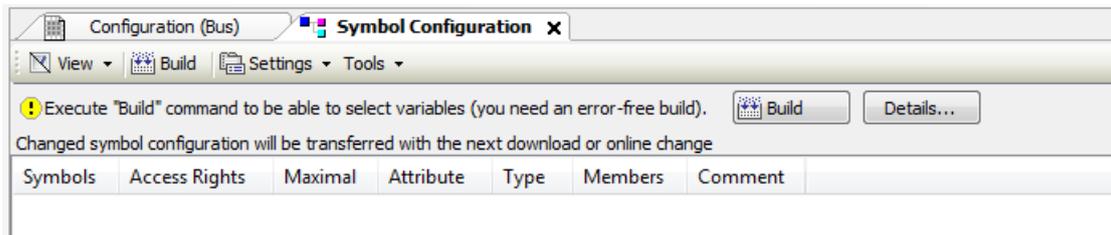


Figure 100: Symbol Configuration Object

The table below presents the descriptions of the *Symbol Configuration* object screen fields.

Field	Description
Symbols	Variable identifier that will be provided to the OPC DA Server.
Access Rights	Indicates what the possible access right level are in the declared symbol. When not utilized, this column remains empty, and the access right level is maximum. Otherwise the access right level can be modified by clicking over this field. The possible options are: Read only  Write only  Read and Write 
Maximal	Indicates the maximum access right level that is possible to assign to the variable. The symbols hold the same meanings from the ones in Access Rights. It's not possible to change it and it's indicated by the presence or not of the <i>attribute 'symbol'</i>
Attribute	Indicates if <i>attribute 'symbol'</i> is being used when the variable is declared. When not used, this column remains empty. For the cases in which the attribute is used, the behavior is the following: attribute 'symbol' := 'read' the column shows  attribute 'symbol' := 'write' the column shows  attribute 'symbol' := 'readwrite' the column shows 
Type	Data type of the declared variable.
Members	When the data type is a Struct, a button is enabled in this column. Clicking on the button will allow the selection of which elements of that struct will be provided to the OPC DA Server.

Field	Description
Comment	Variable comment, inserted on the POU or GVL where the variable was declared. To show up as a variable comment here, the comment must be entered one line before the variable on the editor, while in text mode, or in the comment column when in tabular mode.

Table 126: Symbol Configuration object screen fields description

When altering the project settings, such as adding or removing variables, it's necessary to run the command *Build*, in order to refresh the list of variables. This command must be executed until the message in Figure 100 disappear. After this, all available variables in the project, whether they are declared on POU, GVLs or diagnostics, will be shown here and can be selected. The selected variables will be available on the OPC DA Server to be accessed by the Clients.

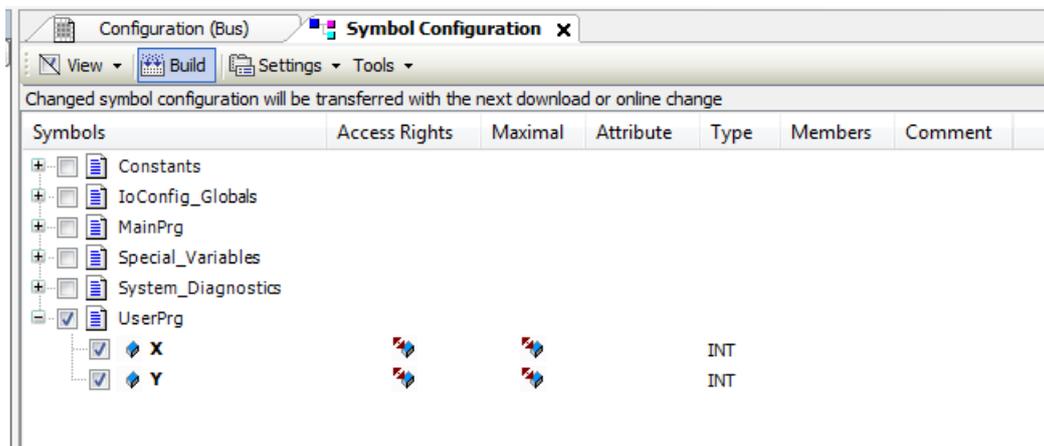


Figure 101: Selecting Variables on the Symbol Configuration

After this procedure, the project must be loaded into a PLC so the variables will be available for communication with the OPC DA Server. If the object Symbol Configuration screen is open and any of the variables, POU or GVLs selected is changed, its name will appear with the red color. The situations in which this may happen is when a variable is deleted or the attribute value is modified.

It's also possible to set which variables will be available on the OPC DA Server through an attribute inserted directly on the POU or GVLs where the variables are declared. When the *attribute 'symbol'* is present on the variable declaration, and it may be before the definition of the POU or GVL name, or to each variable individually, these variables are sent directly to the object *Symbol Configuration*, with a symbol in the *Attribute* column. In this case it's necessary, before loading the project into the CPU, to run the command *Build* from within the object *Symbol Configuration*.

The valid syntaxes to use the attribute are:

- *attribute 'symbol' := 'none'* – when the attribute value is *'none'*, the variables won't be available to the OPC DA Server and won't be shown in the object *Symbol Configuration* screen.
- *attribute 'symbol' := 'read'* - when the attribute value is *'read'*, the variables will be available to the OPC DA Server with read only access right.
- *attribute 'symbol' := 'write'* - when the attribute value is *'write'*, the variables will be available to the OPC DA Server with write only access right.
- *attribute 'symbol' := 'readwrite'* – when the attribute value is *'readwrite'*, the variables will be available to the OPC DA Server with read and write access right.

In the following example of variable declaration, the variables A and B settings allow that an OPC DA Server access them with read and write access. However the variable C cannot be accessed, while the variable D can be accessed with read only access rights.

```
{attribute 'symbol' := 'readwrite'}
PROGRAM UserPrg
VAR
```

```
A: INT;
B: INT;
{attribute 'symbol' := 'none'}
C: INT;
{attribute 'symbol' := 'read'}
D :INT;
END_VAR
```

When a variable with a type different from the basic types is defined, the use of the attribute must be done inside the declaration of this DUT and not only in the context in which the variable is created. For example, in the case of a DUT instance inside of a POU or a GVL that has an attribute, it will not impact in the behavior of this DUT instance elements. It will be necessary to apply the same access right level on the DUT declaration.

ATTENTION

The configurations of the symbols that will be provided to the OPC DA Server are stored inside the PLC project. By modifying these configurations it's necessary to load the application on the PLC so that it's possible to access those variables.

ATTENTION

When a variable is removed from the project and loaded on the PLC unchecking it from the object *Symbol Configuration*, the variable can no longer be read with the OPC Client. If the variable is added again to the project, with the same name and same context, and inserted on the object *Symbol Configuration*, it will be necessary to reboot the OPC Client to refresh the variable address reference, which will be created on a different memory area of the PLC.

5.8.10.2. Configuring a PLC on the OPC DA Server

The configuration of the PLC is done inside MasterTool IEC XE through the option available in the *Online*. It's necessary to run MasterTool IEC XE as administrator.

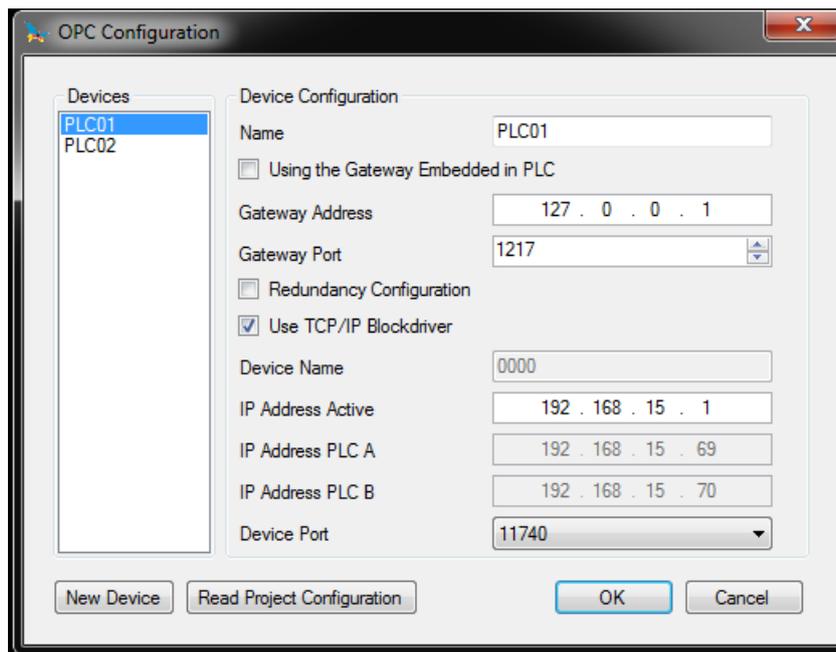


Figure 102: OPC DA Server Settings

The *Gateway Configuration* is the same set in the Gateway used for the communication between the MasterTool IEC XE and the PLC and described in Communication Settings, present in the MasterTool IEC XE User Manual – MU299609. If the configuration used is *localhost* the *Gateway Address* must be filled with 127.0.0.1. This configuration is necessary because the OPC DA Server uses the same communication gateway and the same protocol used for communication between PLC and MasterTool IEC XE.

There's the option *Using the Gateway Embedded in PLC* that can be selected when it's desired to use the Gateway that is in PLC itself. This option can be used to optimize the communication, since it prevent excess traffic through a particular station, when more than one station with OPC Client is connected to the same PLC.

To configure the PLC, there are two possible configuration types, depending on the selection of the checkbox *Use TCP/IP Blockdriver*. When the option isn't selected, the field *Device Name* must be filled with the name of the PLC. This is the name displayed by the PLC selected as active in the *Communication Settings* screen.

The other option is to use the *IP Address* of the Ethernet Interfaces. The same address set on the configuration screens must be put in this field. Furthermore, when this method is used, the port number must be set to 11740. The confirmation will save the OPC DA Server configurations.

Device Configuration	Description	Default Setting	Options
Name	PLC description inside the OPC DA Server configuration file. This field can have any name, but for organizational purposes, it's recommended to use the project name that is loaded in the PLC.	'PLC01'	This field is a STRING and it accepts alphanumeric (letters and numbers) characters and the “_” character. It's not allowed to initiate a STRING with numbers or with “_”. It allows up to 49 characters.
Gateway Address	IP Address of the computer that the OPC DA Server is installed, for the cases in which all PLCs are in the same subnetwork. If there's some PLC that it's in another subnetwork, it must be specified the Gateway used in that subnetwork.	127.0.0.1	0.0.0.0 to 255.255.255.255
Gateway Port	TCP Port for the connection with the Gateway.	1217	2 to 65534
Device Name	It's the PLC name displayed in the <i>Communication Settings</i> of the <i>Device</i> tab. The name is the STRING before the hexadecimal value that is between []. Enabled only when the checkbox <i>Use TCP/IP Blockdriver</i> is not selected.	'0000'	This field is a STRING and it accepts any characters, as done in the PLC name configuration in the <i>Device Communication Settings</i> tab. It allows up to 49 characters.
IP Address Active	IP address of the PLC. Enabled only when the checkbox <i>Use TCP/IP Blockdriver</i> is selected. It is used only when the setting is not redundant.	192.168.15.1	0.0.0.0 to 255.255.255.255

Device Configuration	Description	Default Setting	Options
IP Address PLC A	IP address of the PLC A. Enabled only when the configuration is redundant. It is the primary PLC address to which the server will communicate if there is no failure.	192.168.15.69	0.0.0.0 to 255.255.255.255
IP Address PLC B	IP address of the PLC B. Enabled only when the configuration is redundant. It is the secondary PLC address to which the server will communicate if a failure occurs.	192.168.15.70	0.0.0.0 to 255.255.255.255
Device Port	TCP Port. Enabled only when the checkbox <i>Use TCP/IP Blockdriver</i> is selected.	11740	11740 or 11739

Table 127: Configuration Parameter of each PLC for the OPC DA Server

When a new PLC needs to be configured on the OPC DA Server, simply press the *New Device* button and the configuration will be created. When the setup screen is accessed, a list of all PLCs already configured on the OPC DA Server will be displayed. Existing configurations can be edited by selecting the PLC in the *Devices* list and editing the parameters. The PLCs settings that are no longer in use can be deleted. The maximum number of PLCs configured in an OPC DA Server is 16.

If the automation architecture used specifies that the OPC DA Server must be ran on a computer that does not execute communication with the PLC via MasterTool IEC XE, the tool must be installed on this computer to allow OPC DA Server configuration in the same way as done in other situations.

ATTENTION

To store the OPC DA Server configuration, the MasterTool IEC XE must be run with administrator rights on the Operational System. Depending on the OS version, this privilege must be done in the moment that the program is executed: right-click the MasterTool IEC XE icon and choose *Run as Administrator*.

ATTENTION

The settings of a PLC on the OPC DA Server are not stored in the project created in MasterTool IEC XE. For this reason, it can be performed with an open or closed project. The settings are stored in a configuration file where the OPC DA Server is installed. When changing the settings, it is not required to load the application on the PLC, but depending on the OPC Client it may be necessary to reconnect to the server or load the settings for the data to be updated correctly.

5.8.10.2.1. *Importing a Project Configuration*

Using the button *Read Project Configuration*, as shown in Figure 102, you can assign the configuration of the open project to the PLC configuration that is being edited. For this option to work correctly, there must be an open project and an *Active Path* should be set as described in *Communication Settings*, present in the MasterTool IEC XE User Manual – MU299609. If any of these conditions is not met an error message will be displayed and no data will be modified.

When the above conditions are valid, the PLC settings receive the parameters of the opened project. The *IP Address* and *Gateway Port* information are configured as described in *Communication Settings* according to the *Active Path*. However, the *IP Address* settings are read from NET 1 Ethernet interface settings. The port for connection to the PLC is always assigned in this case as 11740.

5.8.10.3. OPC DA Communication Status and Quality Variables

For each PLC created in the OPC DA Server, status variables are generated, named `_CommState` and `_CommStateOK`. The `_CommState` variable indicates the communication between the OPC and the PLC state. This state can be interpreted by the OPC Clients according to the table below.

State	Value	Description
STATE_TERMINATE	-1	If the communication between the OPC DA Server and the OPC Client is terminated, this value will be returned. When there's more than one OPC Client simultaneously connected, this return will occur on the disconnection of the latter connected one. Besides the fact that this state is in the variable, its value can't be visualized because it only changes when there's no longer a connection with the client.
STATE_PLC_NOT_CONNECTED	0	The PLC configured in the OPC DA Server is not connected. It can happen if the configuration is incorrect (wrong PLC and/or Gateway IP Address) or the PLC is unavailable in that moment.
STATE_PLC_CONNECTED	1	The PLC configured in the OPC DA Server is connected. This is a transitory state during the connection.
STATE_NO_SYMBOLS	2	There are no symbols (variables) available in the PLC configured in the OPC DA Server. It can happen when there are no symbols or there isn't a project loaded on the PLC.
STATE_SYMBOLS_LOADED	3	Finished the process of reading the symbols (variables) from the PLC configured in the OPC DA Server. This is a transitory state during the connection.
STATE_RUNNING	4	After the reading of the symbols (variables) the OPC DA Server is running the periodic update of the values of the available symbols in each configured PLC.
STATE_DISCONNECT	5	There has been a disconnection with the PLC configured in the OPC DA Server.
STATE_NO_CONFIGURATION	6	When the OPC configuration (stored in an OPCServer.ini file) has a wrong syntax, the variable value will be this. Generally, this behavior is not observed for the Master-Tool IEC XE maintains this configuration valid.

Table 128: Description of the Communication states between OPC DA Server and the PLC

The `_CommStateOK` is a variable of the Bool type that indicates if the communication between the OPC DA Server and the PLC is working. When the value is TRUE, it indicates that the communication is working correctly. If the value is FALSE, for some reason it isn't possible to communicate with the PLC.

In addition to monitoring the communication status, the OPC Client can access information on the quality of communication. The quality bits form a byte. They are divided into three groups of bits: *Quality*, *Substatus* and *Limit*. The bits are distributed as follows *QQSSSLL*, in which *QQ* are the *Quality* bits, *SSSS* *Substatus* bits and *LL* *Limit* bits. In this case the *QQ* bits are the most significant in the byte, while the *LL* bits are the least significant.

QQ	Bits values	Definition	Description
0	00SSSSLL	Bad	The value read can't be used because there's some problem with the connection. It's possible to monitor the value of <i>_CommState</i> and diagnose the problem.
1	01SSSSLL	Uncertain	The quality can't be defined and may be presented in the <i>Substatus</i> field.
2	10SSSSLL	NA	This value is reserved and isn't used by the OPC standard.
3	11SSSSLL	Good	The quality is good and the value read can be used.

Table 129: Description of the OPC Quality value

Table 129 presents the possible quality values. The OPC DA Server only returns *Good* and *Bad* Quality values. A OPC Client can maintain the quality as *Uncertain* due to failures in which it can't establish a connection to the Server. In case of monitoring of the 8 quality bits directly from the OPC DA Server, the *Substatus* and *Limit* fields shall be null and the *Good* Quality will be presented as the value 192 and the *Bad* Quality will be value 0.

5.8.10.4. Limits of Communication with OPC DA Server

The table below presents the OPC DA Server configuration limits.

Maximum number of variables communicating with a single PLC	-
Maximum number of PLCs in an OPC DA Server	16
Maximum number of simultaneous connections of an OPC DA Server in a single PLC	8

Table 130: OPC DA Server Communication Limits

Note:

Maximum number of variables communicating with a single PLC: There is no configuration limit. The maximum possible number of variables depends on the processing capacity of the device.

ATTENTION

The Maximum number of simultaneous connections of an OPC DA Server in a single PLC is shared with connections made with the MasterTool IEC XE. I.e. the sum of connections of OPC DA Server and MasterTool IEC XE should not exceed the maximum quantity defined in Table 130.

The communication between the OPC DA Server and the PLC uses the same protocol used in the MasterTool IEC XE communication with the PLC. This protocol is only available for the Ethernet interfaces of the Nexto Series CPUs, it's not possible to establish this kind of communication with the Ethernet expansion modules.

When a communication between the OPC DA Server and the PLC is established, these two elements start a series of transactions aimed at solving the addresses of each declared variables, optimizing the communication in data reading regime. Besides, it's also resolved in this stage the communication groups used by some Clients in order to optimize the communication. This initial process demands some time and depends on the quantity of mapped variables and the processing capacity of the device.

5.8.10.5. Accessing Data Through an OPC DA Client

After the configuration of the OPC DA Server, the available data on all PLCs can be accessed via an OPC Client. In the configuration of the OPC Client, the name of the OPC DA Server must be selected. In this case the name is *CoDeSys.OPC.DA*.

The figure below shows the server selection on the client driver of the BluePlant SCADA software.

ATTENTION

The same way that in MasterTool IEC XE, some tools must be executed with administrator privileges in the Operational System for the correct functioning of the OPC Client. Depending on the OS version, this privilege must be activated in the moment that the program is executed. To do this, right-click MasterTool IEC XE icon and choose *Run as Administrator*.

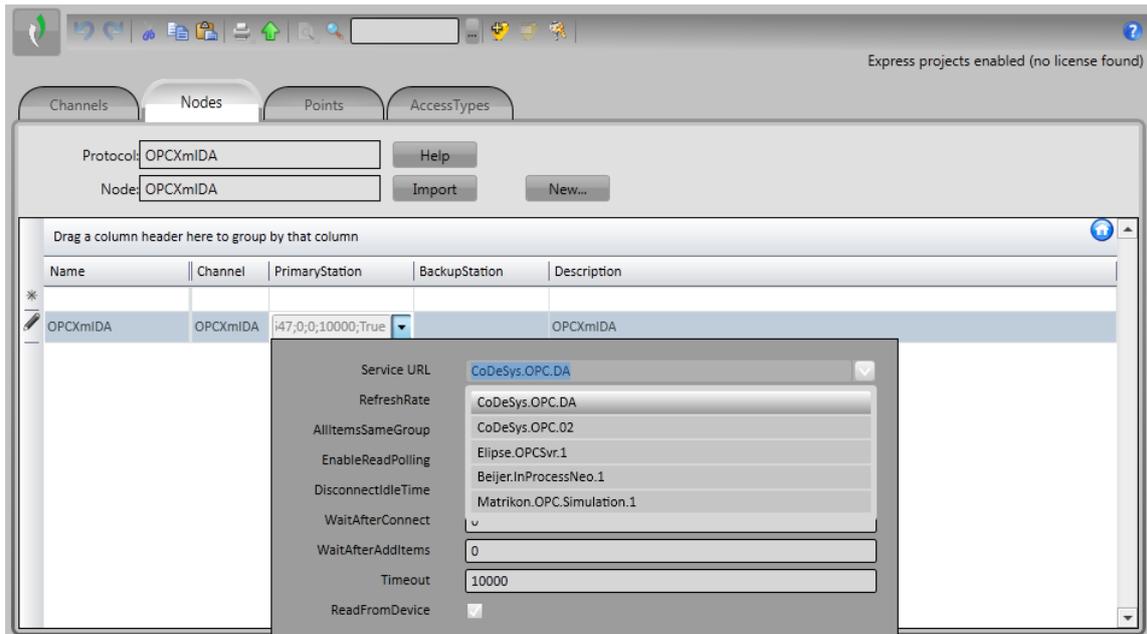


Figure 103: Selecting the OPC DA Server in the Client Configuration

In cases where the server is remotely located, it may be necessary to add the network path or IP address of the computer in which the server is installed. In these cases, there are two configuration options. The first is to directly configure it, being necessary to enable the COM/DCOM Windows Service. However, a simpler way is to use a tunneller tool that abstracts the COM/DCOM settings, and enable a more secure communication between the Client and the Server. For more information on this type of tool, refer to the *NAP151 - Tunneller OPC*.

Once the Client connects with the Server, it's possible to use the TAGs import commands. These commands consult the information declared in the PLC, returning a list with all the symbols available in it.

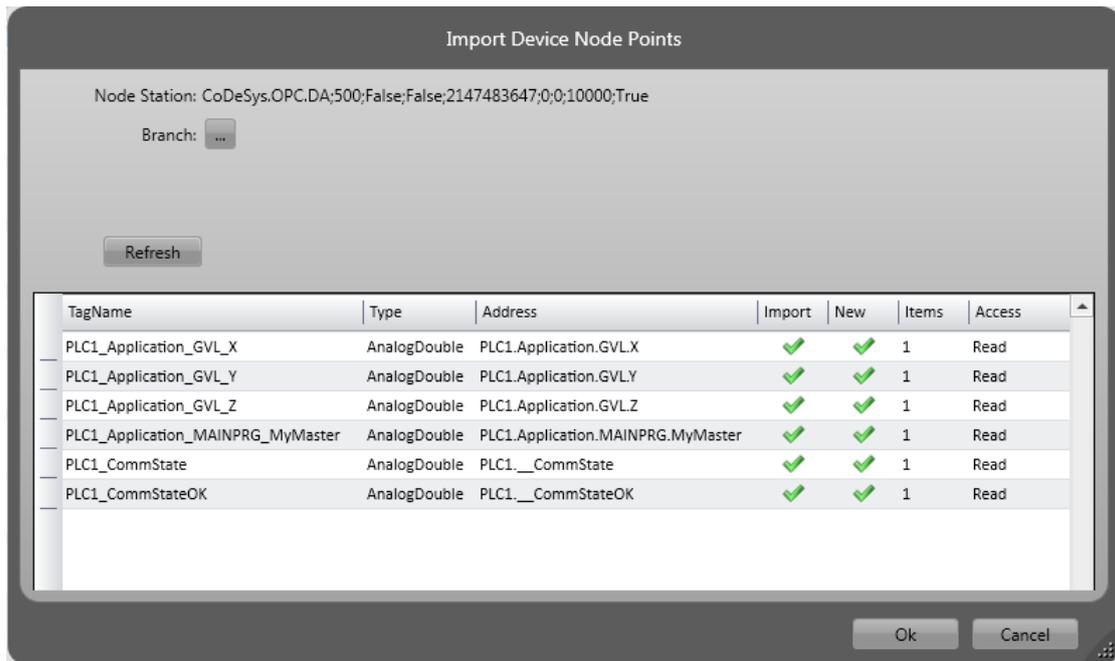


Figure 104: Symbols list consulted by the OPC Client

The list of selected variables will be included in the Client communication list and can be used, for example, in a SCADA system screen.

ATTENTION

The simulation mode of MasterTool IEC XE software can be used for OPC communication tests. The information on how to configure it are presented in the *Testing an OPC Communication using the Simulator* section of the MasterTool IEC XE User Manual – MU299609.

5.8.11. OPC UA Server

The OPC UA protocol is an evolution of the OPC family. Independent of platform, it is designed to be the new standard used in industrial communications.

Based on the client/server architecture, the OPC UA protocol offers numerous advantages in the development of design and facilities in communication with the automation systems.

When it comes to project development, configuring communication and exchanging information between systems is extremely simple using OPC UA technology. Using other address-based drivers, it is necessary to create tables to relate the supervision system tags and programmable controller variables. When data areas change during project development, it is necessary to redo the mappings and new tables with the relationships between the PLC information and the SCADA system.

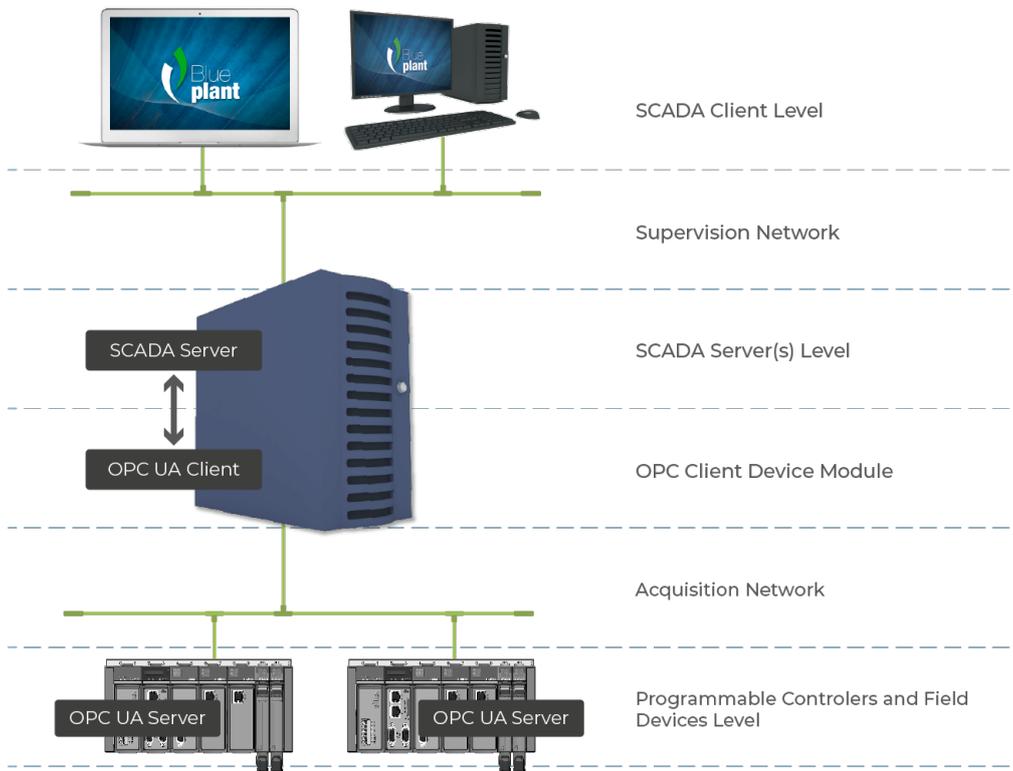


Figure 105: OPC UA Architecture

The figure above presents a typical architecture for SCADA system communication and PLCs in automation design. All roles present in the communication are explicit in this figure regardless of where they are running, they may be on the same equipment or on different equipment. Each of the roles of this architecture is described in table below.

Role	Description
Programmable Controllers and Field Devices Level	The field devices and the PLCs are where the operation state and plant control information are stored. The SCADA system access the information on these devices and store on the SCADA server, so that the SCADA clients can consult it during the plant operation.
OPC UA Server Modules	The OPC UA Server is an internal module of the PLCs responsible for receiving the OPC UA requests and translating them for communication with the field devices.
Acquisition Network	The acquisition network is the network in which OPC UA messages travel to request the data that is collected from the PLCs and field devices.
OPC Client Device Module	The OPC UA Client module, which is part of the SCADA Server, is responsible for making requests to the OPC UA Servers using the OPC UA protocol. The data collected by it is stored in the SCADA Server database.

Role	Description
SCADA Server Level	The SCADA Server is responsible for connecting to the various communication devices and store the data collected by them on a database, so that it can be consulted by the SCADA Clients.
Supervision Network	The supervisory network is the network by which SCADA Clients are connected to SCADA Servers, often using a proprietary SCADA system protocol. In a topology in which multiple Clients are not used or the Server and Client are installed in the same equipment, there is no such network, and in this case this equipment must directly use the OPC UA protocol for communication with the PLC.
SCADA Client Level	The SCADA Clients are responsible for requesting to the SCADA Servers the necessary data to be shown in a screen where the operation of a plant is being executed. Through then it is possible to execute readings and writings on data stored on the SCADA Server database.

Table 131: Roles Description on an OPC UA Server Architecture

When using the OPC UA protocol, the relationship between the tags of the supervisory systems and the process data in the controller variables is completely transparent. This means that if data areas change during project development, there is no need to re-establish relationships between PLC information and SCADA. Simply use the new variable provided by the PLC in the systems that request this data.

The use of OPC UA offers greater productivity and connectivity with SCADA systems. It contributes to reduced application development time and maintenance costs. It also enables the insertion of new data in the communication in a simplified way with greater flexibility and interoperability among the automation systems as it is an open standard.

It is worth noting that the OPC UA is only available on the integrated Ethernet interfaces of the Nexto CPUs. Ethernet expansion modules do not support this functionality.

5.8.11.1. Creating a Project for OPC UA Communication

The steps for creating a project with OPC UA are very similar to the steps described in the section [Creating a Project for OPC DA Communication](#). As with the OPC DA protocol, the configuration of the OPC UA protocol is based on the configuration of the *Symbol Configuration*. To enable the OPC UA, simply enable the *Support OPC UA Features* option in the configuration, as shown in figure below.

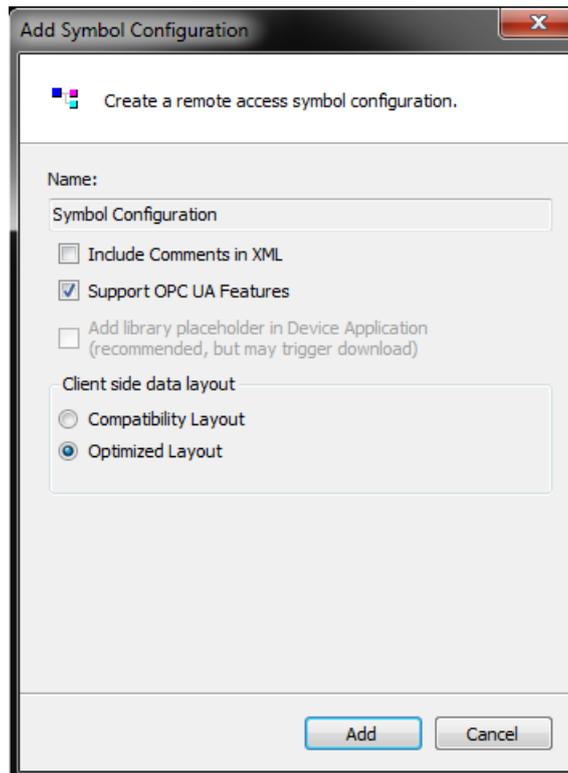


Figure 106: Symbol Configuration Object

ATTENTION

When enabling OPC UA protocol support, OPC DA protocol support is still enabled. You can enable OPC UA and OPC DA communications at the same time to report the variables configured on the *Symbol Configuration* object or via attributes.

Another way to access this configuration, once already created a project with the *Symbol Configuration* object, is given by accessing the *Settings* menu of the configuration tab of the *Symbol Configuration*. Simply select the option *Support OPC UA features* to enable support for the OPC UA protocol, as shown in figure below.

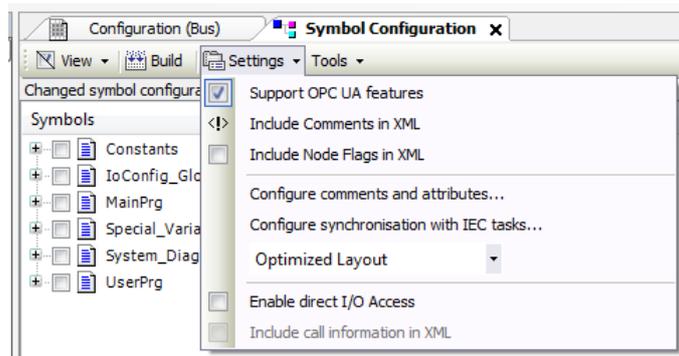


Figure 107: Enabling OPC UA in Object Symbol Configuration

After this procedure the project can be loaded into a PLC and the selected variables will be available for communication with the OPC UA Server.

5.8.11.2. Types of Supported Variables

This section defines the types of variables that support communication via the OPC UA protocol, when declared within GVLs or POU's and selected in the *Symbol Configuration* object (see previous section).

The following types of simple variables are supported:

- BOOL
- SINT
- USINT / BYTE
- INT
- UINT / WORD
- DINT
- UDINT / DWORD
- LINT
- ULINT / LWORD
- REAL
- LREAL
- STRING
- TIME
- LTIME

You can also use structured types (STRUCTs or Function Blocks) created from previous simple types.

Finally, it is also possible to create arrays of simple types or of structured types.

5.8.11.3. Limit Connected Clients on the OPC UA Server

The maximum number of OPC UA clients connected simultaneously in a PLC is 8 (eight).

5.8.11.4. Limit of Communication Variables on the OPC UA Server

There is no configuration limit. The maximum possible number of variables depends on the processing capacity of the device.

When a communication is established between the OPC UA Server and the PLC, these two elements initiate a series of transactions that aim to solve the address of each declared variable, optimizing the communication in regime of reading of data. In addition, at this stage, the classifications of the communication groups used by some Clients are also resolved in order to optimize communication. This initial process takes some time and depends on the amount of variables mapped and the processing capacity of the device.

5.8.11.5. Encryption Settings

If desired, the user can configure encryption for OPC UA communication using the *Basic256SHA256* profile, for a secure connection (cyber security).

To configure encryption on an OPC UA server, you must create a certificate for it using the following steps in the MasterTool programmer:

1. Define an active path for communication with the controller (no login required);
2. From the *View* menu, select *Security Screen*;
3. Click the *Devices* tab on the left side of this screen;
4. Click the icon  to perform a refresh;
5. Click on the *Device* icon, below which will open several certificates (*Own Certificates*, *Trusted Certificates*, *Untrusted Certificates*, *Quarantined Certificates*);
6. Click the icon  to generate a certificate and select the following parameters:
 - *Key length* (bit): 3072
 - *Validity period* (days): 365 (can be modified if desired)
7. Wait while the certificate is calculated and transferred to the controller (this may take a few minutes);
8. Reboot the controller.
9. On the OPC UA client, perform the necessary procedures to connect to the OPC UA server and generate a certificate with the *Basic256Sha256* profile (see specific OPC UA client manual for details);

10. Back to MasterTool, click on the icon  of the *Security Screen* to perform a refresh;
11. On the *Security Screen*, select the "*Quarantined Certificates*" folder under the *Device*. In the right panel you should observe a certificate requested by the OPC UA client;
12. Drag this certificate to the folder "*Trusted Certificates*";
13. Proceed with the settings in the OPC UA client (see specific OPC UA client manual for details).

To remove encryption previously configured on a controller, you must do the following:

1. Define an active path for communication with the controller (no login required);
2. From menu *View*, select *Security Screen*;
3. Click on the *Devices* on the left side of this screen;
4. Click the icon  to perform a refresh;
5. Click on the *Device* icon, below which will open several certificates (*Own Certificates*, *Trusted Certificates*, *Untrusted Certificates*, *Quarantined Certificates*);
6. Click the folder "*Own Certificates*" and in the right panel select the certificate (OPC UA Server);
7. Click the icon  to remove this project and driver certificate;
8. Reset (turn off and on) the controller.

5.8.11.6. Main Communication Parameters Adjusted in an OPC UA Client

Some OPC UA communication parameters are configured on the OPC UA client, and negotiated with the OPC UA server at the time the connection between both is established. The following subsections describe the main OPC UA communication parameters, their meaning, and care to select appropriate values for them.

In an OPC UA client it is possible to group the variables of a server into different *subscriptions*. Each *subscription* is a set of variables that are reported in a single communication packet (*PublishResponse*) sent from the server to the client. The selection of the variables that will compose each subscription is made in the OPC UA client.

ATTENTION

Grouping variables into multiple *subscriptions* is interesting for optimizing the processing capacity and consumption of Ethernet communication bandwidth. Such aspects of optimization are analyzed in greater depth in the OPC UA Server user manual MU214609, where some rules for the composition of *subscriptions* are suggested. This user manual also discusses in more depth several concepts about the OPC UA protocol.

Some of the communication parameters described below must be defined for the server as a whole, others for each *subscription*, and others for each variable that makes up a *subscription*.

5.8.11.6.1. Endpoint URL

This parameter defines the IP address and TCP port of the server, for example:

```
opc.tcp://192.168.17.2:4840
```

In this example, the IP address of the controller is 192.168.17.2.

The TCP port should always be 4840.

5.8.11.6.2. Publishing Interval (ms) and Sampling Interval (ms)

The *Publishing Interval* parameter (unit: milliseconds) must be set for each *subscription*.

The *Sampling Interval* parameter must be set for each variable (unit: milliseconds). However, in many OPC UA clients, the *Sampling Interval* parameter can be defined for a *subscription*, being the same for all the variables grouped in the *subscription*.

Only the variables of a *subscription* whose values have been modified are reported to the client through a *Publish Response* communication packet. The *Publishing Interval* parameter defines the minimum interval between consecutive *Publish Response* packets of the same *subscription*, in order to limit the consumption of processing and Ethernet communication bandwidth.

To find out which subscription variables have changed and are to be reported to the client in the next *Publish Response* packet, the server must perform comparisons, and such (*samplings*) are performed by the same with the *Sampling Interval*. It is recommended that the value of *Sampling Interval* varies between 50% and 100% of the value of the *Publishing Interval*, because there is a relatively high processing consumption associated with the comparison process executed in each *Sampling Interval*.

It can be said that the sum between *Publishing Interval* and *Sampling Interval* is the maximum delay between changing a value on the server and the transmission of the *Publish Response* packet that reports this change. Half of this sum is the average delay between changing a value on the server and the transmission of the *Publish Response* packet that reports this change.

5.8.11.6.3. Lifetime Count and Keep-Alive Count

These two parameters must be configured for each *subscription*.

The purpose of these two parameters is to create a mechanism for deactivating a *subscription* on the initiative of the server, in case it does not receive customer's *PublishRequest* communication packets for this *subscription* for a long time. *PublishRequest* packets must be received by the server so that it can broadcast *Publish Response* packets containing the subscription variables that have changed their values.

If the server does not receive *PublishRequest* packets for a time greater than *Lifetime Count* multiplied by *Publishing Interval*, the server deactivates the *subscription*, which must be re-created by the client in the future if desired.

In situations where the variables of a *subscription* do not change, it could be a long time without the transmission of *PublishResponses* and consequently *PublishRequests* that succeed, causing an undesired deactivation of the *subscription*. To prevent this from happening, the *Keep-Alive Count* parameter was created. If there are no *subscription* data changes for a time equal to *Keep-Alive Count* multiplied by *Publishing Interval*, the server will send a small empty *Publish Response* packet indicating that no variable has changed. This empty *Publish Response* will authorize the client to immediately send the next *PublishRequest*.

The *Keep-Alive Count* value must be less than the *Lifetime Count* value to prevent unwanted deactivation of the *subscription*. It is suggested that *LifeTime Count* be at least 3 times larger than *Keep-Alive Count*.

5.8.11.6.4. Queue Size and Discard Oldest

These parameters must be maintained with the following fixed values, which are usually the default values on the clients:

- Queue Size: 1
- Discard Oldest: enable

According to the OPC UA standard, it is possible to define these parameters for each variable. However, many clients allow you to define common values for all variables configured in a *subscription*.

Queue Size must be retained with value 1 because there is no event support in this implementation of the OPC UA server, so it is unnecessary to define a queue. Increasing the value of *Queue Size* may imply increase communication bandwidth and CPU processing, and this should be avoided.

Discard Oldest must be maintained with the *enable* value, so that the *Publish Response* package always reports the most recent change of value detected for each variable.

5.8.11.6.5. Filter Type and Deadband Type

These parameters must be maintained with the following fixed values, which are usually the default values in the clients:

- Filter Type: *DataChangeFilter*
- Deadband Type: *none*

According to the OPC UA standard, it is possible to define these parameters for each variable. However, many clients allow you to define common values for all variables configured in a *subscription*.

The *Filter Type* parameter must be of *DataChangeFilter*, indicating that value changes in the variables should cause it to be transmitted in a *Publish Response* package.

Deadband Type should be kept in "*none*" because there is no implementation of *deadbands* for analog variables. In this way, any change of the analog variable, however minimal, causes its transmission in a *Publish Response* package.

To reduce processing power and Ethernet communication bandwidth, you can deploy *deadbands* on your own as follows:

- Do not include the analog variable in a *subscription*;
- Instead, include in a *subscription* an auxiliary variable linked to the analog variable;
- Copy the analog variable to the auxiliary variable only when the user-managed *deadband* is extrapolated.

5.8.11.6.6. PublishingEnabled, MaxNotificationsPerPublish and Priority

It is suggested that the following parameters be maintained with the following values, which are usually the default values in the clients:

- *PublishingEnabled*: *true*
- *MaxNotificationsPerPublish*: *0*
- *Priority*: *0*

These parameters must be configured for each *subscription*.

PublishingEnable must be “true” so that the *subscription* variables are reported in case of change of value.

MaxNotificationsPerPublish indicates how many of the variables that have changed value can be included in the same *Publish Response* package. The special value “0” indicates that there is no limit to this, and it is recommended to use this value so that all changed variables are reported in the same *Publish Response* package.

Priority indicates the relative priority of this *subscription* over others. If at any given moment the server should send multiple *Publish Response* packages of different *subscriptions*, it will prioritize the one with the highest value of priority. If all *subscriptions* have the same priority, *Publish Response* packets will be transmitted in a fixed sequence.

5.8.11.7. Accessing Data Through an OPC UA Client

After configuration of the OPC UA Server the data available in all PLCs can be accessed via a Client OPC UA. In the configuration of the OPC UA Client, the address of the correct OPC UA Server must be selected. In this case the address *opc.tcp://ip-address-of-device:4840*. The figure below shows the server selection in the SCADA BluePlant client software driver.

ATTENTION

Like MasterTool IEC XE, some tools need to be run with administrator rights on the Operating System for the correct operation of the OPC UA Client. Depending on the version of the Operating System this right must be authorized when running the program. For this operation right click on the tool executable and choose the option *Run as administrator*.

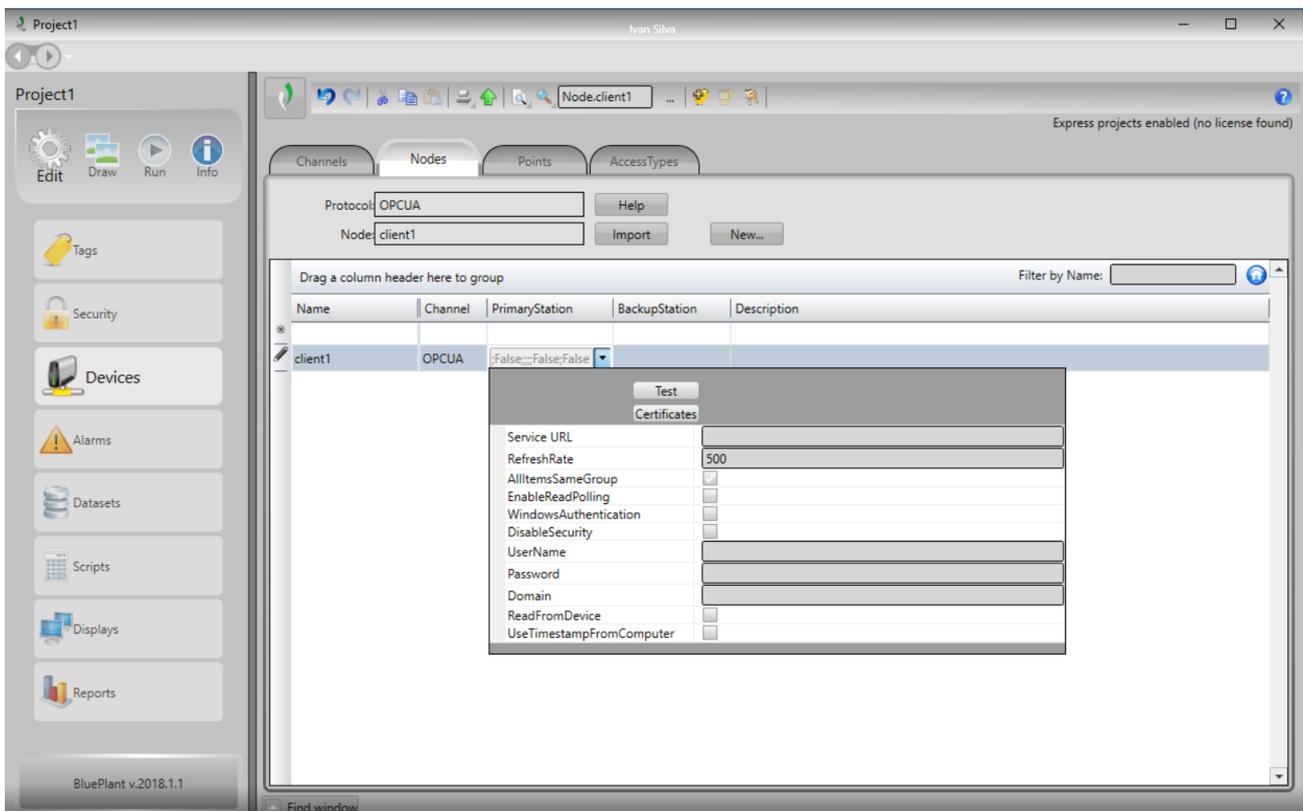


Figure 108: Selecting OPC UA Server in Client Configuration

Once the Client connects to the Server, TAG import commands can be used. These commands query information declared in the PLC, returning a list with all the symbols made available by the PLC.

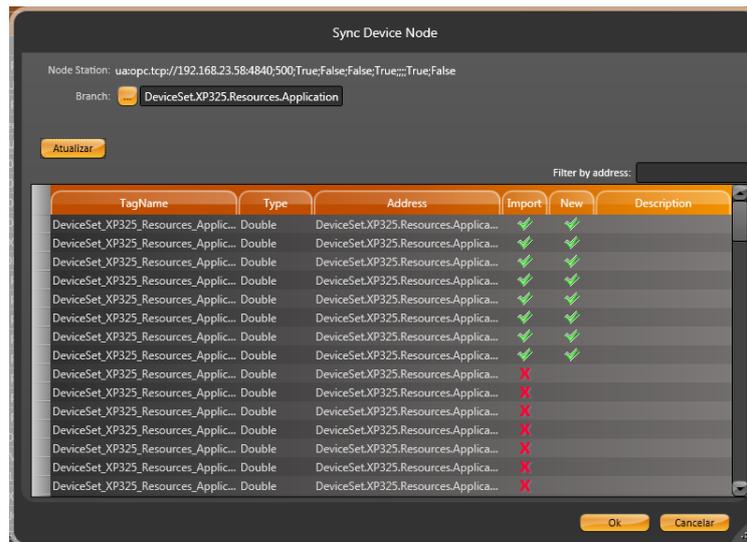


Figure 109: List of Symbols Browsed by OPC UA

The list of selected variables will be included in the Client's communications list and can be used, for example, in screens of a SCADA system.

5.8.12. EtherCAT Master

EtherCAT (*Ethernet Control Automation Technology*) is a master-slave architecture protocol with high performance, for deterministic Ethernet, that allows real time performance as it updates 1000 distributed I/O in 30 μ S or 100 servomotors axis each 100 μ S using twisted pair cables or optic fiber. Besides, it supports flexible topology, allowing for line, tree and/or star connections.

An Ethernet frame can be processed in real time instead of being received, interpreted and copied as process data in each connection. The FMMU (*Fieldbus Memory Management Unit*) in each Slave node reads the data that are addressed to it at the same time that the telegram is forwarded to the next device. In a similar way, the input data are inserted as the telegram is passed. Because of this, the frames are delayed just a few nanoseconds. Access on the Ethernet terminals can be made in any order as the data sequence is independent of the physical order. It can perform Broadcast, Multicast and between slaves communications.

The EtherCAT protocol allows a precise synchronization, that is required, for example, in applications where several axis simultaneously perform coordinated movements, it can be done through an exact adjust of the *Distributed Clock*. There's also the possibility to configure devices that, as opposed to synchronous communication, have an elevated tolerance degree inside the communication system.

The configuration of EtherCAT modules is initially determined by the *Device Description Files* of the Master and Slave devices used, and can be modified by the user in the *Configuration Editor* dialog boxes. However, for conventional applications and with the desire of an as easy as possible manipulation, large-scale configurations can be automated by choosing the *Autoconfig* mode in [EtherCAT Master - General](#).

Note the possibility of modifying the Master and Slave configuration parameters also in operational mode, through the Master and Slave instances, according to the availability of the device in question.

5.8.12.1. Installing and inserting EtherCAT Devices

In order to be able to insert and configure EtherCAT devices as objects in the device tree, the Slave devices must be installed.

The Master device is automatically installed by the default MasterTool IEC XE installation. The EtherCAT Master defines which Slaves can be inserted.

To install the Slave devices the *Device Repository* must be opened, use the *EtherCAT XML Device description Configuration File (*.xml)* filter and select the device description files (*EtherCAT XML Device Description / ESI EtherCAT Slave Information*), supplied with the hardware. The Slave descriptions are available as XML files (file type: *.xml).

An EtherCAT Master can be added to the *Devices Tree* through the *Add Device* command, through the context menu of the CPU NET connectors.

Under a master, one or more slaves can be added, selecting an EtherCAT Master and running the *Add Device* command (context menu of the EtherCAT Master) or running the *Scan For Devices* command.

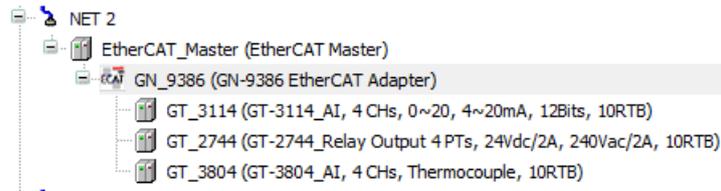


Figure 110: EtherCAT Configuration Example

ATTENTION

- Only one EtherCAT Master instance per project is allowed.
- Only available on the NET connectors of the PLC.
- It cannot be used when the NETs are set as redundant.
- It cannot be used when Project has cluster redundancy.
- Other drivers cannot be instantiated in the same NET port as the EtherCAT Master.

5.8.12.1.1. EtherCAT - Scan Devices

The *Scan For Devices* command, available in the EtherCAT Master context menu, runs a search for the Slave devices physically installed in the EtherCAT network of the PLC currently connected. This means that with this command it's possible to detect and visualize the hardware components in the window presented in the figure below, allowing the user to map them directly in the project *Device Tree* do projeto.

It's noteworthy that, when the *Scan For Devices* command is selected, a connection with the PLC will be automatically established before the search begins and terminated when the search ends. So, for the first execution of this command, the Gateway connection must be configured and a program with the EtherCAT Master configured must be loaded into the PLC. In case of future additions of Slave devices, in order to run this command, it's necessary that the EtherCAT network is stopped. To do this, put to TRUE the *bStopBus* bit, present in the variables of the EtherCAT Master Diagnostics.

When the command is executed, the *Scanned Devices* field will contain a list of all devices and modules found during the last scan. To add them to the project, just click on the button *Copy All Devices To Project*. It's also possible to perform a comparison of the devices found in the search with the ones in the project by selecting the box *Show differences to project*.

If you add an EtherCAT Master module to the Project and use the *Scan For Devices* command, you will have a list of all the available EtherCAT Slaves. Entries in bold will be shown, if there's more than one device with the same description. With a double click on the entrance a list will open, and so the desired device can be selected.

After completing the changes in the EtherCAT network configuration, it's necessary to do a new project download, for the changes to take effect.

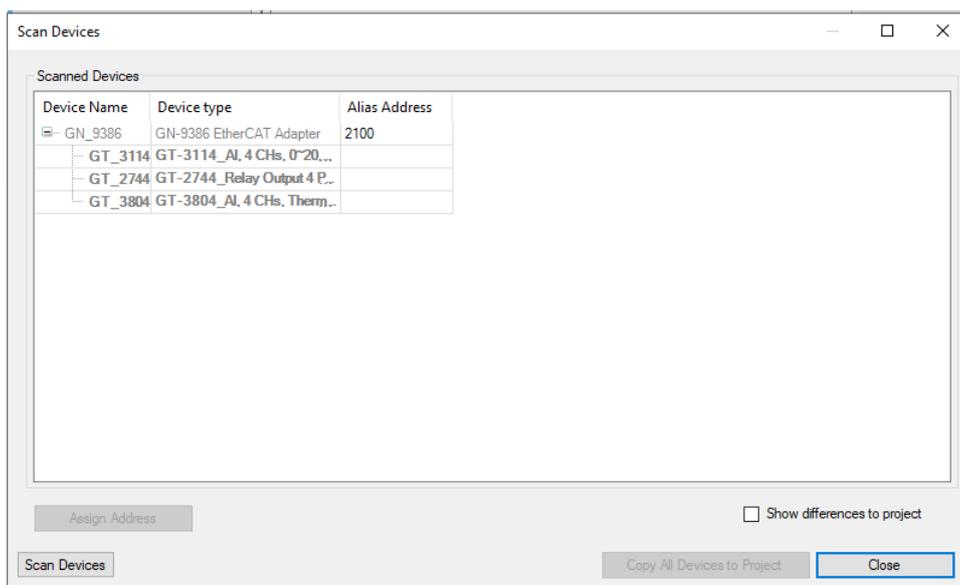


Figure 111: EtherCAT Devices Search Dialog

5.8.12.2. EtherCAT Master Settings

Below are listed the options to carry out the EtherCAT Master configuration, such as defined in *Device Description File*.

5.8.12.2.1. EtherCAT Master - General

Below are the general parameters found in the initial screen of the EtherCAT Master configuration, according figure below.

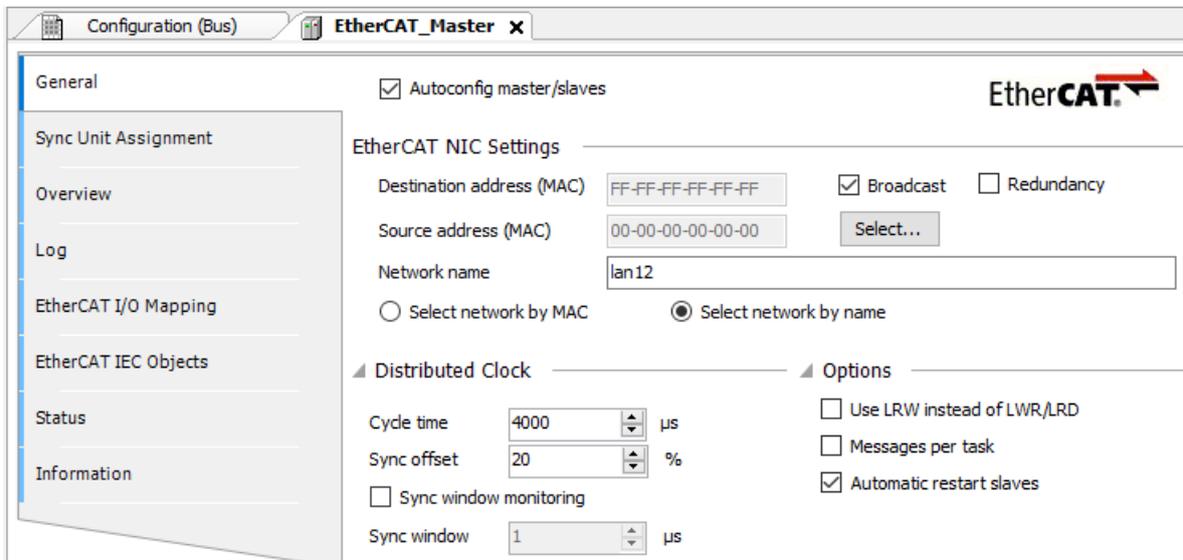


Figure 112: EtherCAT Master Configuration Dialog

Device Configuration	Description	Factory De- fault	Possible Values
Autoconfig master/slaves	Enable the Master and Slave automatic configuration.	Marked	Marked Unmarked
Cycle time [μs]	Sets the time period in which a new data telegram must be send to the bus.	4000	2000 to 1000000
Sync Offset [%]	Adjust the offset, from the PLC cycle, of the EtherCAT Slave synchronization interrupt.	20	-50 to 50
Sync window monitoring	If enabled, this option allows monitoring the Slave synchronization.	Unmarked	Marked Unmarked
Sync window [μs]	Time for the Sync Window Monitoring.	1	1 to 32768
Use LRW instead of LWR/LRD	Enabling of the combined read and write commands.	Unmarked	Marked Unmarked
Messages per task	If enabled, the read and write commands that are dealing with input and output messages can be done in different tasks.	Unmarked	Marked Unmarked

Device Configuration	Description	Factory Default	Possible Values
Automatic restart slaves	Restart the devices when the communication is aborted.	Marked	Marked Unmarked

Table 132: EtherCAT Master Configuration

Notes:

Autoconfig master/slaves: If this option is enabled, most of Master and Slave configuration will be made automatically, based on the description files and implicit calculations. In this case, the FMMU / Sync dialog will not be available. If it's unchecked the *Image In Address* and *Image Out Address* options will be available to the user.

ATTENTION

The *Autoconfig* mode is enabled by default and usually enough and highly recommended for standard applications. If it's disabled, all configuration definitions will have to be made manually, and thus, some specialized knowledge is required. To configure a Slave-to-Slave communication, the *Autoconfig* option must be disabled.

Cycle time: Time period after which, a new data telegram must be sent to the bus. If *Distributed Clock* functionality is enabled, the value of this parameter will be transferred to the Slaves clocks. This way, a precise data exchange synchronization can be achieved, which is especially important in cases where the distributed process demands simultaneous actions. So, a very precise time base, with a jitter significantly smaller than a microsecond, for all the network can be achieved.

Sync Offset: This value allows the adjustment of the offset of the EtherCAT Slave synchronization interrupt to the PLC cycle. Normally, the PLC task cycle begins 20% later than the Slaves synchronization interruption. This means that the PLC task can be delayed by 80% of the cycle time and no message will be lost.

Sync Window: If the synchronization of all Slaves are inside this time window, the EtherCAT Master *bDistributed-ClockInSync* diagnostic will be set to TRUE, otherwise it will be set to FALSE. When Distributed Clock is used, it's highly recommended to use a dedicated task with high priority as the *Bus cycle task* of the EtherCAT Master. To do this, it's necessary to use [Project Profiles](#) that allows the creation of new tasks, then create a cyclic task with priority 0 (real time task) and link it to the master *Bus cycle task* on the [EtherCAT Master - I/O Mapping](#) tab of the EtherCAT Master. The user can also change the value of the *wDCInSyncWindow* variable, configuring the maximum jitter allowed on the synchronization between master and slaves.

Use LRW instead of LWR/LRD: Activating this option enables the Slave-to-Slave communication because, instead of using separated reading (LRD) and write (LWR) commands, combined reading/writing (LRW) commands will be used.

Automatic Restart Slaves: By enabling this option, the Master will restart the Slaves as soon as the communication is aborted.

5.8.12.2.2. *EtherCAT Master - Sync Unit Assignment*

This tab of the EtherCAT Master configuration editor shows all slaves that are entered below a specific master with an assignment to the sync units.

With EtherCAT sync units, multiple slaves are configured into groups and subdivided into smaller units. For each group, the job counter can be monitored for better and more accurate error detection. As soon as a slave is missing from a group of synchronization units, the other slaves in the group are also shown as missing. Detection occurs immediately on the next bus cycle because the job counter is checked continuously. With device diagnostics, the missing group can be remedied as quickly as possible.

Unaffected groups remain operable without any interference.

5.8.12.2.3. *EtherCAT Master - Overview*

This tab of the EtherCAT Master configuration editor provides an overview of the states of all slaves, which are entered below this master and have an address. Modules are not displayed.

5.8.12.2.4. *EtherCAT Master - I/O Mapping*

This EtherCAT Master configuration editor tab offers the possibility to change the task that will be used for bus updates.

5.8.12.2.5. EtherCAT Master - IEC Objects

This tab of the EtherCAT Master configuration editor lists *objects* that allow access to the device from the IEC application. In online mode, this is used for monitoring.

5.8.12.2.6. EtherCAT Master - Status / Information Tabs

The Status tab of the EtherCAT Master configuration editor provides status information (e.g. 'Running', 'Stopped') and diagnostic messages specific of the device and the internal bus system.

The Information tab, present on the EtherCAT Master configuration editor, shows, if available, the following general information about the module: *Name, Vendor, Type, Version Number, Category, Order Number, Description, Image.*

5.8.12.3. EtherCAT Slave Configuration

Below are listed the main EtherCAT Slave configuration options, as defined in the *Device Description File.*

5.8.12.3.1. EtherCAT Slave - General

Below are presented the general parameters found in EtherCAT Slave configuration initial screen. This field is only available if the *Autoconfig* mode (Master) isn't enabled.

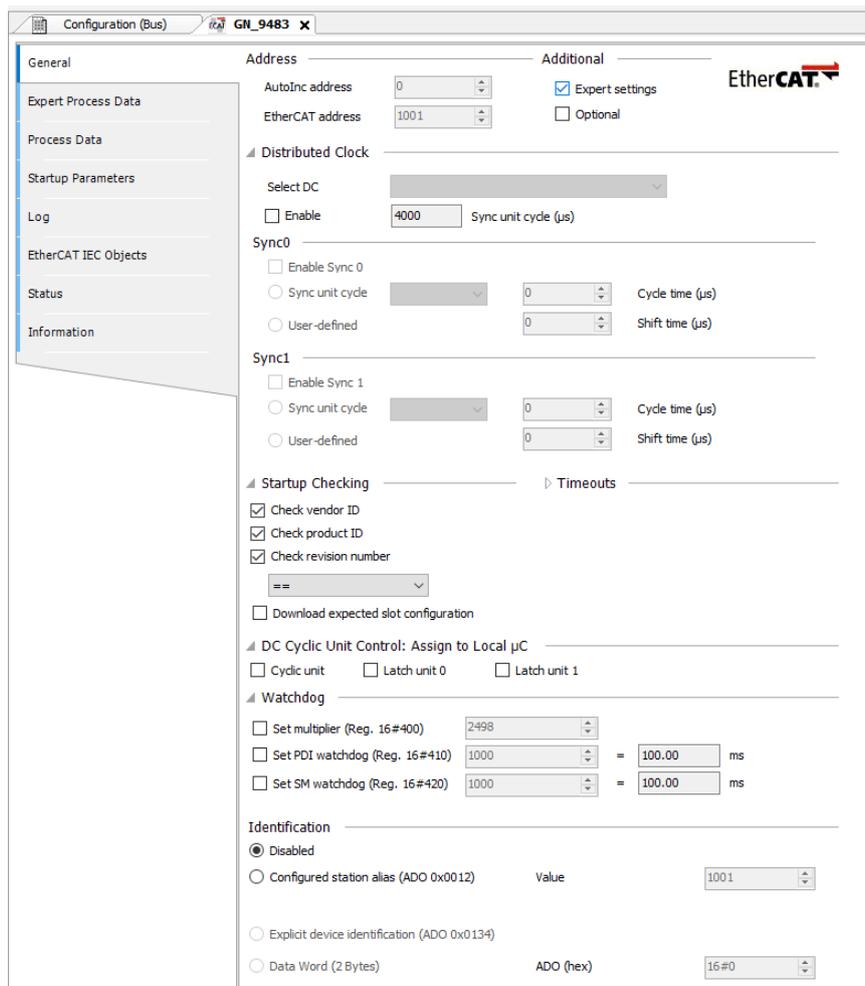


Figure 113: EtherCAT Slave Configuration Dialog

Device Configuration	Description	Default Value	Options
AutoInc Address	Auto incremental Address (16-bit) defined by the Slave position in the network.	-	-65535 to 0
EtherCAT Address	Slave final address, assign by the Master during startup. This address is independent from the position in the network.	-	1 to 65535
Expert settings	Enable the Slave advanced Settings options.	Unmarked	Marked Unmarked
Optional	Declare the Slave as Optional.	Unmarked	Marked Unmarked
Select DC	Show all Distributed Clock configurations provided by the device description file.	-	-
Enable Distributed Clock	Enable the Distributed Clock configuration options.	Unmarked	Marked Unmarked
Sync Unit Cycle [μs]	Show the Cycle Time set in Master.	100000	2000 to 1000000
Enable (Sync 0)	Enable the Sync 0 synchronization unit configurations.	Unmarked	Marked Unmarked
Sync Unit Cycle (Sync 0)	By selecting this option, the Cycle Time will be determined by the product of the factor and the Sync Unit Cycle.	Unmarked	Marked Unmarked
User Defined (Sync 0)	If this option is selected, the desired time, in microseconds, can be directly set into the Cycle Time (μ s) field.	Unmarked	Marked Unmarked
Cycle Time [μs] (Sync 0)	Show the cycle time currently set.	100000	1 to 2147483647
Shift Time [μs] (Sync 0)	Time between the sync events and the "Output Valid" or "Input Latch" time.	0	-2147483648 to 2147483647
Enable (Sync 1)	Enable the Sync 1 synchronization unit configurations.	Unmarked	Marked Unmarked
Sync Unit Cycle (Sync 1)	By selecting this option, the Cycle Time will be determined by the product of the factor and the Sync Unit Cycle.	Unmarked	Marked Unmarked
User Defined (Sync 1)	If this option is selected, the desired time, in microseconds, can be directly set into the Cycle Time (μ s) field.	Unmarked	Marked Unmarked
Cycle Time [μs] (Sync 1)	Show the cycle time currently set.	100000	1 to 2147483647

Device Configuration	Description	Default Value	Options
Shift Time [μ s] (Sync 1)	Time between the sync events and the “Output Valid” or “Input Latch” time.	0	-2147483648 to 2147483647
Check Vendor ID	If unmarked, it will disable the Vendor ID Check.	Marked	Marked Unmarked
Check Product ID	If unmarked, it will disable the Product ID Check.	Marked	Marked Unmarked
SDO Access	Set a time reference for the timeout check of a SDO Access.	-	0 to 100000
I -> P	Set a time reference for the timeout check of the switch from Init to Pre-Operation mode.	-	0 to 100000
P -> S/S -> O	Set a time reference for the timeout check of the switch from Pre-Operation to Safe-Operation and from Safe-Operation to Operational modes.	-	0 to 100000
Cyclic Unit	Set the Unit Cycle to the local microprocessor.	Unmarked	Marked Unmarked
Latch Unit 0	Set the Latch Unit 0 to the local microprocessor.	Unmarked	Marked Unmarked
Latch Unit 1	Set the Latch Unit 1 to the local microprocessor.	Unmarked	Marked Unmarked

Table 133: EtherCAT Slave Configurations

Notes:

AutoInc Address: This address is used only during startup, when the Master is assigning the EtherCAT addresses to the Slaves. When for this matter, the first telegram runs through the Slaves, each fast-read Slave increases its *AutoInc* Address by 1. The Slave with address 0 finally will receive the data.

Optional: If a Slave is declared as *Optional*, no error message will be created in case the device doesn't exist in the bus system. Thus a *Station alias* address must be defined and written to the EEPROM. This option is only available if the option *Autoconfig Master/Slaves* in the settings of the EtherCAT Master is activated and if this function is supported by the EtherCAT Slave.

Enable Distributed Clock: If the *Distributed Clock* functionality is enabled, the data exchange cycle time, displayed in the *Sync Unit Cycle (μ s)* field will be determined by the *Master Cycle Time*. Thus the master clock can synchronize the data exchange within the network. The settings for handling the synchronization unit(s) depend on the Slave.

Enable Sync 0: If this option is activated, the *Sync0* synchronization unit is used. A synchronization unit describes a set of process data which is exchanged synchronously.

Sync Unit Cycle (Sync 0): If this option is activated, the *Master Cycle Time*, multiplied by the chosen factor will be used as synchronization cycle time for the slave. The *Cycle Time (μ s)* field shows the currently set cycle time.

Shift Time: The Shift Time describes the time between the sync events (*Sync0*, *Sync1*) and the *Output Valid* or *Input Latch* times. Writable value, if the slave supports shifting of *Output Valid* or *Input Latch*.

Enable Sync 1: If this option is selected, the synchronization unit *Sync1* is used. A synchronization unit is a set of process data which is exchange synchronously.

Sync Unit Cycle (Sync1): If this option is activated, the *Master Cycle Time*, multiplied by the chosen factor will be used as synchronization cycle time for the slave. The *Cycle Time (μ s)* field shows the currently set cycle time.

Check Vendor ID and Product ID: By default, at startup of the system the *Vendor ID* and/or the *Product ID* will be checked against the current configured settings. If a mismatch is detected, the bus will be stopped and no further actions will be executed. This serves to avoid the download of an erroneous configuration. This option is intended to switch off the check, if necessary.

SDO Access: By default there's no timeout set for the SDO list submit action at system startup. However, if it's necessary to check if this action exceeds a certain time, it must be defined (in microseconds) in this field.

I -> P: By default there's no timeout set for the state transition from *Init* to *Pre-Operational*. However, if it's necessary to check if this action exceeds a certain time, it must be defined (in microseconds) in this field.

P -> S / S -> O: By default there's no timeout set for the state transition from *Pre-Operational* to *Safe-Operational* and from *Safe-Operational* to *Operational*. However, if it's necessary to check if this action exceeds a certain time, it must be defined (in microseconds) in this field.

DC cycle unit control: Choose the desired option(s) concerning the *Distributed Clock* functions in order to define, which should be assigned to the local microprocessor. The control is done in register 0x980 in the EtherCAT slave. The possible settings: *Cyclic Unit, Latch Unit 0, Latch Unit 1*.

Enable: If the setting *Optional* is not activated, this setting can be activated if explicitly supported by the device description of the slave. It allows direct assignment of an alias address in order to get the slaves address independent of its position within the bus. If the option *Optional* is activated, this checkbox is disabled.

5.8.12.3.2. EtherCAT Slave - Process Data

The *Process Data* tab of the EtherCAT Slave configurator editor shows the slave input and output process data, each defined by name, type and index by the device description file, as seen in figure below.

The selected input (to be read) and output (to be written) of the device are available in the [EtherCAT Slave - I/O Mapping](#) dialog as PLC inputs and outputs to which project variables might be mapped.

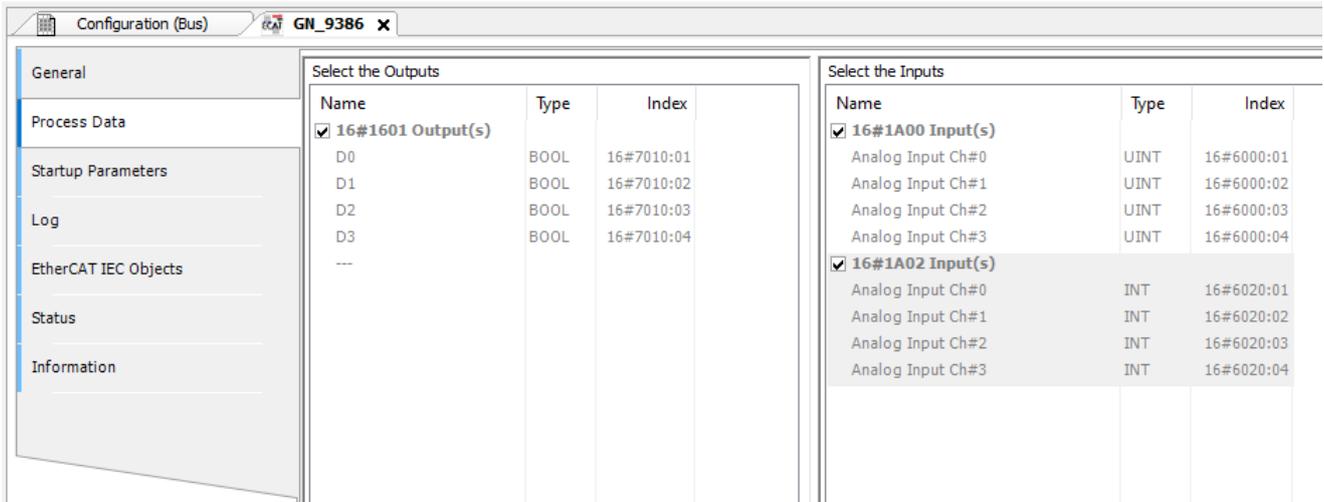


Figure 114: Process Data Dialog

The *Expert Process Data* dialog will only be available in the EtherCAT Slave configuration editor if the *Enable Expert Settings* option is activated. It provides another, more detailed, vision of the process data, adding to what is presented in the *Process Data* tab. Furthermore, the download of the *PDO Assignment* and the *PDO Configuration* can be activated in this dialog.

ATTENTION

If the Slave doesn't accept the PDO Configuration, it will stay in Pre-Operational state and none real time data exchange will be possible.

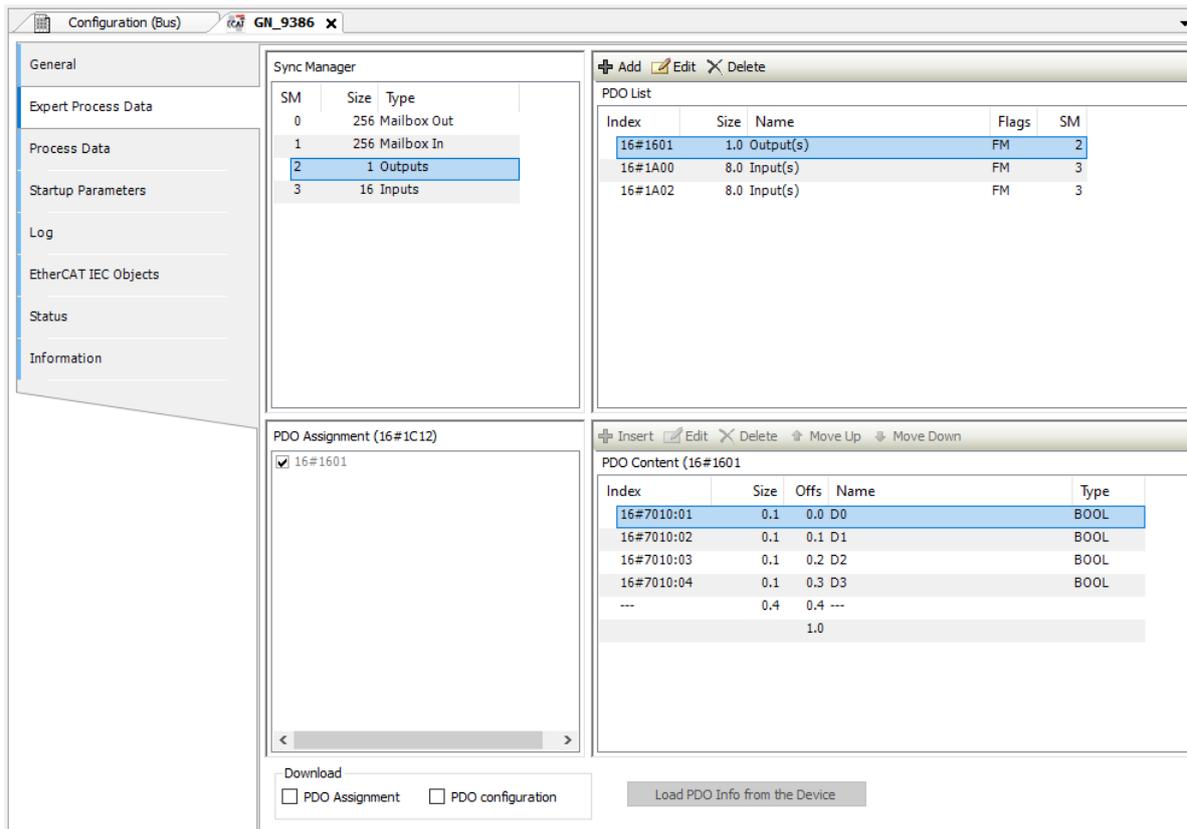


Figure 115: Expert Process Data Dialog

This dialog is divided in four sections and two options:

- *Sync Manager*: List of *Sync Manager* with data size and type of PDOs.
- *PDO Assignment*: List of PDOs assigned to the selected *Sync Manager*. The checkbox activates the PDO and I/O channels are created. It is similar to the simple PDO configuration windows. Here only PDOs can be enabled or disabled.
- *PDO List*: List of all PDOs defined in the device description file. Single PDOs can be deleted, edited or added by executing of the respective command from the context menu.
- *PDO Content*: Displays the content of the PDO selected in the section above. Entries can be deleted, edited or added by executing of the respective command from the context menu.
- *PDO Assignment*: If activated a CoE write command will be added to index 0x1CXX to write the PDO configuration 0x16XX or 0x1A00.
- *PDO Configuration*: If activated several CoE write commands will be added to write the PDO mapping to the slave.

ATTENTION

If a Slave doesn't support the PDO configuration, a download may result in a Slave error. This function should only be used by experts.

5.8.12.3.3. EtherCAT Slave - Edit PDO List

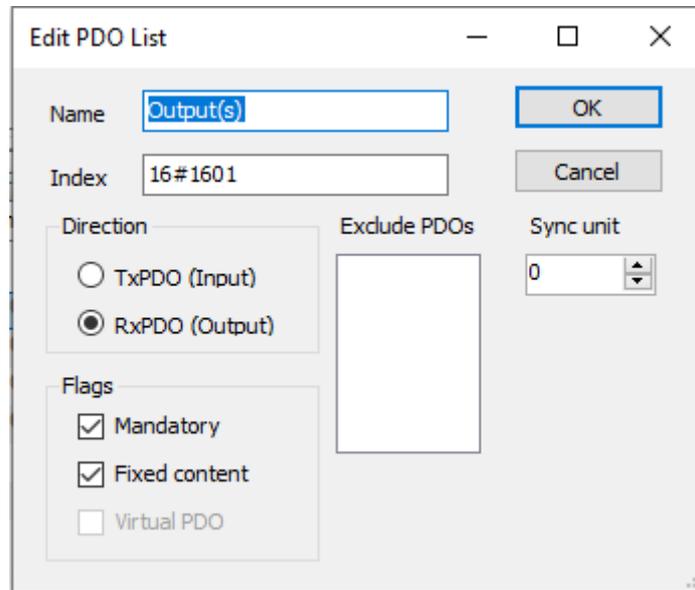


Figure 116: Edit PDO List Dialog

This dialog is opened through the context menu from the PDO List area, presented in Figure 115. Below are some explanations on the configuration options presented in this dialog.

- *Name*: Name of the PDO input.
- *Index*: Index of the PDO in being edited.
- *TxPDO (Input)*: If activated, the PDO will be transferred from the Master to the Slave.
- *RxPDO (Output)*: If activated, the PDO will be transferred from the Slave to the Master.
- *Mandatory*: The PDO is necessary and can't be unchecked in the *PDO Assignment* area.
- *Fixed Content*: The PDO content is fixed and can't be changed. It's not possible to add entries in the *PDO Content* panel.
- *Virtual PDO*: Reserved for future use.
- *Exclude PDOs*: It's possible to define a list of PDO that can, or can't, be selected along with the PDO being edited in the *PDO Assignment* area, or in the *Process Data* tab. If a PDO is marked in this list, it can't be selected, turning into gray in the *PDO Assignment* area when the PDO in edition is selected.
- *SyncUnit*: ID of the PDO *Sync Manager* shall assigned to.

5.8.12.3.4. EtherCAT Slave - Startup Parameters

In the *Startup Parameters* tab, parameters for the device can be defined, which will be transferred by SDOs (*Service Data Objects*) or IDN at the system's startup. The options available in this tab, as well as the access possibilities, vary according to the EtherCAT Slave used and they are present in the *Device Description File*.

5.8.12.3.5. EtherCAT Slave - I/O Mapping

This tab of the EtherCAT Slave configuration editor offers the possibility to assign the project variables to the EtherCAT inputs or outputs. This way, the EtherCAT Slave variables can be controlled by the *User Application*.

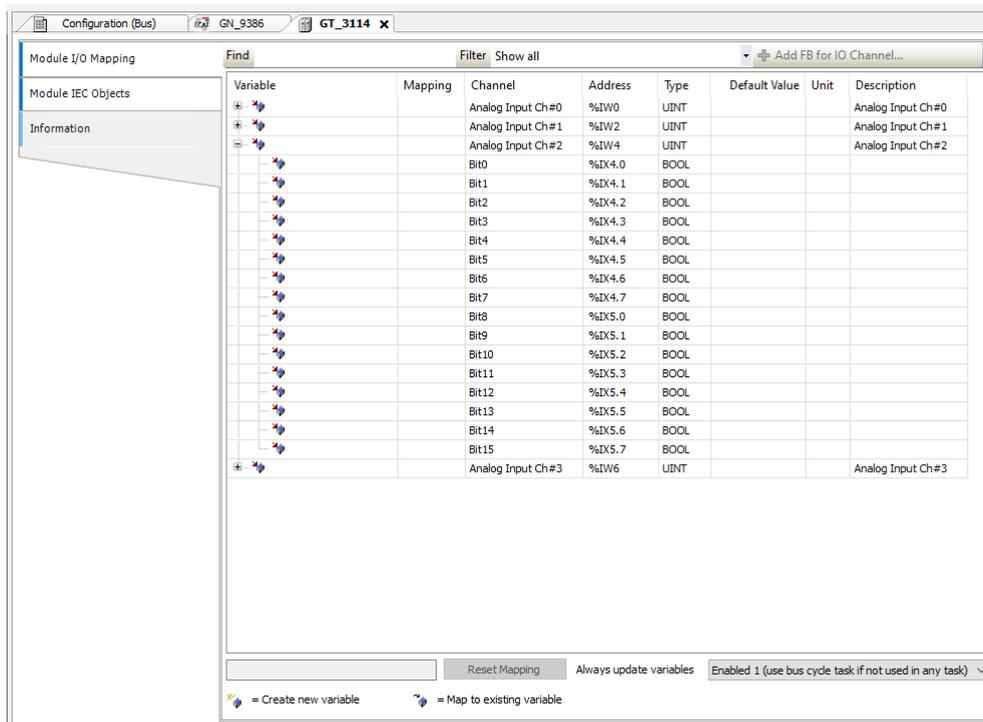


Figure 117: Slave I/O Mapping Dialog

5.8.12.3.6. EtherCAT Slave - Status and Information

The *Status* tab of the EtherCAT Slave provides status information (e.g. 'Running', 'Stopped') and device-specific diagnostic messages, also on the used card and the internal bus system.

The *Information* tab, presented in the EtherCAT Slave configuration editor, shows, if available, the following general information about the module: *Name, Vendor, Type, Version, Categories, Order Number, Description, Image.*

5.8.13. EtherNet/IP

The EtherNet/IP is a master-slave architecture protocol, consisting of an EtherNet/IP Scanner (master) and one or more EtherNet/IP Adapters (slave).

The Ethernet/IP protocol is based on CIP (*Common Industrial Protocol*), which have two primary purposes: The transport of control-oriented data associated with I/O devices and other system-related information to be controlled, such as configuration parameters and diagnostics. The first one is done through implicit messages, while the second one is done through explicit messages.

Their runtime system can act as either Scanner or Adapter. Each CPU's NET interface support only one EtherNet/IP instance and it can't be instanced on an Ethernet expansion module.

An EtherNet/IP Adapter instance supports an unlimited number of modules or Input/Output bytes. In these modules, can be added variables of types: BYTE, BOOL, WORD, DWORD, LWORD, USINT, UINT, UDINT, ULINT, SINT, INT, DINT, LINT, REAL and LREAL.

ATTENTION

EtherNet/IP can't be used together with Ethernet Redundant Mode or with Half-Cluster's redundancy.

ATTENTION

To avoid communication issues, EtherNet/IP Scanner can only have Adapters configured within the same subnetwork.

5.8.13.1. Ethernet Adapter

To add an EtherNet/IP Scanner or Adapter it's needed to add an *Ethernet Adapter* under the desired NET. This can be done through the command *Add Device*. Under this *Ethernet Adapter* it's possible to add a *Scanner* or an *Adapter*.

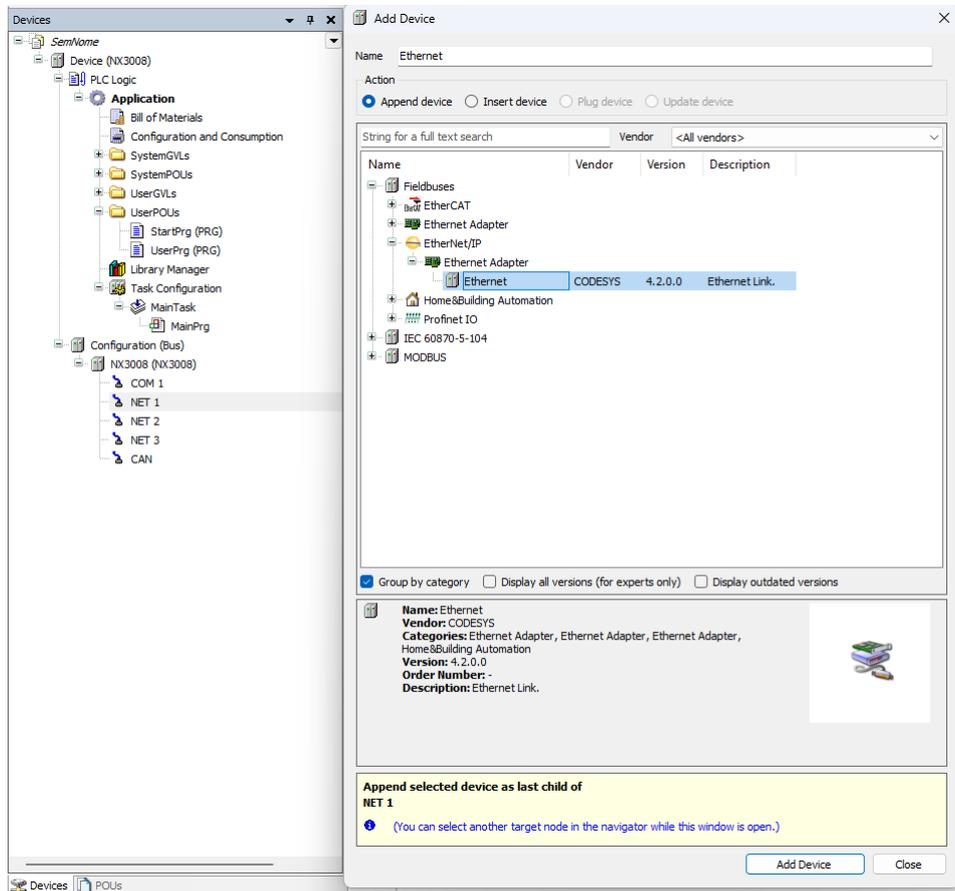


Figure 118: Adding an Ethernet Adapter

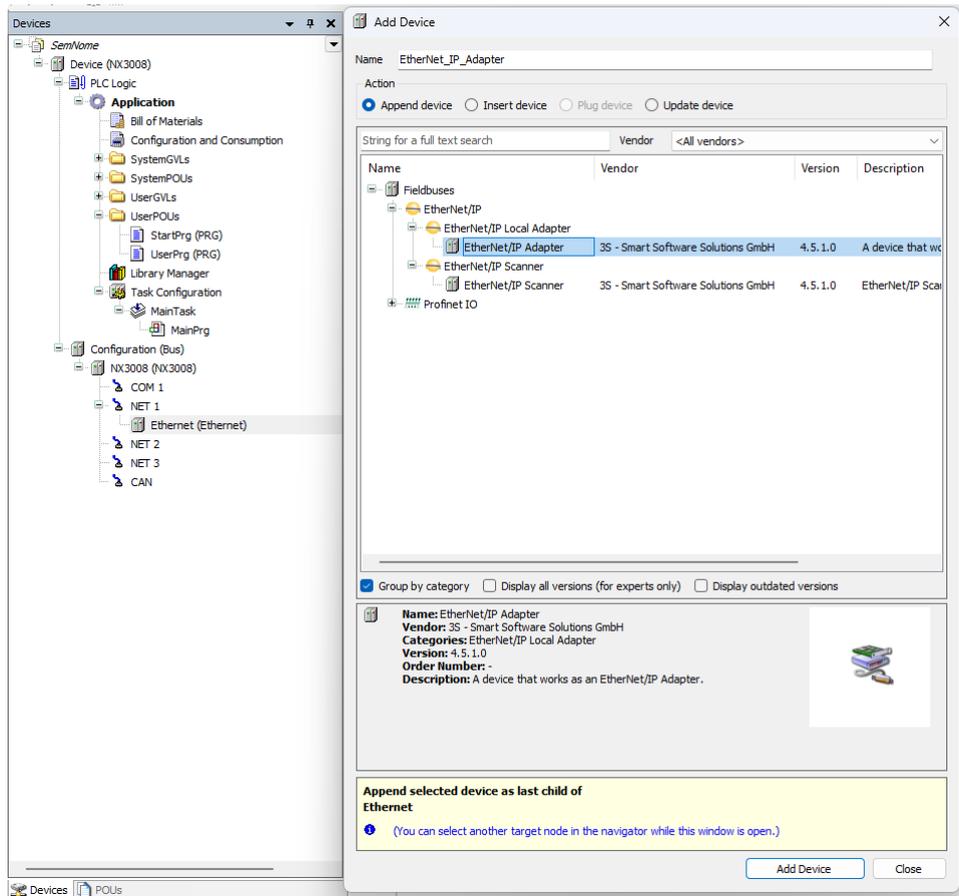


Figure 119: Adding an EtherNet/IP Adapter or Scanner

5.8.13.2. EtherNet/IP Scanner Configuration

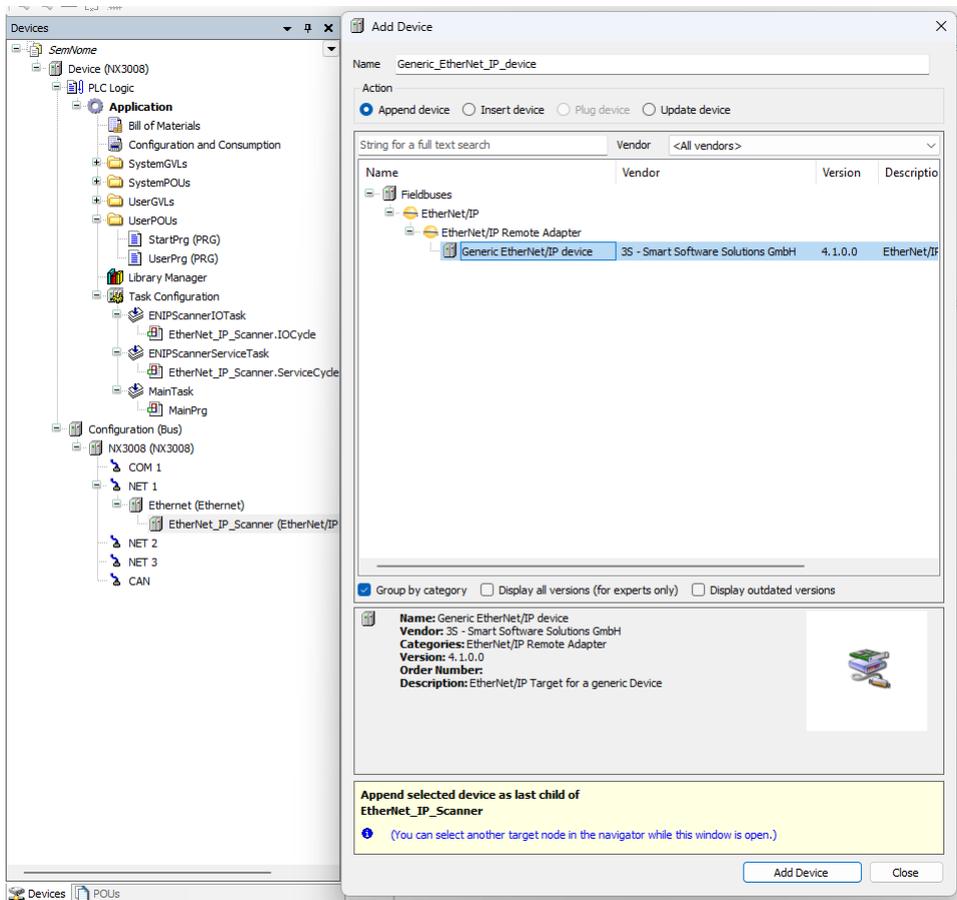


Figure 120: Adding an EtherNet/IP Adapter Under the Scanner

5.8.13.2.1. Geral

After open the Adapter declared under the Scanner it's possible to configure it as needed. The first Tab is *General*, on it is possible to configure the *IP address* and the *Electronic Keying* parameters. These parameters must be checked or unchecked if the adapter being used is installed on MasterTool. Otherwise, if the Adapter used is of type Generic. The Vendor ID, Device Type, Product Code, Large Revision, and Small Revision fields must be filled in with the correct vendor's information and the boxes checked as much as necessary. Altus, for its part, has its own ID, which is "1454".

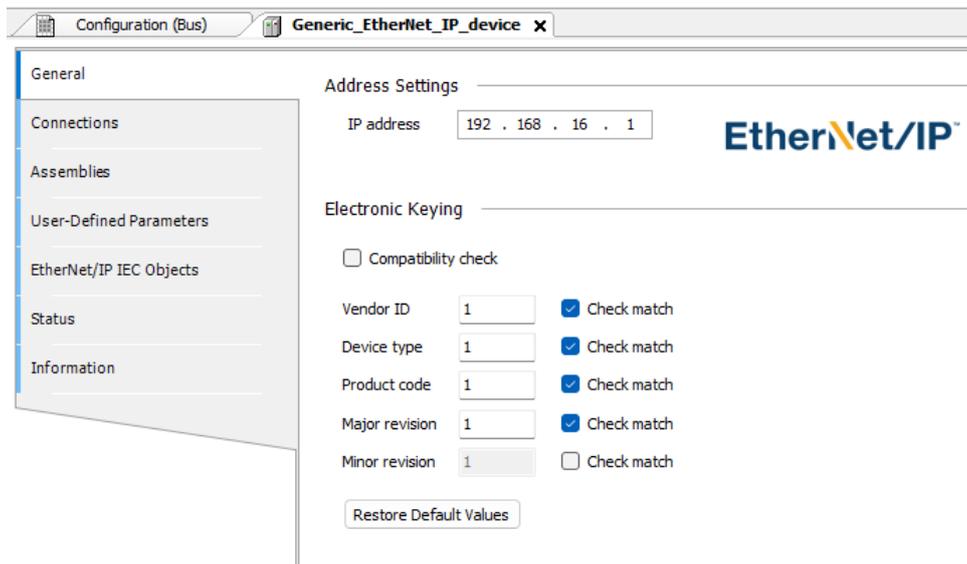


Figure 121: EtherNet/IP General Tab

5.8.13.2.2. Connections

The upper area of the *Connections* tab displays a list of all configured connections. When there is an *Exclusive Owner* connection in the EDS file, it is inserted automatically when the Adapter is added. The configuration data for these connections can be changed in the lower part of the view.

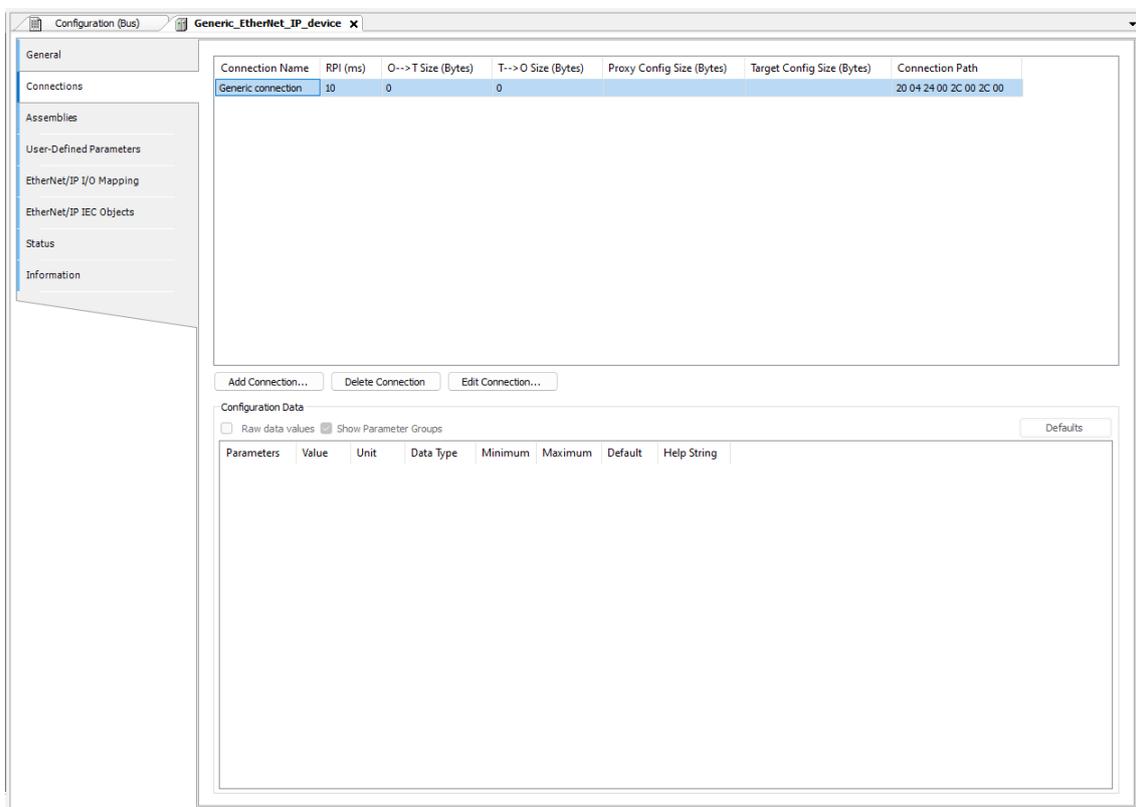


Figure 122: EtherNet/IP Connection Tab

Notes:

For two or more EtherNet/IP Scanners to connect to the same Remote Adapter:

1. Only one of the Scanners can establish an *Exclusive Owner* connection.
2. The same value of *RPI(ms)* must be configured for the Scanners.

The configuration data is defined in the EDS file. The data is transmitted to the remote adapter when the connection is opened.

Configuration	Description	Default Value	Options
RPI (ms)	Request Packet Interval: exchange interval of the input and output data.	10 ms	Multiple the Interval of the Bus Cycle Task to which it is associated
O -> T Size (Bytes)	Size of the producer data from the Scanner to the Adapter (O -> T)	0	0 - 65527
T -> O Size (Bytes)	Size of the consumer data from the Adapter to the Scanner (T -> O)	0	0 - 65531
Proxy Config Size (Bytes)	Proxy configuration data size	-	-
Device Config Size (Bytes)	Device configuration data size.	-	-
Connection Path	Address of the configuration objects - input objects - output objects.	Automatically generated path	Automatically generated path, User-defined path and Path defined by symbolic name

Table 134: EtherNet/IP Connection parameters

To *add* new connections there is the button *Add Connection...* which will open the *New connection* window. In this window, you can configure a new connection type from those predefined in the Adapter's EDS or a connection from zero when using a Generic device.

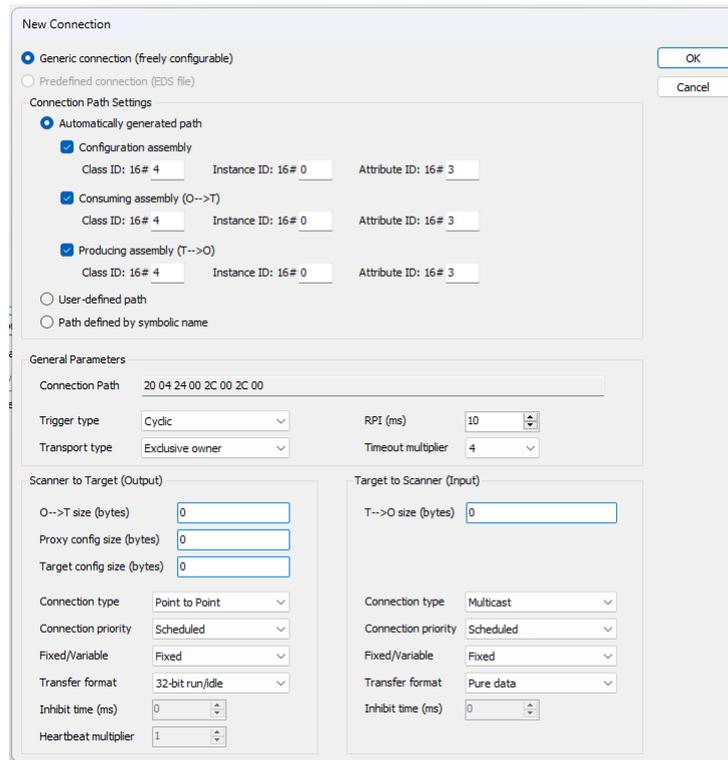


Figure 123: EtherNet/IP New Connection's Window

5.8.13.2.3. Assemblies

The upper area of the *Assemblies* tab displays a list of all configured connections. When a connection is selected, the associated inputs and outputs are displayed in the lower area of the tab.

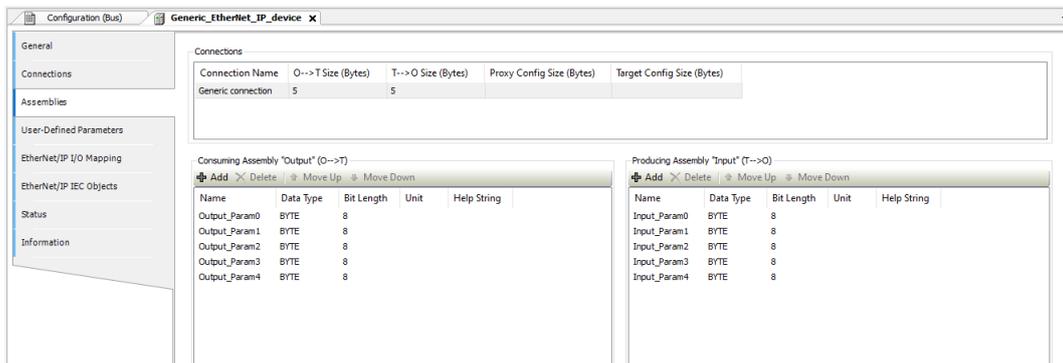


Figure 124: EtherNet/IP Assemblies

Output Assembly and Input Assembly:

Configuration	Description
Add	Opens the dialog box “Add Input/Output”
Delete	Deletes all selected Input-s/Outputs.
Move Up	Moves the selected Input/Output within the list.
Move Down	The order in the list determines the order in the I/O mapping.

Table 135: EtherNet/IP Assemblies tab

Dialog box *Add Input/Output*:

Configuration	Description
Name	Name of the input/output to be inserted.
Help String	
Data type	Type of the input/output to be inserted. This type also define its Bit Length.
Bit Length	This value must not be edited.

Table 136: EtherNet/IP “Add Input/Output” window

5.8.13.2.4. *User-Defined Parameters*

The *User-Defined Parameters* tab displays all additional parameters that are transmitted once only into the bus system during the phase of the starting procedure allotted to this. The parameters are transmitted to the remote adapter via acyclic services.

ATTENTION

The user parameters are also transmitted again when a connection is reestablished, for example after the failure of a remote adapter.

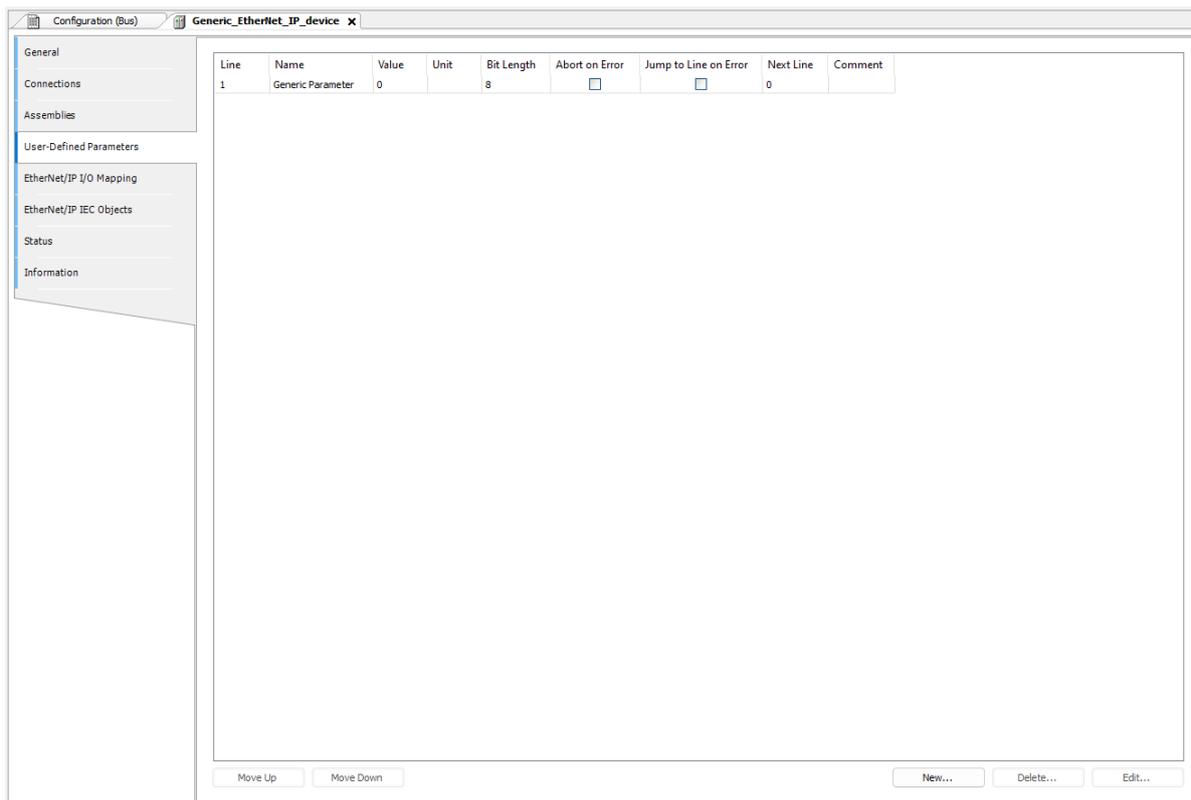


Figure 125: User-Defined Parameters Tab - EtherNet/IP

Configuration	Description
New	Opens the Select Parameters dialog for adding a new parameter.
Edit	Opens the Select Parameters dialog for changing an existing parameter.
Move up	Changes the order of the user parameters.
Move down	The order of the parameters in the list corresponds to the order at the initialization.
Value	The value of the respective parameter can be changed directly by double-clicking the value.
Abort If Error	In case of error, the entire transmission of the parameters is aborted.

Configuration	Description
Jump to Line If Error	In case of error, the program resumes with the line specified in the Next Line column. In this way, an entire block can be skipped during the initialization, or a return can be defined.

Table 137: User-Defined Parameters tab - EtherNet/IP

Note:

Jump to Line If Error: A return can lead to an infinite loop if it is never possible to write a certain parameter.

5.8.13.2.5. EtherNet/IP I/O Mapping

I/O Mapping tab shows, in the *Variable* column, the name of the automatically generated instance of the *Adapter* under *IEC Objects*. In this way, the instance can be accessed by the application. Here the project variables are mapped to adapter’s inputs and outputs.

5.8.13.3. EtherNet/IP Adapter Configuration

The EtherNet/IP Adapter requires Ethernet/IP Modules. The Modules will provide I/O mappings that can be manipulated by user application through %I or %Q addresses according to its configuration.

New Adapters can be installed on MasterTool with the EDS Files. The configuration options may differ depending on the device description file of the added Adapter.

5.8.13.3.1. General

The first tab of the EtherNet/IP Adapter is the *General* tab. Here you can set the parameters of the *Electronic Keying* used in the scanner to check compatibility. In this tab, you can also install the EDS of the device directly in the MasterTool device repository or export it.

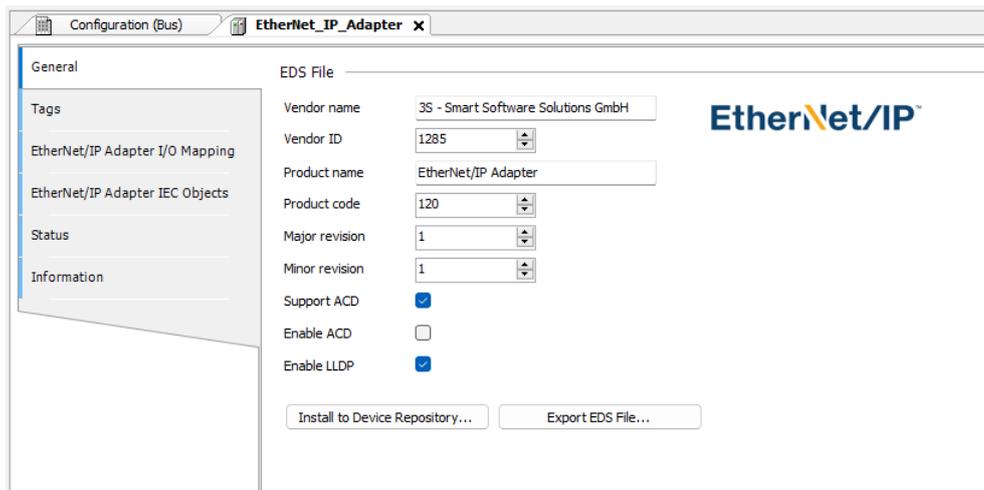


Figure 126: EtherNet/IP General Tab

5.8.13.3.2. EtherNet/IP Adapter: I/O Mapping

On the *EtherNet/IP I/O Mapping* tab, you can configure which bus cycle task the Adapter will execute.

5.8.13.4. EtherNet/IP Module Configuration

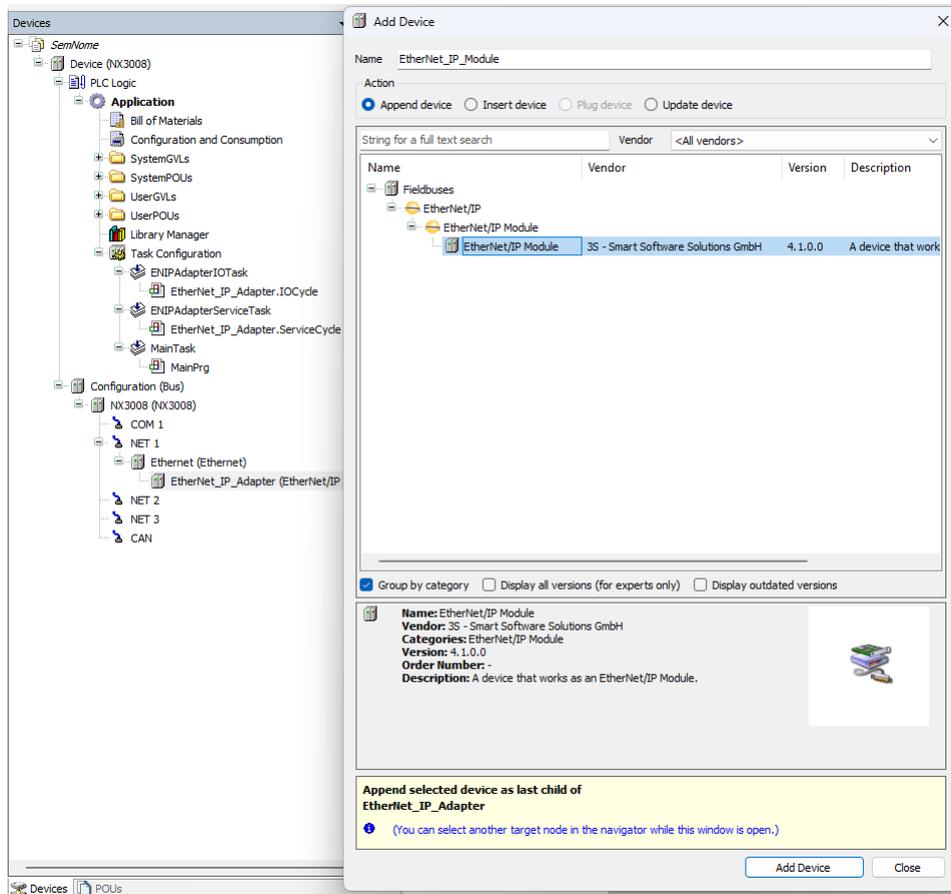


Figure 127: Adding an EtherNet/IP Module under the Adapter

5.8.13.4.1. Assemblies

The parameters of the module's *General* tab follow the same rules as described in the 135 and 136 tables.

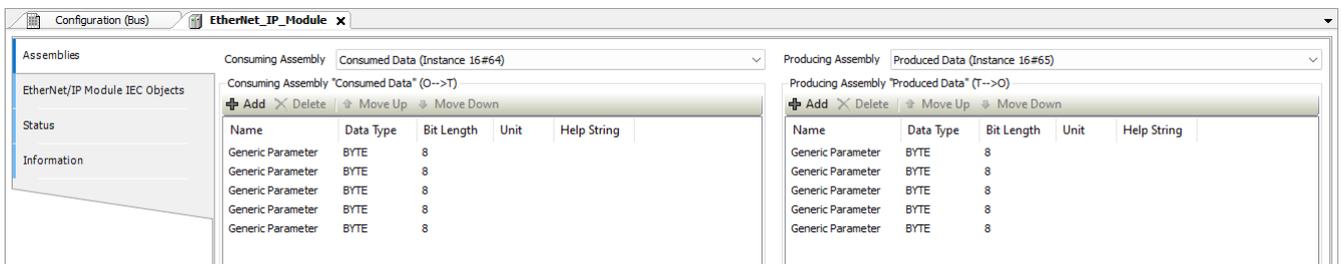


Figure 128: EtherNet/IP Module Assemblies tab

5.8.13.4.2. EtherNet/IP Module: I/O Mapping

The I/O Mapping tab shows, in the *Variable* column, the name of the automatically generated Adapter instances. In this way, the instance can be accessed by the user application.

5.8.14. IEC 60870-5-104 Server

As select this option at MasterTool, the CPU starts to be an IEC 60870-5-104 communication server, allowing connection with up to three client devices. To each client the driver owns one exclusive event queue with the following features:

- Size: 1000 events
- Retentivity: non retentive
- Overflow policy: keep the newest

To configure this protocol, it is needed to do the following steps:

- Add a protocol IEC 60870-5-104 Server instance to one of the available Ethernet channel. To realize this procedure consult the section [Inserting a Protocol Instance](#)
- Configure the Ethernet interface. To realize this procedure consult the section [Ethernet Interfaces Configuration](#)
- Configure the general parameters of protocol IEC 60870-5-104 Server with connection mode Port or IP, and the TCP port number when the selected connection mode is IP
- Add and configure devices, defining the proper parameters
- Add and configure the IEC 60870-5-104 mappings, specifying the variable name, type of object, object address, size, range, dead band and type of dead band
- Configure the link layer parameters, specifying the addresses, communication time-outs and communication parameters
- Configure the application layer parameters, synchronism configuration, commands, as well as transmission mode of *Integrated Totals* objects

The descriptions of each configuration are related below, in this section.

5.8.14.1. Type of data

The table below shows the supported variable type by the Nexto Series CPU for each protocol IEC 60870-5-104 data type.

Object Type	IEC Variables Type
Single Point Information (M_SP_NA)	BOOL
	BIT
Double Point Information (M_DP_NA)	DBP
Step Position Information (M_ST_NA)	USINT
Measured Value, normalized value (M_ME_NA)	INT
Measured Value, scaled value (M_ME_NB)	INT
Measured Value, short floating point value (M_ME_NC)	INT
	UINT
	DINT
	UDINT
	REAL
Integrated Totals (M_IT_NA)	INT
	DINT
Bitstring Information (M_BO_NA)	DWORD
Single Command (C_SC_NA)	BOOL
	BIT
Double Command (C_DC_NA)	DBP
Regulating Step Command (C_RC_NA)	DBP
Setting Point Command, normalized Value (C_SE_NA)	INT
Setting Point Command, scaled Value (C_SE_NB)	INT

Object Type	IEC Variables Type
Setting Point Command, short floating point Value (C_SE_NC)	REAL
Bitstring Command (C_BO_NA)	DWORD

Table 138: Variables Declaration to IEC 60870-5-104

Notes:

Regulating Step Command: The *Lower* and *Higher* object states of the C_RC_NA are associated respectively to *OFF* and *ON* internal DBP type states.

Step Position Information: According to item 7.3.1.5 of Standard IEC 60870-5-101, this 8 bit variable is composed by two fields: value (defined by the 7 bits less significant) and transient (defined as the most significant bit, which indicates when the measured device is transitioning).

Below, there is a code example for fields manipulation in an USINT type variable. Attention, because this code doesn't consist if the value is inside the range, therefore this consistency remains at user's charge.

```
PROGRAM UserPrg
VAR
usiVTI: USINT; // Value with transient state indication, mapped for the Client
siValue: SINT; // Value to be converted to VTI. Must be between -64 and +63
bTransient: BOOL; // Transient to be converted to VTI
END_VAR

usiVTI := SINT_TO_USINT(siValue) AND 16#3F;
IF siValue < 0 THEN
usiVTI := usiVTI OR 16#40;
END_IF
IF bTransient THEN
usiVTI := usiVTI OR 16#80;
END_IF
```

PROFIBUS: Except by the digital objects, the protocol IEC 60870-5-104's analog and counters objects data types are different from PROFIBUS analogs and counters modules data types, not being possible to map such PROFIBUS variable types directly to IEC 60870-5-104 clients.

In these cases it is needed to create an intermediary variable, to be mapped in the IEC 60870-5-104 client, and properly convert the types, as can be observed on the example's code below.

```
PROGRAM UserPrg
VAR
iAnalogIn: INT;
iAnalogOut: INT;
diCounter: DINT;
END_VAR

// Analog input conversion from WORD (PROFIBUS) to INT (IEC104)
iAnalogIn:= WORD_TO_INT(wNX6000in00);

// Analog output conversion from INT(IEC104) to WORD (PROFIBUS)
wNX6100out00:= INT_TO_WORD(iAnalogOut);

// Counter conversion from WORDs high+low (PROFIBUS) to DINT (IEC104)
diCounter:= DWORD_TO_DINT(ROL(WORD_TO_DWORD(wNX1005cnt00H), 16) OR wNX1005cnt00L
);
```

5.8.14.2. Double Points

The double digital points are used to indicate equipment position, such as valves, circuit breakers and sectioners, where the transition between open and close states demand a determined time. Can thus indicate an intermediary transition state between both final states.

Double digital points are also used as outputs and, in an analogous way, it is necessary to keep one of the outputs enabled for a certain time to complete the transition. Such actuation is done through pulses, also known by trip/close commands, with determined duration (enough to the switching of the device under control).

Consult the Double Points section of Utilization Manual for information about double digital points through DBP data type.

Once the Nexto Series digital input and output modules don't support DBP points mapping, some application trickery are needed to make it possible. Remembering that is also not possible to use the *PulsedCommand* function, defined at the *LibRtuStandard* library, to operate the Nexto Series digital double points.

5.8.14.2.1. Digital Input Double Points

For the digital input modules it is needed two auxiliary variables' declaration, to be mapped on the digital input module, besides the double point that is wished to map on the server:

- The double point value variable: type DBP
- The simple point OFF/TRIP value variable: type BOOL
- The simple point ON/CLOSE value variable: type BOOL

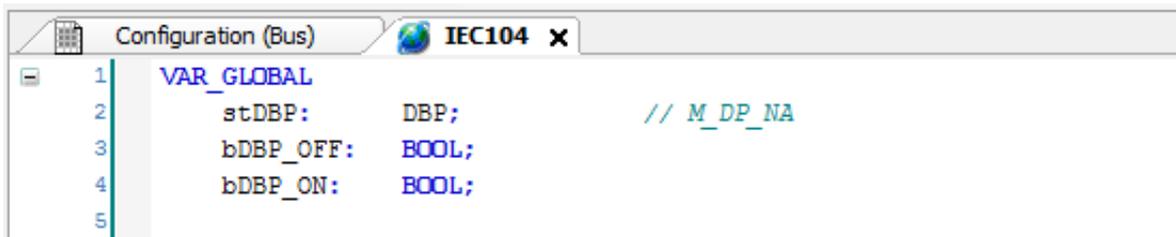


Figure 129: Double Point Variables Declaration Example

Done the variables declaration, it is necessary to create a link between the value variables and the digital input module quality, through the CPU's *Internal Points* tab:

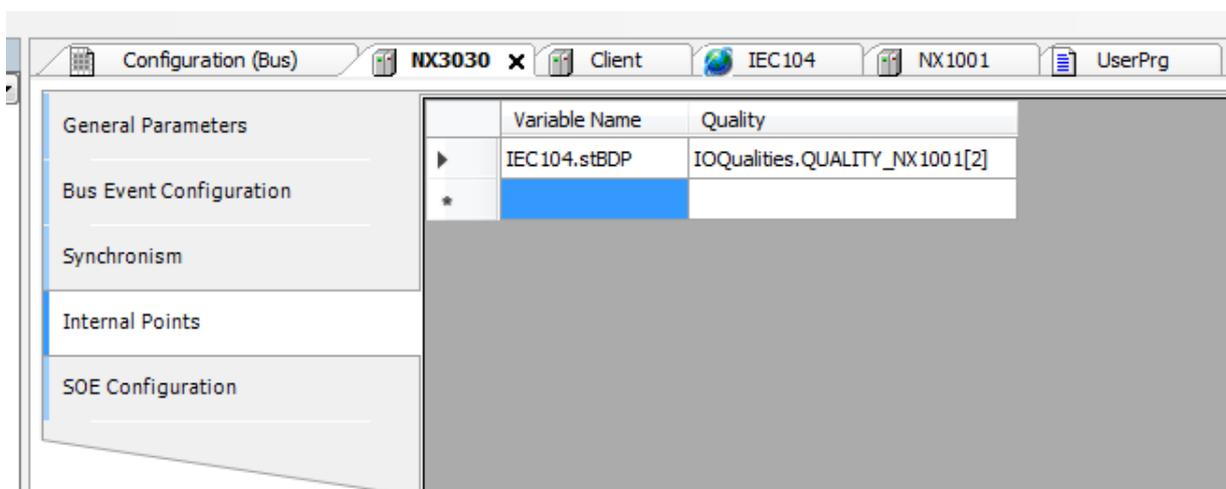


Figure 130: Double Point Variables Attribution to Internal Points

The double point value variable must be mapped at the server IEC 60870-5-104 driver, and both simple variables at the Nexto Series digital input module (in that example, a NX1001). Typically the OFF (TRIP) state is mapped to the even input and the ON (CLOSE) state to the odd input.

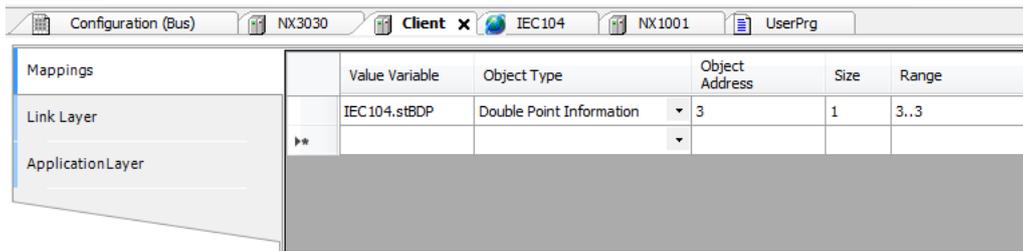


Figure 131: Double Point Variables Mapping on the Client IEC 60870-5-104

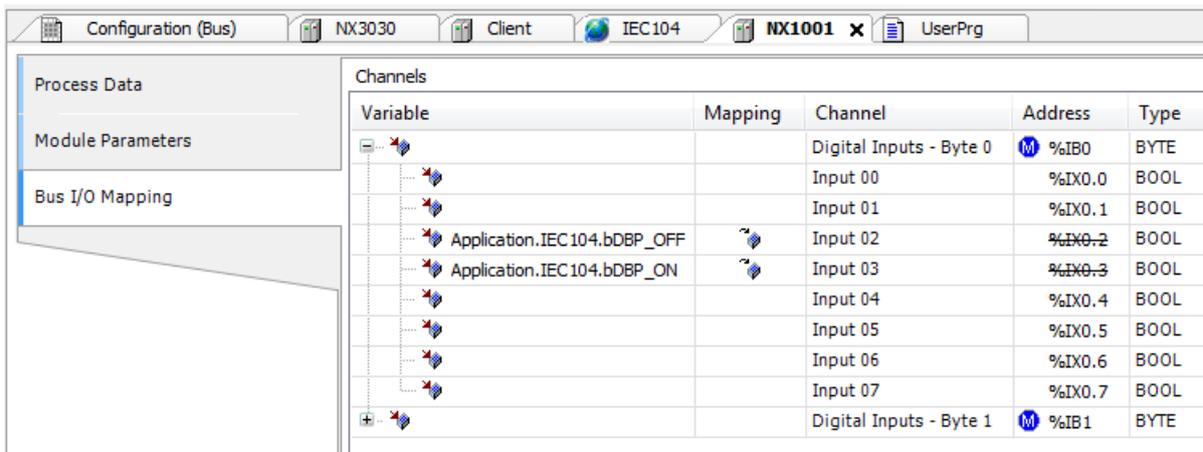


Figure 132: Variables Mapping at the Module Inputs

At last, the user must insert two code lines in its application, to be cyclically executed, to simple variables value attribution to double point:

- DBP value variable, index ON, receive simple point ON value
- DBP value variable, index OFF, receive simple point OFF value

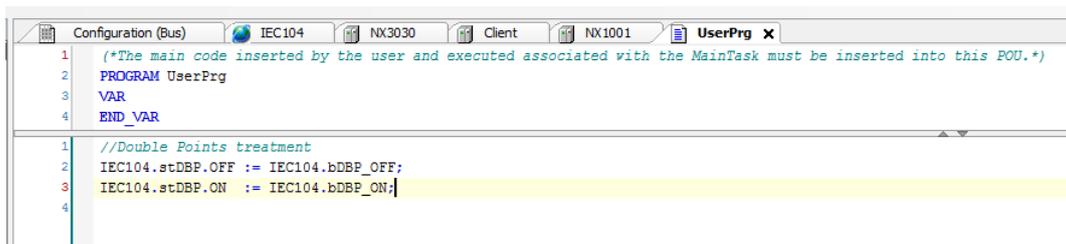


Figure 133: Variables' Values Attribution to the Double Point

5.8.14.2.2. Digital Output Double Points

For the digital output modules it must be used the *CommandReceiver* function block to intercept double points actuation commands originated from the clients IEC 60870-5-104. Consult the section [Interception of Commands Coming from the Control Center](#) for further information.

The example code below, POU *CmdRcv*, treats pulsed commands received from clients for a digital double point, mapped in a NX2020 module. Besides the following ST code it is need to map a DBP point in Nexto's IEC 60870-5-104 server.

Value Variable	Object Type	Object Address	Size	Range	Counter Variable	Dead Band Variable	Dead Band Type	Select Required	Short Pulse (ms)	Long Pulse (ms)
CmdRcv.dbpIEC104	Double Command	1	1	1..1			Disabled	False	1000	2000

Figure 134: Mapping of Digital Output Double Point variables on IEC 60870-5-104 Client

```

PROGRAM CmdRcv
VAR
CmdReceive:  CommandReceiver; // Interceptor Instance
fbPulsedCmd: PulsedCommandNexto; // Pulsed Command Instance
byResult:    BYTE; // Pulsed command result
dbpIEC104:   DBP; // Variable mapped in the IEC 104
bSetup:     BOOL:= TRUE; // Interceptor initial setup
END_VAR

// Executes the function configuration in the first cycle
IF bSetup THEN
CmdReceive.dwVariableAddr:= ADR(dbpIEC104);
CmdReceive.bExec:= TRUE;
CmdReceive.eCommandResult:= COMMAND_RESULT.NONE;
CmdReceive.dwTimeout:= 256 * 10;
bSetup:= FALSE;
END_IF

// In case a command is captured:
IF CmdReceive.bCommandAvailable THEN

// Treats each one of the possible commands
CASE CmdReceive.sCommand.eCommand OF

COMMAND_TYPE.NO_COMMAND:

    // Inform that there is an invalid command.
    // Does nothing and must move on by time-out.

COMMAND_TYPE.SELECT:

    // Treats only commands for double points
    IF CmdReceive.sCommand.sSelectParameters.sValue.eParamType =
        DOUBLE_POINT_COMMAND THEN
        // Returns command finished with success
        // (controlled by IEC104 protocol)
        byResult:= 7;
    ELSE
        // Returns command not supported
        byResult:= 1;
    END_IF

COMMAND_TYPE.OPERATE:

    // Treats only commands for double points

```

```

IF CmdReceive.sCommand.sOperateParameters.sValue.eParamType =
DOUBLE_POINT_COMMAND THEN
// Pulse generation in outputs
IF CmdReceive.sCommand.sOperateParameters.sValue.sDoublePoint.bValue THEN
// Executes TRIP function
fbPulsedCmd(
byCmdType:= 101,
byPulseTime:= DWORD_TO_BYTE(CmdReceive.sCommand.sOperateParameters.
sValue.sDoublePoint.sPulseConfig.dwOnDuration/10),
ptDbpVarAdr:= ADR(dbpIEC104),
stQuality:= IOQualities.QUALITY_NX2020[4],
byStatus=> byResult);
ELSE
// Executes CLOSE function
fbPulsedCmd(
byCmdType:= 102,
byPulseTime:= DWORD_TO_BYTE(CmdReceive.sCommand.sOperateParameters.
sValue.sDoublePoint.sPulseConfig.dwOffDuration/10),
ptDbpVarAdr:= ADR(dbpIEC104),
stQuality:= IOQualities.QUALITY_NX2020[5],
byStatus=> byResult);
END_IF
ELSE
// Returns command not supported
byResult:= 1;
END_IF

COMMAND_TYPE.CANCEL:

// Returns command finished with success
// (controlled by IEC104 protocol)
byResult:= 7;

END_CASE

// Treats the pulsed command function result
// and generates the answer to the intercepted command
CASE byResult OF
1: // Invalid type of command
CmdReceive.eCommandResult:= COMMAND_RESULT.NOT_SUPPORTED;
CmdReceive.bDone:= TRUE;
2: // Invalid input parameters
CmdReceive.eCommandResult:= COMMAND_RESULT.INCONSISTENT_PARAMETERS;
CmdReceive.bDone:= TRUE;
3: // Parameter change in running
CmdReceive.eCommandResult:= COMMAND_RESULT.PARAMETER_CHANGE_IN_EXECUTION;
CmdReceive.bDone:= TRUE;
4: // Module did not answered the command(absent)
CmdReceive.eCommandResult:= COMMAND_RESULT.HARDWARE_ERROR;
CmdReceive.bDone:= TRUE;
5: // Command started and in running (does not returns nothing)
6: // Another command has been sent to this point and it is running
CmdReceive.eCommandResult:= COMMAND_RESULT.LOCKED_BY_OTHER_CLIENT;
CmdReceive.bDone:= TRUE;
7: // Command finished with success
CmdReceive.eCommandResult:= COMMAND_RESULT.SUCCESS;

```

```

    CmdReceive.bDone:= TRUE;
END_CASE

END_IF

CmdReceive();

IF CmdReceive.bDone THEN
CmdReceive.bDone:= FALSE;
END_IF

```

As can be observed in the previous code, to help in the pulse generation in Nexto's digital double outputs, it was created and used a function block equivalent to *PulsedCommand* function of library *LibRtuStandard*. The *PulsedCommandNexto()* function block shows up coded in ST language.

```

FUNCTION_BLOCK PulsedCommandNexto
VAR_INPUT
byCmdType:    BYTE;    // command type:
                // 100 = status
                // 101 = close/on
                // 102 = trip/off
byPulseTime:  BYTE;    // Pulse duration (in hundredths of second)
ptDbpVarAdr:  POINTER TO DBP; // DBP variable address (can be mapped)
stQuality:    QUALITY;  // DBP point quality(digital module)
END_VAR
VAR_OUTPUT
bON:          BOOL;    // Odd output mapped on Nexto DO module
bOFF:         BOOL;    // Even output mapped on Nexto DO module
byStatus:     BYTE:= 7; // Function return:
                // 1 = invalid command
                // 2 = Time out of valid range (2..255)
                // 3 = command changed in running time
                // 4 = module did not answer to the command (absent)
                // 5 = command started or running
                // 6 = There is already an active command on this point
                // 7 = pulse command finished with success
END_VAR
VAR
byState:      BYTE;    // Function block state
udiPulseEnd:  UDINT;  // Pulse end instant
END_VAR

// PulsedCommandNexto state machine
CASE byState OF

0: // Init state, ready to receive commands:
CASE byCmdType OF

100:// Just returns the last status

101: // Execute pulse ON:
    // Valids the pulse duration
    IF byPulseTime > 1 THEN
        // Check if there is already an active command on this point

```

```

IF ptDbpVarAdr^.ON OR ptDbpVarAdr^.OFF THEN
  // Returns that there is already an active command
  byStatus:= 6;
ELSE
  // Enables CLOSE output
  ptDbpVarAdr^.ON:= TRUE;
  ptDbpVarAdr^.OFF:= FALSE;
  // Next state: execute pulse ON
  byState:= byCmdType;
  // Returns started command
  byStatus:= 5;
END_IF
ELSE
  // Returns the out of range pulse
  byStatus:= 2;
END_IF

102: // Execute pulse OFF
// Validates the pulse duration
IF byPulseTime > 1 THEN
  // Check if there is already an active command on this point
  IF ptDbpVarAdr^.ON OR ptDbpVarAdr^.OFF THEN
    // Returns that there is already an active
    byStatus:= 6;
  ELSE
    // Enables TRIP output
    ptDbpVarAdr^.ON:= FALSE;
    ptDbpVarAdr^.OFF:= TRUE;
    // Next step: execute pulse OFF
    byState:= byCmdType;
    // Returns started command
    byStatus:= 5;
  END_IF
ELSE
  // Returns the out of range pulse
  byStatus:= 2;
END_IF
ELSE
  // Returns invalid command
  byStatus:= 1;
END_CASE

// Memorizes the instant of the pulse end
udiPulseEnd:= SysTimeGetMs() + BYTE_TO_UDINT(byPulseTime) * 10;

101, 102:// Continues the pulse execution ON/OFF
// It returns that the command is running
byStatus:= 5;
// Checks the running parameter change
IF byCmdType <> 100 AND byCmdType <> byState THEN
  // Returns the running parameter change
  byStatus:= 3;
END_IF
// Checks pulse end
IF SysTimeGetMs() >= udiPulseEnd THEN
  // Disable TRIP and CLOSE outputs

```

```
ptDbpVarAdr^.ON:= FALSE;
ptDbpVarAdr^.OFF:= FALSE;
// Returns finished command, only if the command has not changed
IF byCmdType = 100 OR byCmdType = byState THEN
    byStatus:= 7;
END_IF
// Next state: initial
byState:= 0;
END_IF

END_CASE

// Checks digital module (DBP point) quality
IF stQuality.VALIDITY <> QUALITY_VALIDITY.VALIDITY_GOOD THEN
// Disable TRIP and CLOSE outputs
ptDbpVarAdr^.ON:= FALSE;
ptDbpVarAdr^.OFF:= FALSE;
// Returns absent module
byStatus:= 4;
// Next state: initial
byState:= 0;
END_IF

// Copy DBP output states to the simple outputs
bON:= ptDbpVarAdr^.ON;
bOFF:= ptDbpVarAdr^.OFF;
```

5.8.14.3. General Parameters

To the *General Parameters* configuration of an IEC 60870-5-104 Server according to figure below follow the table below parameters:

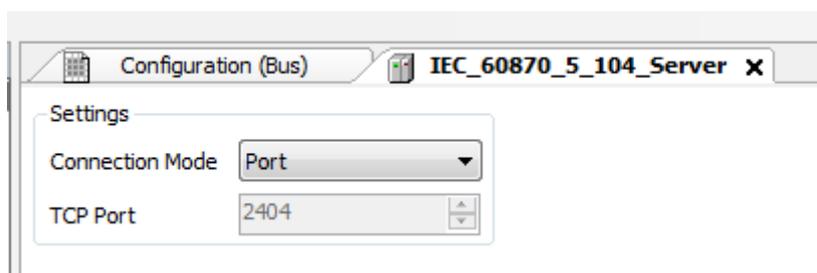


Figure 135: Server IEC 60870-5-104 General Parameters Screen

Parameter	Description	Factory Default	Possibilities
Connection Mode	Set the connection mode with the Connected Client modules.	Port	Port IP
TCP Port	Defines which PLC's TCP port number will be used to communicate with the Connected Client modules. In case the "Connection Mode" field is set as "IP".	2404	1 to 65535

Table 139: IEC 60870-5-104 Server General Parameters Configuration

5.8.14.4. Data Mapping

To configure the IEC 60870-5-104 Server data relation, viewed on figure below follow the parameters described on table below:

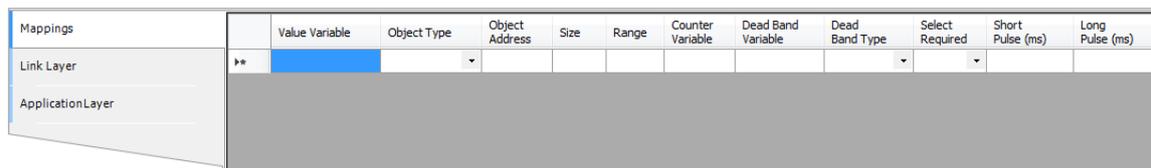


Figure 136: IEC 60870-5-104 Server Mappings Screen

Parameter	Description	Factory Default	Possibilities
Value Variable	Symbolic variable name	-	Name of a variable declared in a POU or GVL

Parameter	Description	Factory Default	Possibilities
Object Type	IEC 60870-5-104 object type configuration	-	Single Point Information Double Point Information Step Position Information Measured Value (Normalized) Measured Value (Scaled) Measured Value (Short Floating Point) Integrated Totals Bitstring Information (32 Bits) Single Command Double Command Regulating Step Command Setting Point Command (Normalized) Setting Point Command (Scaled) Setting Point Command (Short Floating Point) Bitstring Command (32 Bits)
Object Address	IEC 60870-5-104 mapping first point's index	-	1 to 65535
Size	Specifies the maximum data quantity that an IEC 60870-5-104 mapping will can access	-	1 to 86400000
Range	Configured data address range	-	-
Counter Variable	Name of the symbolic variable which will hold the counter variable's value	-	Name of a variable declared in a POU, GVL or counter module
Dead Band Variable	Name of the symbolic variable which will hold the dead band's value	-	Name of a variable declared in a POU or GVL
Dead Band Type	Defines the dead band type to be used in the mapping	Disabled	Absolute Disabled Integrated
Select Required	Defines if it is required a previous select to run a command	False	True False
Short Pulse (ms)	Defines the short pulse time to an IEC 60870-5-104 digital command	1000	1 to 86400000
Long Pulse (ms)	Defines the long pulse time to an IEC 60870-5-104 digital command	2000	1 to 86400000

Table 140: IEC 60870-5-104 Server Mappings Configuration

Notes:

Value Variable: When a read command is sent, the return received in the answer is stored in this variable. When it is a write command, the written value is going to be stored in that variable. The variable can be simple, array, array element or can be at structures.

Counter Variable: This field applies only on mapping of *Integrated Totals* type objects, being this the controller variable to be managed on process. It must has same type and size of the variable declared on *Value Variable* column, which value is going to be read, or reported to, the client in case of events.

ATTENTION

When the *Counter Variable* has a quality variable associated, to the quality to be transferred to the frozen variable at freeze command, it must be associated a quality variable to the frozen one. This procedure must be done through *Internal Points* tab.

Dead Band Variable: This field applies only to input analog variables (*Measured Value* type objects) mappings. It must has same type and size of the variable declared on *Value Variable* column. New dead band variable values are going to be considered only when the input analog variable change its value.

Dead Band Type: The configuration types available to dead band are:

Function type	Configuration	Description
Dead Band Type	Disabled	In this option, any value change in a group's point, as smaller it is, generates an event to this point.
	Absolute	In this option, if the group's point value absolute change is bigger than the value in "Dead Band" field, an event is going to be generated to this point.
	Integrated	In this option, if the absolute of the integration of the group's point value change is bigger than the value in "Dead Band" field, an event is going to be generated to this point. The integration interval is one second.

Table 141: IEC 60870-5-104 Server Mappings Dead Band Types

Short Pulse and Long Pulse: At the define of short and long pulses duration time it must be considered the limits supported by the device which will treat the command. For example, case the destiny is an output card, which is not supported in native by Nexto Series. It must be checked at the module's Datasheet what the minimum and maximum times, as well as the resolution, to running the pulsed commands.

5.8.14.5. Link Layer

To the IEC 60870-5-104 Server link layer parameters configuration, shown on figure below, follow the described parameters on table below:

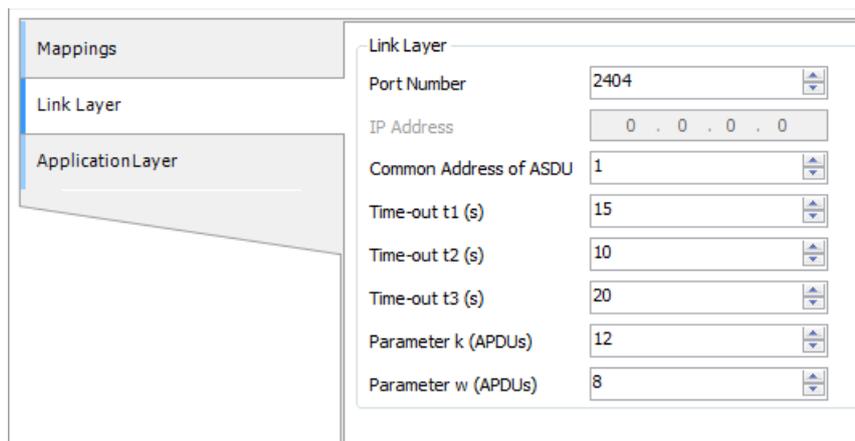


Figure 137: Server IEC 60870-5-104 Link Layer Configuration Screen

Parameter	Description	Factory Default	Possibilities
Port Number	Listened port address to client connection. Used when the client connection isn't through IP	2404	1 to 65535
IP Address	Connected client IP, used when the client connection is through IP	0.0.0.0	1.0.0.1 to 223.255.255.254
Common Address of ASDU	IEC 60870-5-104 address, if the connected client is through IP	1	1 to 65534
Time-out t1 (s)	Time period (in seconds) that the device waits the receiving of an acknowledge message after sent an APDU message type I or U (data), before close the connection	15	1 to 180
Time-out t2 (s)	Time period (in seconds) that the device waits to send a watch message (S-Frame) acknowledging the data frame receiving	10	1 to 180
Time-out t3 (s)	Time period (in seconds) in what is going to be sent a message to link test in case there is no transmission by both sides	20	1 to 180
Parameter k (APDUs)	Maximum number of data messages (I-Frame) transmitted and not acknowledged	12	1 to 12
Parameter w (APDUs)	Maximum number of data messages (I-Frame) received and not acknowledged	8	1 to 8

Table 142: IEC 60870-5-104 Server Link Layer Configuration

Note:

The fields *Time-out t1 (s)*, *Time-out t2 (s)* and *Time-out t3 (s)* are dependents between themselves and must be configured in a way that *Time-out t1 (s)* be bigger than *Time-out t2 (s)* and *Time-out t3 (s)* be bigger than *Time-out t1 (s)*. If any of these rules be not respected, error messages are going to be generated during the project compilation.

ATTENTION

For slow communication links (example: satellite communication), the parameters *Time-out t1 (s)*, *Time-out t2 (s)* and *Time-out t3 (s)* must be properly adjusted, such as doubling the default values of these fields.

5.8.14.6. Application Layer

To configure the IEC 60870-5-104 Server application layer, shown on figure below, follow the parameters described on table below:

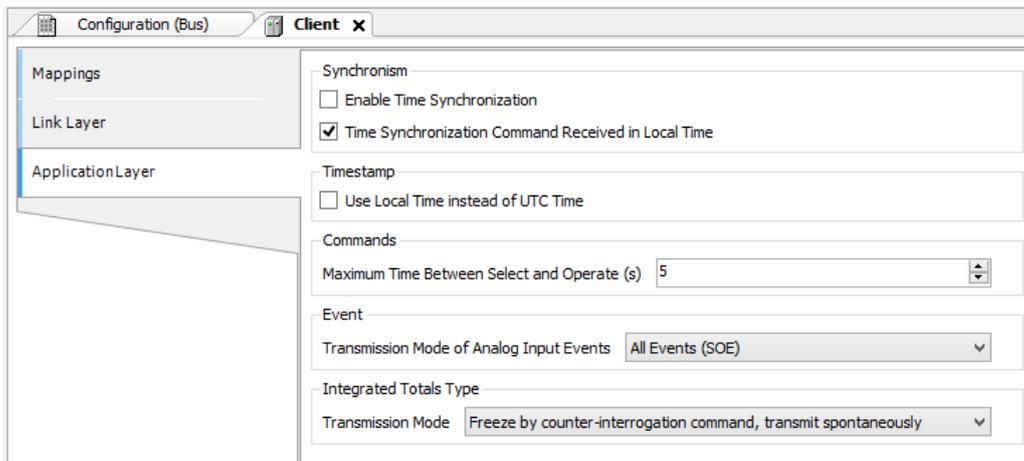


Figure 138: Server IEC 60870-5-104 Application Layer Configuration Screen

Parameter	Description	Factory Default	Possibilities
Enable Time Synchronization	Option to Enable/Disable time sync request	Disabled	Disabled Enabled
Time Synchronization Command Received in Local Time	Option to Enable/Disable the treatment of the synchronization command in local time	Enabled	Disabled Enabled
Use Local Time instead of UTC Time	Option to Enable/Disable the time stamp in local time for events	Disabled	Disabled Enabled
Maximum Time Between Select and Operate (s)	Time period in which the selection command will remain active (the count starts from the received selection command acknowledge) waiting the Operate command	5	1 to 180

Parameter	Description	Factory Default	Possibilities
Transmission Mode of Analog Input Events	Analog input events transmission mode	All Events (SOE)	All Events (SOE) Most Recent Event
Transmission Mode	Frozen counters transmission mode (Integrated Totals)	Freeze by counter-interrogation command, transmit spontaneously	Freeze by counter-interrogation command, transmit spontaneously Freeze and transmit by counter-interrogation command

Table 143: IEC 60870-5-104 Server Application Layer Configuration

Notes:

Enable Time Synchronization: Once enabled, allow the IEC 60870-5-104 Server adjust the CPU’s clock when a sync command is received.

Time Synchronization Command Received in Local Time: When enabled, the IEC 60870-5-104 Server adjusts the CPU clock by treating the time received in the synchronization command as local time. Otherwise, this time is considered UTC.

Use Local Time instead of UTC Time: Once enabled, the time stamp of the events generated by IEC 60870-5-104 Server will be sent according to the CPU’s local time.

ATTENTION

When the time sync option is checked in more than one server, the received times from different servers will be overwritten in the system clock in a short time period, being able to cause undesirable behaviors due to delays on messages propagation time and system load.

Transmission Mode of Analog Inputs Events: The Analog Inputs Events transmission modes available are the following:

Function Type	Configuration	Description
Transmission Mode of Analog Input Events	All Events (SOE)	All analog events generated are going to be sent.
	Most Recent Event	It is sent only the most recent analog event.

Table 144: IEC 60870-5-104 Server Transmission Modes of Analog Inputs Events

Transmission Mode: The available transmission modes of the frozen counters (*Integrated Totals*) are the following:

Function Type	Configuration	Description
Transmission Mode	Freeze by counter-interrogation command, transmit spontaneously	Equivalent to the counters acquisition D Mode (Integrated Totals) defined by Standard IEC 60870-5-101. In this mode, the control station's counters interrogation commands, freeze the counters. Case the frozen values have been modified, they are reported through events.
	Freeze and transmit by counter-interrogation command	Equivalent to the counters acquisition C Mode (Integrated Totals) defined by Standard IEC 60870-5-101. In this mode, the control station's counters interrogation commands, freeze the counters. The subsequent counters interrogation commands (read) are sent by the control station to receive the frozen values.

Table 145: IEC 60870-5-104 Server Transmission Modes of the Frozen Counters

ATTENTION

The Standard IEC 60870-5-104, section *Transmission control using Start/Stop*, foresee the commands *STARTDT* and *STOPDT* utilization to data traffic control between client and server, using simple or multiple connections. Despite Nexto supports such commands, its utilization isn't recommended to control data transmission, mainly with redundant CPUs, because such commands aren't synchronized between both CPUs. Instead of using multiple connections between client and Nexto server, it's suggested the use of NIC Teaming resources to supply (physically) redundant Ethernet channels and preserve the CPU resources (CPU control centers).

5.8.14.7. Server Diagnostic

The IEC 60870-5-104 Server protocol diagnostics are stored in *T_DIAG_IEC104_SERVER_1* type variables, which are described in table below:

Diagnostic variable of type T_DIAG_IEC104_SERVER_1.*	Size	Description
Command bits, automatically reset:		
tCommand.bStop	BOOL	Disable Driver
tCommand.bStart	BOOL	Enable Driver
tCommand.bDiag_01_Reserved	BOOL	Reserved
tCommand.bDiag_02_Reserved	BOOL	Reserved
tCommand.bDiag_03_Reserved	BOOL	Reserved
tCommand.bDiag_04_Reserved	BOOL	Reserved
tCommand.bDiag_05_Reserved	BOOL	Reserved
tCommand.bDiag_06_Reserved	BOOL	Reserved
Diagnostics:		
tClient_X.bRunning	BOOL	IEC 60870-5-104 Server is running

Diagnostic variable of type T_DIAG_IEC104_SERVER_1.*	Size	Description
tClient_X.eConnectionStatus. CLOSED	ENUM(BYTE)	Communication channel closed. Server won't accept connection request. ENUM value (0)
tClient_X.eConnectionStatus. LISTENING		Server is listening to the configured port and there is no connected clients. ENUM value (1)
tClient_X.eConnectionStatus. CONNECTED		Connected client. ENUM value (2)
tClient_X.tQueueDiags. bOverflow	BOOL	Client queue is overflowed
tClient_X.tQueueDiags. wSize	WORD	Configured queue size
tClient_X.tQueueDiags. wUsage	WORD	Events number in the queue
tClient_X.tQueueDiags. dwReserved_0	DWORD	Reserved
tClient_X.tQueueDiags. dwReserved_1	DWORD	Reserved
tClient_X.tStats.wRXFrames	WORD	Number of received frames
tClient_X.tStats.wTXFrames	WORD	Number of sent frames
tClient_X.tStats.wCommErrors	WORD	Communication errors counter, including physical layer, link layer and transport layer errors.
tClient_X.tStats.dwReserved_0	DWORD	Reserved
tClient_X.tStats.dwReserved_1	DWORD	Reserved

Table 146: IEC 60870-5-104 Server Diagnostics

5.8.14.8. Commands Qualifier

The standard IEC 60870-5-104 foresees four different command qualifiers for the objects *Single Command*, *Double Command* and *Regulating Step Command*, all supported by the Nexto Server.

Each object type has a specific behavior to each command qualifier, as can be seen on the table below.

Qualifier	Protocol IEC 60870-5-104 object type		
	Single Command	Double Command	Regulating Step Command
No additional definition (default)	Same behavior of persistent qualifier.	Same behavior of short pulse qualifier.	Same behavior of short pulse qualifier.
Short pulse duration	Requires command interception to application treatment. Other way it will return a negative acknowledge message (fail).	Requires command interception to application treatment. Other way it will return a negative acknowledge message (fail).	Requires command interception to application treatment. Other way it will return a negative acknowledge message (fail).
Long pulse duration			
Persistent output	The output is going to be on or off and that will remain until new command, according to value (ON or OFF) commanded by the client.		

Table 147: IEC 60870-5-104 Server Commands Qualifier

Note:

Command Interception: For further information about commands interception of IEC 60870-5-104 clients, consult section [Interception of Commands Coming from the Control Center](#), implemented through *CommandReceiver* function block.

5.8.15. CANOpen Manager

CANopen is a protocol based on CAN bus which provides fast I/O update (around 5 ms for a 1000 kbit/s network with a few slaves) with a simple twisted pair physical bus infrastructure.

The CANopen Manager (master) is responsible for controlling the slave devices, managing their operation state and exchanging I/O and other service data. By default, the CANopen manager protocol activities (bus cycle) are executed on the context of MainTask, keeping it synchronous with the execution of application code.

The configuration of CANopen network is performed with the support of EDS files, which describes the I/O data and service objects (PDO and SDO) of the slave and must be provided by the device manufacturer.

Additionally, an application library called CiA405 is provided with FunctionBlocks which allows to perform several specific actions like changing the slave state (NMT), receiving emergency object, querying the slave state and performing SDO read/write commands. The complete description of CiA405 library can be found on *Online Help* (F1) of MasterTool IEC XE.

ATTENTION

- Only one CANopen Manager instance per project is allowed
- The CANopen specification allows up to 127 nodes (including Manager).

A special care must be taken considering the physical bus length and the selected baudrate. The following table shows the maximum bus length that can be used safely with a given baudrate:

Baudrate	Maximum Bus Length
1000 kbit/s	25 m
500 kbit/s	100 m
250 kbit/s	250 m
125 kbit/s	500 m
100 kbit/s	700 m
< 50 kbit/s	1000 m

Table 148: Baudrate X Bus Length

5.8.15.1. Installing and inserting CANopen Devices

The configuration of a CANopen network uses the same standard procedure of other fieldbuses configuration on MasterTool IEC XE.

To add a CANopen Manager, right-click on the *CAN* interface and select *Add Device*. Expand the items until finding *CANopen_Manager* device and click on the *Add Device* button. The *CANopen Manager* device will appear below the CAN interface as shown on the following picture:

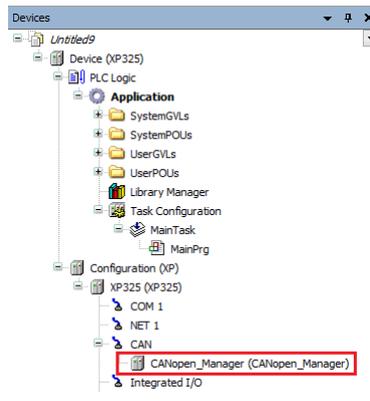


Figure 139: Adding CANopen Manager

To add a CANopen slave device, first you need to install it on the *Device Repository*. To do that, go to *Tools -> Device Repository* and install the device EDS file.

After that, right-click on the *CANopen_Manager* device and click on *Add Device*. Search the devices you desire and click on *Add Device* button like shown on the following picture:

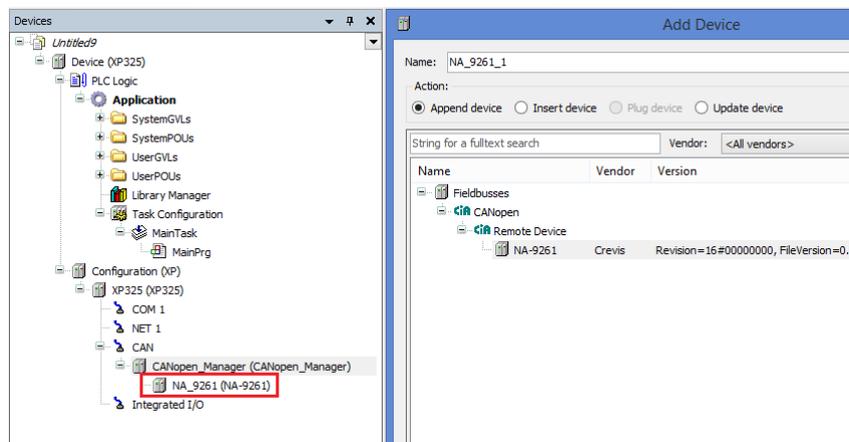


Figure 140: Adding CANopen Slave Device

5.8.15.2. CANopen Manager Configuration

The CANopen Manager comes with a ready-to-use configuration (default values). Typically, it is just needed to set the correct baudrate and slave address to have a network running.

The main parameters of CANopen manager are located at *General* tab:

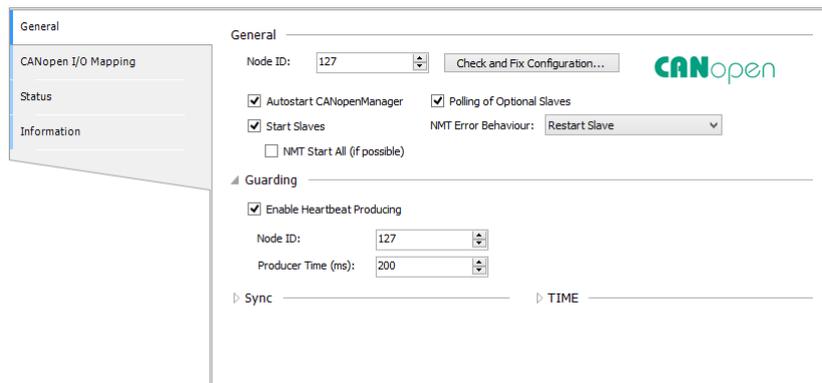


Figure 141: CANopen Manager general parameters

The detailed description of CANopen Manager general parameters can be found on section *Device Editors -> CANopen* of MasterTool IEC XE Online Help (F1).

Additionally, the tab *CANopen I/O Mapping* allows to change the bus cycle task:

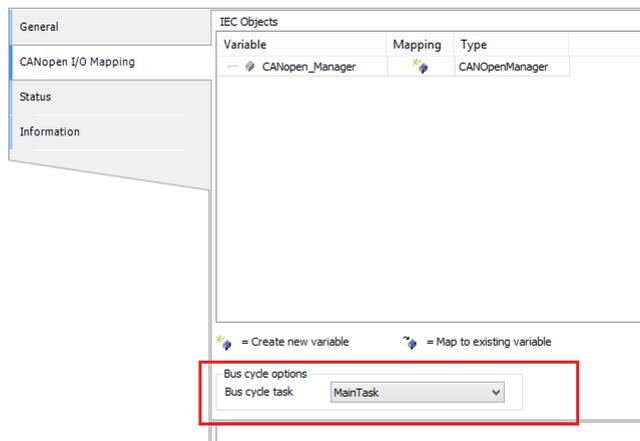


Figure 142: CANopen Manager bus cycle task setting

By default, the bus cycle task is configured to use the MainTask. This is the recommended setting for most of the applications. Changing this setting is only required on a very specific scenario which requires the implementation of a time-critical control loop using CANopen I/O (5ms lets say) that can not be performed on MainTask due to heavy application code.

5.8.15.3. CANopen Slave Configuration

The configuration of CANopen Remote Devices (Slaves) is separated in the first four tabs shown on the following picture:

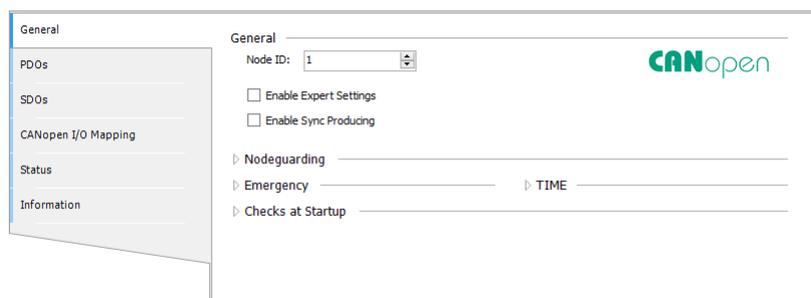


Figure 143: CANopen Slave parameters

The *General* tab contains the slave address (Node ID), Nodeguarding and Emergency object settings.

The *PDO* tab contains the configuration of process data (I/O data) that will be exchanged.

The *SDO* tab contains the SDO objects which can be selected to be accessed by SDO read/write FunctionBlock provided by CiA405 library.

The detailed description of CANopen Slave parameters can be found on section "*Device Editors -> CANopen* of Master-Tool IEC XE Online Help (F1).

5.8.16. PROFINET Controller

For correct use of the PROFINET Controller protocol, it is necessary to consult the manual MU214621 - Nexto Series PROFINET Manual .

5.9. Communication Performance

5.9.1. MODBUS Server

The MODBUS devices configurable in the Nexto CPU run in the background, with a priority below the user application and cyclically. Thus, their performance varies depending on the remaining time, taking into account the difference between the interval and time that the application takes to run. For example, a MODBUS device in an application that runs every 100 ms, with a running time of 50 ms, will have a lower performance than an application running every 50 ms to 200 ms of interval. It happens because in the latter case, the CPU will have a longer time between each MainTask cycle to perform the tasks with lower priority.

It also has to be taken into account the number of cycles that the device, slave or server takes to respond to a request. To process and transmit a response, a MODBUS RTU Slave will takes two cycles (cycle time of the MODBUS task), where as a MODBUS Ethernet Server task takes only one cycle. But this is the minimum time between receipt of a request and the reply. If the request is sent immediately after the execution of a task MODBUS cycle time may be equal to 2 or 3 times the cycle time for the MODBUS slave and from 1 to 2 times the cycle time for the MODBUS server.

In this case: Maximum Response Time = 3 * (cycle time) + (time of execution of the tasks) + (time interframe chars) + (send delay).

For example, for a MODBUS Ethernet Server task with a cycle of 50 ms, an application that runs for 60 ms every 100 ms, the server is able to run only one cycle between each cycle of the application. On the other hand, using the same application, running for 60 ms, but with an interval of 500 ms, the MODBUS performs better, because while the application is not running, it will be running every 50 ms and only each cycle of the MainTask it will take longer to run. For these cases, the worst performance will be the sum of the Execution Time of the user application with the cycle time of the MODBUS task.

For the master and client devices the operating principle is exactly the same, but taking into account the polling time of the MODBUS relation and not the cycle time of the MODBUS task. For these cases, the worst performance of a relationship will be performed after the polling time, along with the user application Execution Time.

It is important to stress that the running MODBUS devices number also changes its performance. In an user application with Execution Time of 60 ms and interval of 100 ms, there are 40 ms left for the CPU to perform all tasks of lower priority. Therefore, a CPU with only one MODBUS Ethernet Server will have a higher performance than a CPU that uses four of these devices.

5.9.1.1. CPU's Integrated Interfaces

For a device MODBUS Ethernet Server, we can assert that the device is capable to answer a x number of requisitions per second. Or, in other words, the Server is able to transfer n bytes per second, depending on the size of each requisition. As smaller is the cycle time of the MODBUS Server task, higher is the impact of the number of connections in his answer rate. However, for cycle times smaller than 20 ms this impact is not linear and the table below must be viewed for information.

The table below exemplifies the number of requisitions that a MODBUS Server inserted in a integrated Ethernet interface is capable to answer, according to the cycle time configured for the MODBUS task and the number of active connections:

Number of Active Connections	Answered requisitions per second with the MODBUS task cycle at 5 ms	Answered requisitions per second with the MODBUS task cycle at 10 ms	Answered requisitions per second with the MODBUS task cycle at 20 ms
1 Connection	185	99	50
2 Connections	367	197	100
4 Connections	760	395	200
7 Connections	1354	695	350
10 Connections	1933	976	500

Table 149: Communication Rate of a MODBUS Server at Integrated Interface

ATTENTION

The communication performances mentioned in this section are just examples, using a CPU with only one device MODBUS TCP Server, with no logic to be executed inside the application that could delay the communication. Therefore, these performances must be taken as the maximum rates.

For cycle times equal or greater than 20 ms, the increase of the answer rate is linear, and may be calculated using an equation:

$$N = C \times (1 / T)$$

Where:

N is the medium number of answers per second;

C is the number of active connections;

T is the MODBUS task interval in seconds.

As an example a MODBUS Server, with only one active connection and a cycle time of 50 ms we get:

$$C = 1; T = 0,05 \text{ s};$$

$$N = 1 \times (1 / (0,05))$$

$$N = 20$$

That is, in this configuration the MODBUS Server answers, on average, 20 requisitions per second.

In case the obtained value is multiplied by the number of bytes in each requisition, we will obtain a transfer rate of n bytes per second.

5.9.1.2. Remote Interfaces

The performance of a device MODBUS Server in one remote Ethernet interface is similar to the performance in the CPU's integrated interfaces.

However, due to time of the communication between the CPU and the modules, the maximum performance is limited. For only one active connection, the number of answers is limited in the maximum of 18 answers per second. With more active connections, the number of answers will increase linearly, exactly like the integrated interfaces, however being limited at the maximum of 90 answers per second. So, for a remote Ethernet interface, we will have the following forms to calculate his performance:

For $T \leq 55 \text{ ms}$ is used:

$$N = C \times (18,18 - (18,18 / (0,055 \times 1000)))$$

And for $T \geq 55 \text{ ms}$ is used:

$$N = C \times (Z - (Z / (T \times 1000)))$$

Where N is the medium number of answers per second, C is the number of active connections and T is equal to the cycle time of the MODBUS task (in seconds).

The user must pay attention to the fact that the maximum performance of a device MODBUS Server in one remote Ethernet interface is 90 answers of requisitions per second.

5.9.2. OPC UA Server

The OPC UA Server MU214609 analyzes the performance of OPC UA communication in greater detail, including addressing the consumption of Ethernet communication bandwidth. This manual also discusses concepts about the operation of the OPC UA protocol.

5.9.3. IEC 60870-5-104 Server

The IEC 60870-5-104 Server driver is executed by the CPU in the same way as the other communication drivers Servers, that is, in the background, with a priority below the user application and cyclically. The task of this The driver specifically executes every 50 ms, and 1 driver execution cycle is enough to process and respond to requests. However, as it is a low priority task, it is not guaranteed to be able to run at this frequency because depends on the percentage of free CPU (difference between the MainTask interval and the time that the user application takes to be executed) and also concurrency with tasks from other protocols configured in the CPU.

To help in the comprehension of the driver IEC 60870-5-104 Server performance are presented the result of some test done with an IEC 60870-5-104 Client simulator, connected to a NX3030 running an IEC 60870-5-104 Server. The configured data base was compose of 900 digital points and 100 analog points (all with quality and time stamp), and the MainTask was using 70 ms (of the 100 ms interval).

- Time to complete a general interrogation command: less than one second
- Time to transfer 900 digital events + 100 analog events: 6 seconds

5.10. System Performance

In cases where the application has only one MainTask user task responsible for the execution of a single Program type programming unit called MainPrg (as in Single Profile), the PLC consumes a certain amount of time for the task to be processed. At that time we call it as *Execution Time*.

In an application the average application *Execution Time* can be known using the MasterTool IEC XE in the *Device* item of its *Devices Tree* as follows:

PLC Logic-> Application-> Task Configuration in the *Monitor* tab, *Average Cycle Time* column.

The user must pay attention to the *Cycle Time* so that it does not exceed 80% of the interval set in the MainTask user task. For example, in an application where the interval is 100 ms, an appropriate *Cycle Time* is up to 80 ms. This is due to the fact that the CPU needs time to perform other tasks such as communication processing, processing of the display and memory card, and these tasks take place within the range (the remaining 20% of *Cycle Time*).

ATTENTION

For very high cycle times (typically higher than 300 ms), even that the value of 80% is respected, it may occur a reduction in the display response time and of the diagnostics key. In case the 80 percentage is not respected and the running time of the user task is closer or exceeds the interval set for the MainTask, the screen and the diagnosis button cannot respond once its priority in the system running is lower than the user tasks. In case an application with errors is loaded in the CPU, it may be necessary to restart it without loading this application as shown in the System Log section.

ATTENTION

The CPU's system logs of the Nexto Series, starting from firmware version 1.4.0.33 now reloaded in case of a CPU reset or a reboot of the *Runtime System*, that is, you can view the older logs when one of these conditions occurs.

5.10.1. I/O Scan Time

For a project that uses digital I/O modules, being them inserted into the bus and declared in the project, the MainTask time will increase according to the number of modules. The table below illustrates the average time that is added to the MainTask:

Declared Modules in the Bus	Added Time in the MainTask Cycle Time (μ S)
5	300
10	700
20	1000

Table 150: I/O Scanning Time

In projects that use remote I/Os, for example, using the NX5001 PROFIBUS-DP Master module, the manual of the respective module has to be consulted for information about performance and influences of the module in the execution of user tasks.

5.10.2. Memory Card

Data transfers involving the memory card is performed by the CPU in the background, as this gives priority to the execution of user application and communication processing. Thus, the transfer of files to the card may suffer an additional significant time, depending on the Cycle Time of the user application.

The time required to read/write files on the card will be directly affected by the Cycle Time of the user application since this application has priority in execution.

Further information about the use of the memory card see [Memory Card](#) section.

5.11. RTC Clock

The CPUs have an internal clock that can be used through the *NextoStandard.lib* library. This library is automatically loaded during the creation of a new project (to perform the library insertion procedure, see [Libraries](#) section). The figure below shows how to include the blocks in the project:

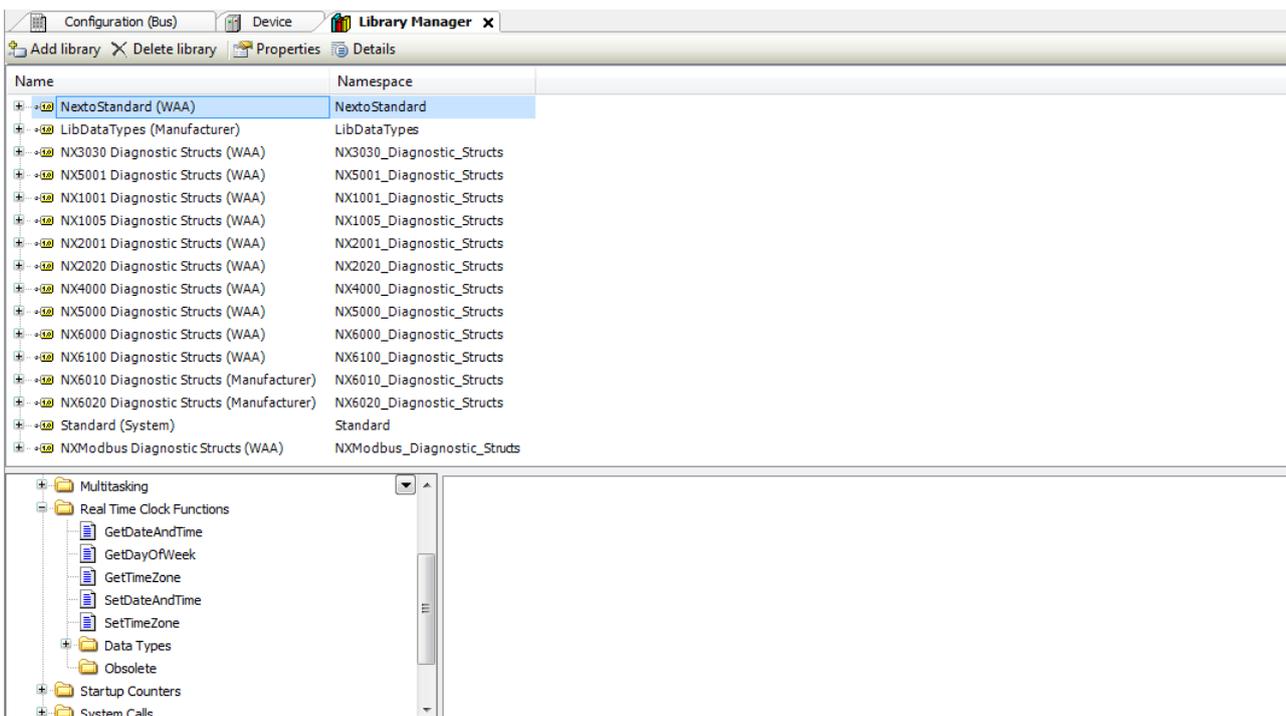


Figure 144: Clock Reading and Writing Blocks

ATTENTION

Function blocks of RTC Reading and Writing, previously available in 2.00 MasterTool IEC XE or older become obsolete from 2.00 or newer, the following blocks are no longer used: *NextoGetDateAndTime*, *NextoGetDateAndTimeMs*, *NextoGetTimeZone*, *NextoSetDateAndTime*, *NextoSetDateAndTimeMs* and *NextoSetTimeZone*.

5.11.1. Function Blocks for RTC Reading and Writing

Among other function blocks, there are some very important used for clock reading (*GetDateAndTime*, *GetDayOfWeek* and *GetTimeZone*) and for date and time new data configuring (*SetDateAndTime* and *SetTimeZone*). These functions always use the local time, that is, take into account the value defined by the *Time Zone*.

The proceedings to configure these two blocks are described below.

5.11.1.1. Function Blocks for RTC Reading

The clock reading can be made through the following functions:

5.11.1.1.1. GetDateAndTime



Figure 145: Date and Hour Reading

Input Parameters	Type	Description
DATEANDTIME	EXTENDED_DATE_AND_TIME	This variable returns the value of date and hour of RTC in the format shown at Table 160.

Table 151: Input Parameters of GetDateAndTime

Output Parameters	Type	Description
GETDATEANDTIME	RTC_STATUS	Returns the function error state, see Table 162.

Table 152: Output Parameters of GetDateAndTime

Utilization example in ST language:

```
PROGRAM UserPrg
VAR
Result : RTC_STATUS;
DATEANDTIME : EXTENDED_DATE_AND_TIME;
xEnable : BOOL;
END_VAR
-----
IF xEnable = TRUE THEN
```

```
Result := GetDateAndTime (DATEANDTIME);
xEnable := FALSE;
END_IF
```

5.11.1.1.2. *GetTimeZone*

The following function reads the Time Zone configuration, this function is directly related with time in Time Zone at SNTP synchronism service:

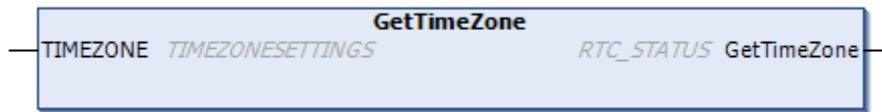


Figure 146: Configuration Reading of Time Zone

Input Parameters	Type	Description
TIMEZONE	TIMEZONESETTINGS	This variable presents the reading of Time Zone configuration.

Table 153: Input Parameters of GetTimeZone

Output Parameters	Type	Description
GetTimeZone	RTC_STATUS	Returns the function error state, see Table 162.

Table 154: Output Parameters of GetTimeZone

Utilization example in ST language:

```
PROGRAM UserPrg
VAR
GetTimeZone_Status : RTC_STATUS;
TimeZone : TIMEZONESETTINGS;
xEnable : BOOL;
END_VAR

-----
IF xEnable = TRUE THEN
GetTimeZone_Status := GetTimeZone(TimeZone);
xEnable := FALSE;
END_IF
```

5.11.1.1.3. *GetDayOfWeek*

GetDayOfWeek function is used to read the day of the week.



Figure 147: Day of Week Reading

Output Parameters	Type	Description
GetDayOfWeek	DAYS_OF_WEEK	Returns the day of the week. See Section 161.

Table 155: Output Parameters of GetDayOfWeek

When called, the function will read the day of the week and fill the structure *DAYS_OF_WEEK*.

Utilization example in ST language:

```

PROGRAM UserPrg
VAR
DayOfWeek : DAYS_OF_WEEK;
END_VAR
-----
DayOfWeek := GetDayOfWeek ();
    
```

5.11.1.2. **RTC Writing Functions**

The clock settings are made through function and function blocks as follows:

5.11.1.2.1. *SetDateAndTime*

SetDateAndTime function is used to write the settings on the clock. Typically the precision is on the order of hundreds of milliseconds.



Figure 148: Set Date And Time

Input parameters	Type	Description
REQUEST	BOOL	This variable, when receives a rising edge, enables the clock writing.
DATEANDTIME	EXTENDED_DATE _AND_TIME	Receives the values of date and hour with milliseconds. See section 160.

Table 156: Input Parameters of SetDateAndTime

Output parameters	Type	Description
DONE	BOOL	This variable, when true, indicates that the action was successfully completed.
EXEC	BOOL	This variable, when true, indicates that the function is processing the values.
ERROR	BOOL	This variable, when true, indicates an error during the Writing.
STATUS	RTC_STATUS	Returns the error occurred during the configuration. See Table 162.

Table 157: Output Parameters of SetDateAndTime

When a rising edge occurs at the *REQUEST* input, the function block will write the new *DATEANDTIME* values on the clock. If the writing is successfully done, the *DONE* output will be equal to *TRUE*. Otherwise, the *ERROR* output will be equal to *TRUE* and the error will appear in the *STATUS* variable.

Utilization example in ST language:

```

PROGRAM UserPrg
VAR
SetDateAndTime : SetDateAndTime;
xRequest : BOOL;
DateAndTime : EXTENDED_DATE_AND_TIME;
xDone : BOOL;
xExec : BOOL;
xError : BOOL;
xStatus : RTC_STATUS;
END_VAR
-----
IF xRequest THEN
    SetDateAndTime.REQUEST:=TRUE;
    SetDateAndTime.DATEANDTIME:=DateAndTime;
    xRequest:= FALSE;
END_IF
SetDateAndTime ();
SetDateAndTime.REQUEST:=FALSE;
IF SetDateAndTime.DONE THEN
    xExec:=SetDateAndTime.EXEC;
    xError:=SetDateAndTime.ERROR;
    xStatus:=SetDateAndTime.STATUS;
END_IF
    
```

ATTENTION

If the user attempts to write time values outside the RTC range, the values will be converted to valid ones, as long as they do not exceed the range described in section [RTC Operating Limits](#). For example, if the user tries to write the value 2000 ms, it will be converted to 2 seconds; if 100 seconds are written, it will be converted to 1 minute and 40 seconds; if 30 hours are written, it will be converted to 1 day and 6 hours, and so on.

5.11.1.2.2. *SetTimeZone*

The following function block makes the writing of the time zone settings:

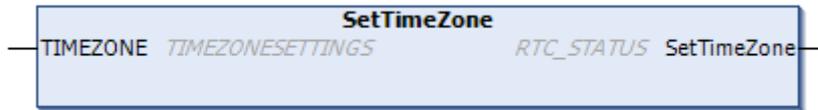


Figure 149: Writing of the Time zone Settings

Input parameters	Type	Description
TIMEZONE	TIMEZONESETTINGS	Structure with time zone to be configured. See Table 163.

Table 158: SetTimeZone Input Parameters

Output parameters	Type	Description
SetTimeZone	RTC_STATUS	Returns the error occurred during the reading/setting. See Table 162.

Table 159: SetTimeZone Output Parameters

When called, the function will configure the *TIMEZONE* with the new system time zone configuration. The configuration results is returned by the function.

Utilization example in ST language:

```

PROGRAM UserPrg
VAR
Status : RTC_STATUS;
TimeZone : TIMEZONESETTINGS;
xWrite : BOOL;
END_VAR

-----
//FB SetTimeZone
IF (xWrite = TRUE) THEN
Status := SetTimeZone(TimeZone);
  IF Status = RTC_STATUS.NO_ERROR THEN
    xWrite := FALSE;
  END_IF
END_IF

```

ATTENTION

To adjust the clock, time and date values must be within the range described in section [RTC Operating Limits](#); otherwise, an error will be reported through the *STATUS* output parameter. For more details about the *STATUS* output parameter, refer to section [RTC_STATUS](#).

5.11.2. RTC Data Structure

The reading and setting function blocks of the Nexto Series CPUs RTC use the following data structures in its configuration:

5.11.2.1. EXTENDED_DATE_AND_TIME

This structure is used to store the RTC date when used the function blocks for date reading/setting within milliseconds of accuracy. It is described in the table below:

Structure	Type	Variable	Description
EXTENDED_DATE_AND_TIME	BYTE	byDayOfMonth	Stores the day of the set date.
	BYTE	ByMonth	Stores the month of the set date.
	WORD	wYear	Stores the year of the set date.
	BYTE	byHours	Stores the hour of the set date.
	BYTE	byMinutes	Stores the minutes of the set date.
	BYTE	bySeconds	Stores the seconds of the set date.
	WORD	wMilliseconds	Stores the milliseconds of the set date.

Table 160: EXTENDED_DATE_AND_TIME

5.11.2.2. DAYS_OF_WEEK

This structure is used to store the day of week:

Enumerable	Value	Description
DAYS_OF_WEEK	0	INVALID_DAY
	1	SUNDAY
	2	MONDAY
	3	TUESDAY
	4	WEDNESDAY
	5	THURSDAY
	6	FRIDAY
	7	SATURDAY

Table 161: DAYS_OF_WEEK Structure

5.11.2.3. RTC_STATUS

This enumerator is used to return the type of error in the RTC setting or reading and it is described in the table below:

Enumerator	Value	Description
RTC_STATUS	NO_ERROR (0)	There is no error.
	UNKNOWN_COMMAND (1)	Unknown command.
	DEVICE_BUSY (2)	Device is busy.
	DEVICE_ERROR (3)	Device with error.
	ERROR_READING_OSF (4)	Error in the reading of the valid date and hour flag.
	ERROR_READING_RTC (5)	Error in the date and hour reading.
	ERROR_WRITING_RTC (6)	Error in the date and hour writing.
	ERROR_UPDATING_SYSTEM_TIME (7)	Error in the update of the system's date and hour.
	INTERNAL_ERROR (8)	Internal error.
	INVALID_TIME (9)	Invalid date and hour.
	INPUT_OUT_OF_RANGE (10)	Out of the limit of valid date and hour for the system.
	SNTP_NOT_ENABLE (11)	Error generated when the SNTP service is not enabled and it is done an attempt for modifying the time zone.

Table 162: RTC_STATUS

5.11.2.4. TIMEZONESETTINGS

This structure is used to store the time zone value in the reading/setting requests of the RTC's function blocks and it is described in table below:

Structure	Type	Variable	Description
TIMEZONESETTINGS	INT	iHour	Set time zone hour.
	INT	iMinutes	Set time zone minute.

Table 163: TIMEZONESETTINGS

Note:

Function Blocks of Writing and Reading of Date and Hour: different libraries of *NextoStandard*, which have function blocks or functions that may perform access of reading and writing of date and hour in the system, are not indicated. The *NextoStandard* library has the appropriate interfaces for writing and reading the system's date and hour accordingly and for informing the correct diagnostics.

5.11.3. RTC Operating Limits

The values presented in [Table 164](#) indicate the earliest and latest time instants that the RTC clock can represent. The minimum value corresponds to the earliest date and time that can be set, while the maximum value represents the latest valid future date and time. These limits must be respected when setting or reading the product's clock, ensuring that all date and time functions operate correctly.

Parameter	Minimum	Maximum
Day	1	31

Parameter	Minimum	Maximum
Month	1	12
Year	2000	2099
Hour	0	23
Minute	0	59
Second	0	59
Millisecond	0	999

Table 164: Valid value range for the RTC Clock

5.12. User Files Memory

Nexto Series CPUs have a memory area destined to the general data storage, in other words, the user can store several project files of any format in the CPU memory. This memory area varies according to the CPU model used (check [Memory](#) section).

In order to use this area, the user must access a project in the MasterTool IEC XE software and click on the *Devices Tree*, placed at the program left. Double click on the *Device* item and, after selecting the CPU in the *Communication Settings* tab which will be open, select the *Files* tab and click on *Refresh*, both in the computer files column (left) and in the CPU files column (right) as shown on figure below.

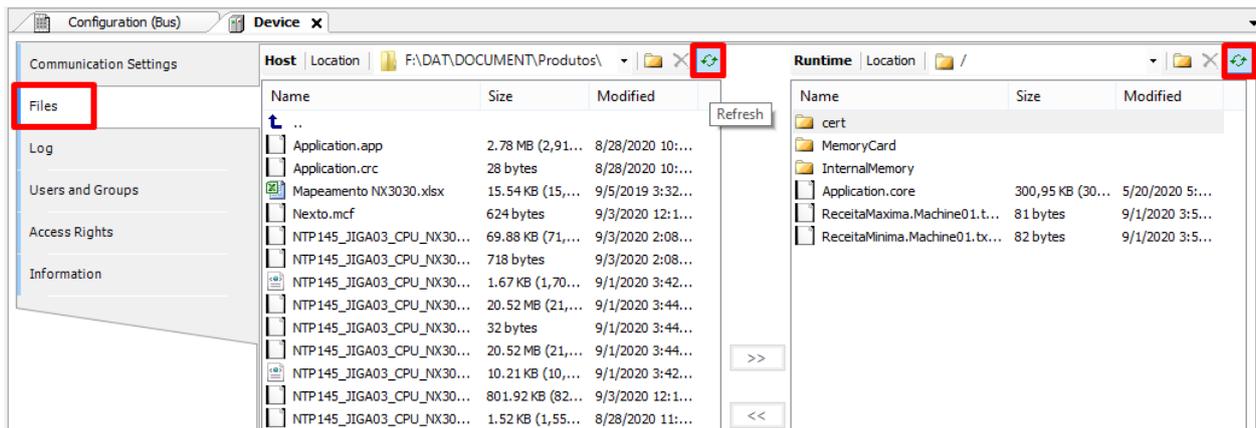


Figure 150: User Files Access

After updating the CPU column of files, the root directory of files stored in the CPU will be shown. Then it will be possible to select the folder where the files will be transferred to. The *InternalMemory* folder is a default folder to be used to store files in the CPU’s internal memory, since it is not possible to transfer files to the root directory. If necessary, the user can create other folders in the root directory or subfolders inside the *InternalMemory* folder.

The *MemoryCard* folder is the directory where the memory card is mounted, if it is inserted into the CPU. Files which are transferred to the *MemoryCard* are being transferred directly into the memory card. As new features are being added to the product, some folders may appear and which should be ignored by the user.

In order to perform a file transfer from the microcomputer to the CPU just select the desired file in the left column and press the “>” key located in the center of the screen, as shown in figure below. The download time will vary depending on file size and cycle time (execution) of the current application of the CPU and may take several minutes.

The user does not need to be in *Run Mode* or connected to the CPU to perform the transfers, since it has the ability to connect automatically when the user performs the transfer.

4. INITIAL PROGRAMMING

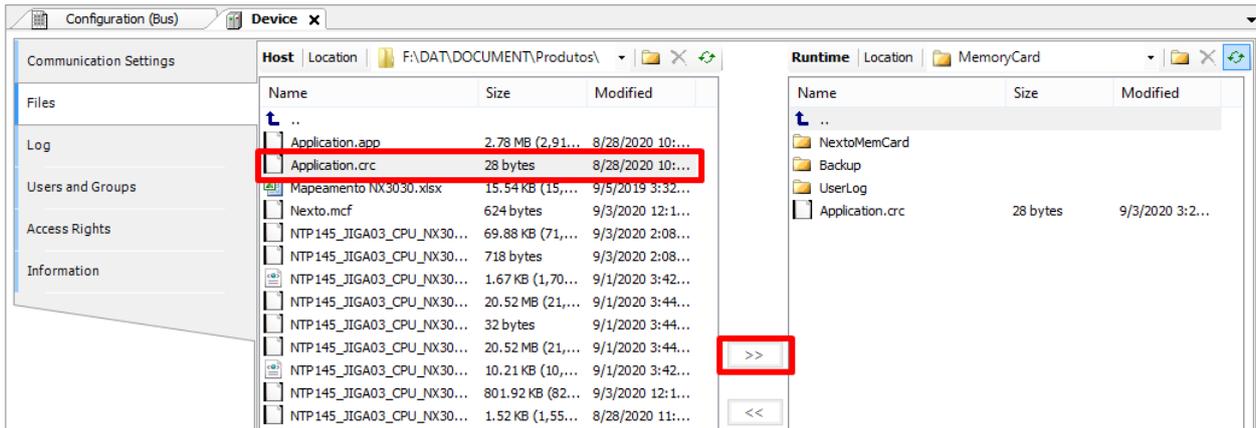


Figure 151: Files Transference

ATTENTION

The files contained in the folder of a project created by MasterTool IEC XE have special names reserved by the system in this way cannot be transferred through the *Files* tab. If the user wishes to transfer a project to the user memory, you must compact the folder and then download the compressed file (*.zip for example).

In case it is necessary to transfer documents from the CPU to the PC in which the MasterTool IEC XE software is installed, the user must follow a very similar procedure to the previously described, as the file must be selected from the right column and the button “<<” pressed, placed on the center of the screen.

Furthermore, the user has some operation options in the storing files area, which are the following:

- New directory : allows the creation of a new folder in the user memory area.
- Delete item : allows the files excluding in the folders in the user memory area.
- Refresh : allows the file updating, on the MasterTool IEC XE screen, of the files in the user memory area and in the computer.

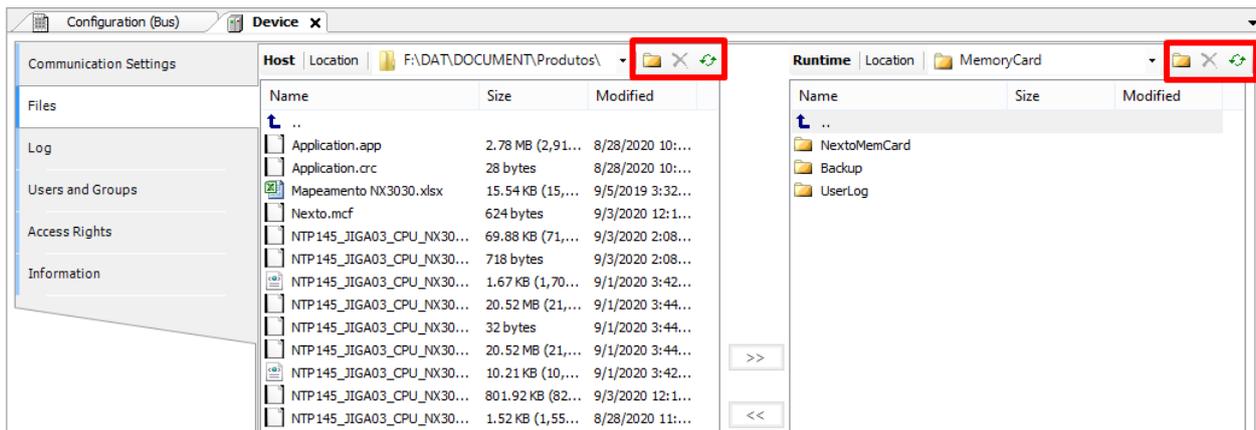


Figure 152: Utilization Options

ATTENTION

For a CPU in Stop Mode or with no application, the transfer rate to the internal memory is approximately 150 Kbytes/s.

5.13. Memory Card

Among other memories, Nexto Series CPUs allow the user the utilization of a memory card. It is defined according the features described in [Memory Card Interface](#) section which stores files.

When the card is inserted in the CPU and it presents a file type different from FAT32, it automatically identifies those files and questions the user if he wants to format the files. In negative case the user cannot use the card, as it is not mounted. The card presence is not displayed. If the user decides to format the files, the CPU takes a few minutes to execute the operation, depending on the cycle time (execution) of the application which is running in the CPU. Once the memory card is mounted, the CPU will read its general information, leaving access to the memory card slower in the first few minutes. This procedure is done only when the card is inserted, in case of the CPU reset or through the device's web page.

ATTENTION

It is recommended to format the memory card directly in the Nexto CPU in order to avoid possible use problems, mounting time increase or even the incorrect functioning. It is not recommended to remove the memory card or de-energize the CPU during the formatting or during the files transfer as it can cause the loss of data as well as irreversible damages.

5.13.1. Memory Card Configuration

A web page was developed for managing the memory card. Among the features offered are formatting, the option to unmount and remove the card, and the ability to enable and disable the card interface. These settings were developed in the "Memory Card" section of the CPU webpage, under the "Management" tab. In addition to the settings, information about the device's current status, total and free storage space, both measured in *kB*, are also displayed. The image below shows the home page, with the interface enabled and no devices connected.

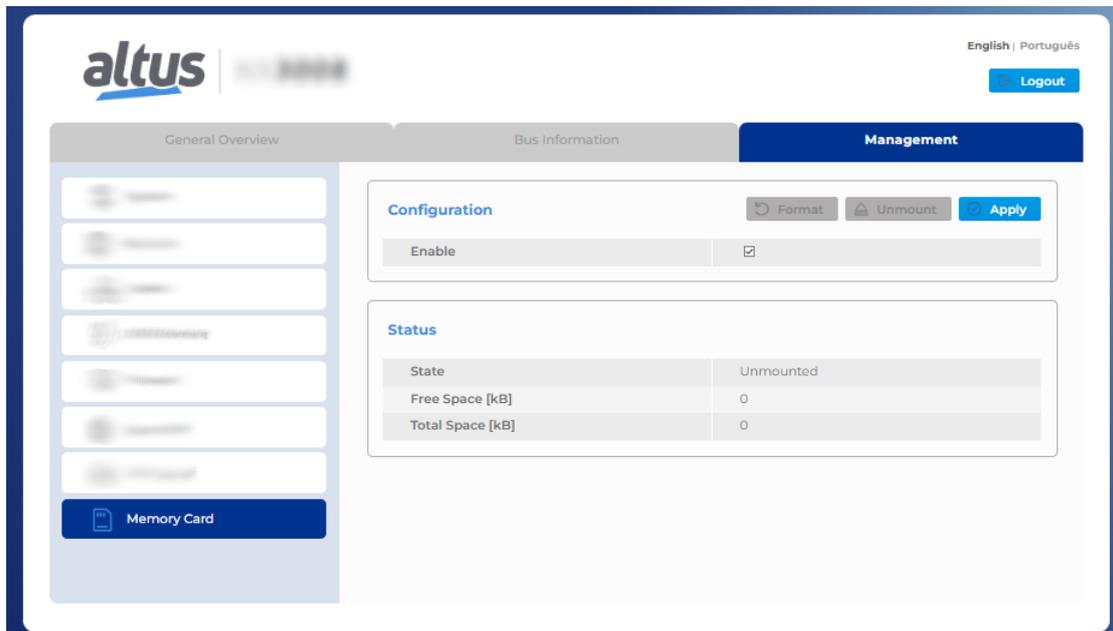


Figure 153: Memory Card Home Page

As long as there is no memory card inserted and mounted in the CPU, the *Format* and *Unmount* buttons remain locked for use. The **Status** table indicates the *Unmounted* state. When a memory card is inserted into the CPU, the *Format* button is enabled for use. After the card is mounted, the *Unmount* button also becomes available for use. When inserting a memory card into the CPU, it may take a few moments for the card to be mounted and the information updated on the web page. The image below shows the web page when a card is connected and mounted in the CPU.

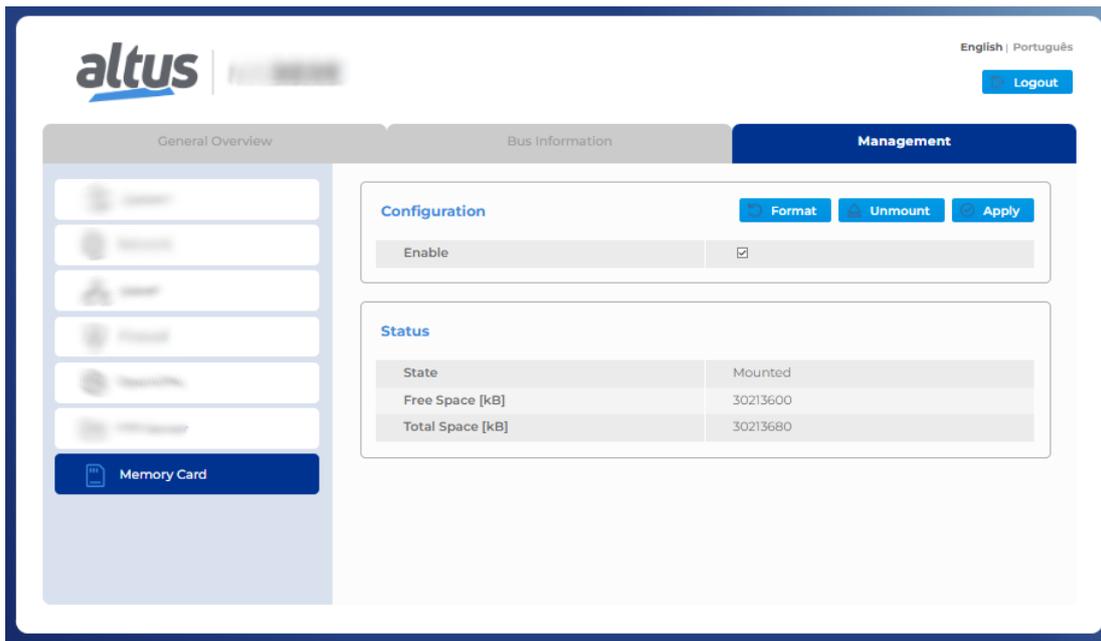


Figure 154: Memory Card Device Mounted

5.13.1.1. Formatting the Memory Card

To format the device, use the **Format** button. When you click, a *pop-up* style message will appear, asking you to confirm the operation. The image below presents this message.

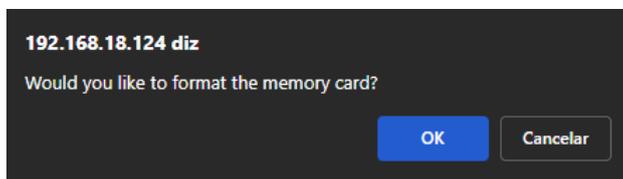


Figure 155: Format Confirmation Message

Upon confirming with the **OK** button, the operation begins, after which all configurations are blocked. The **Format**, **Unmount** and **Apply** buttons, as well as the checkbox, become unavailable during formatting. The formatting process is indicated in the **Status** table, with the **State** value changed to **Formatting...**, as shown in the figure below.

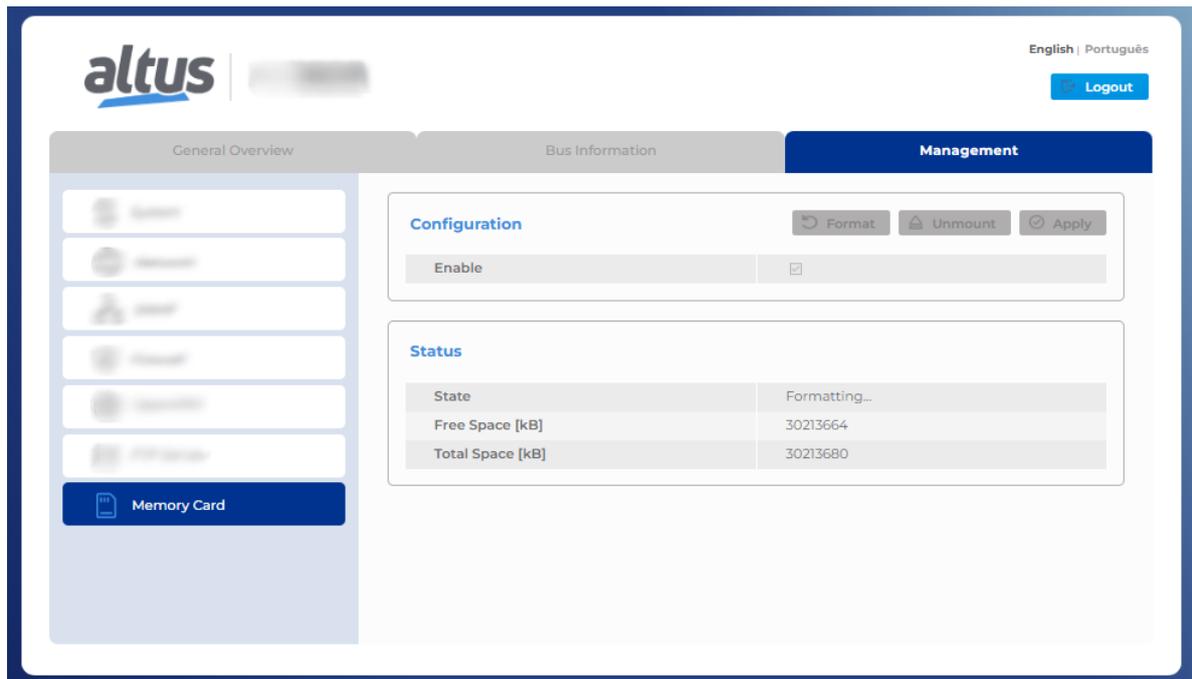


Figure 156: Formatting Memory Card

At the end of the formatting process, a message is displayed indicating that the operation has been completed on the device. The following figure shows this message.

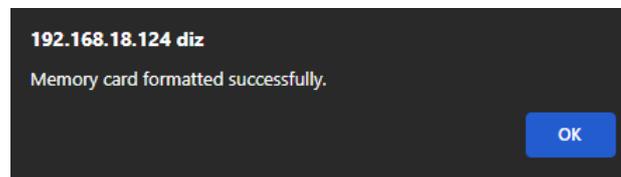


Figure 157: Formatting Complete Message

Upon completion of the operation, the web page returns to its initial state, unlocking all buttons, as well as the checkbox, as shown in figure [Memory Card Device Mounted](#).

5.13.1.2. Unmounting the Memory Card

To unmount and remove the device, click the **Unmount** button. A confirmation *pop-up* will appear asking you to confirm the operation. The image below shows this message.

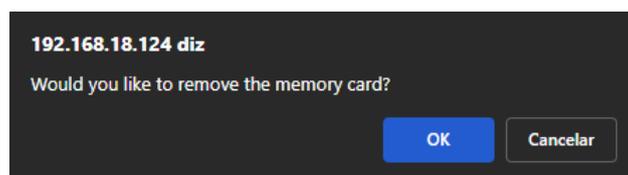


Figure 158: Confirmation Message to Unmount

Upon confirming with the **OK** button, the operation begins, after which all configurations are blocked. The **Format**, **Unmount** and **Apply** buttons, as well as the checkbox, become unavailable during unmounting operation. The unmounting process is indicated in the **Status** table, with the **State** value changed to **Unmounting...**, as shown in the figure below.

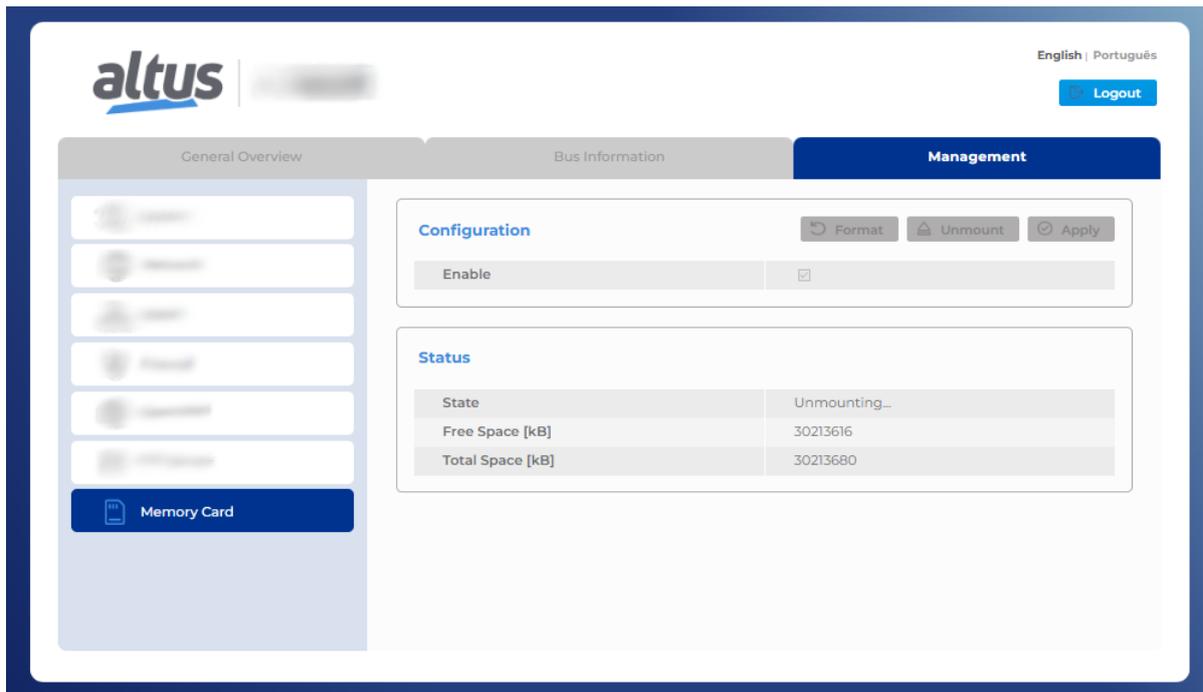


Figure 159: Unmounting Memory Card

At the end of the unmounting process, a message is displayed indicating that the operation on the device has been completed. The following figure shows this message.

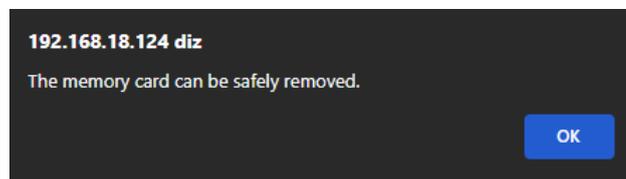


Figure 160: Unmount Complete Message

Upon completion of the operation, the **Format** and **Apply** buttons, as well as the checkbox, become available for use. The **Unmount** button remains locked because the card has already been unmounted. The *Status* table displays the data for an unmounted card, as can be seen in the image below:

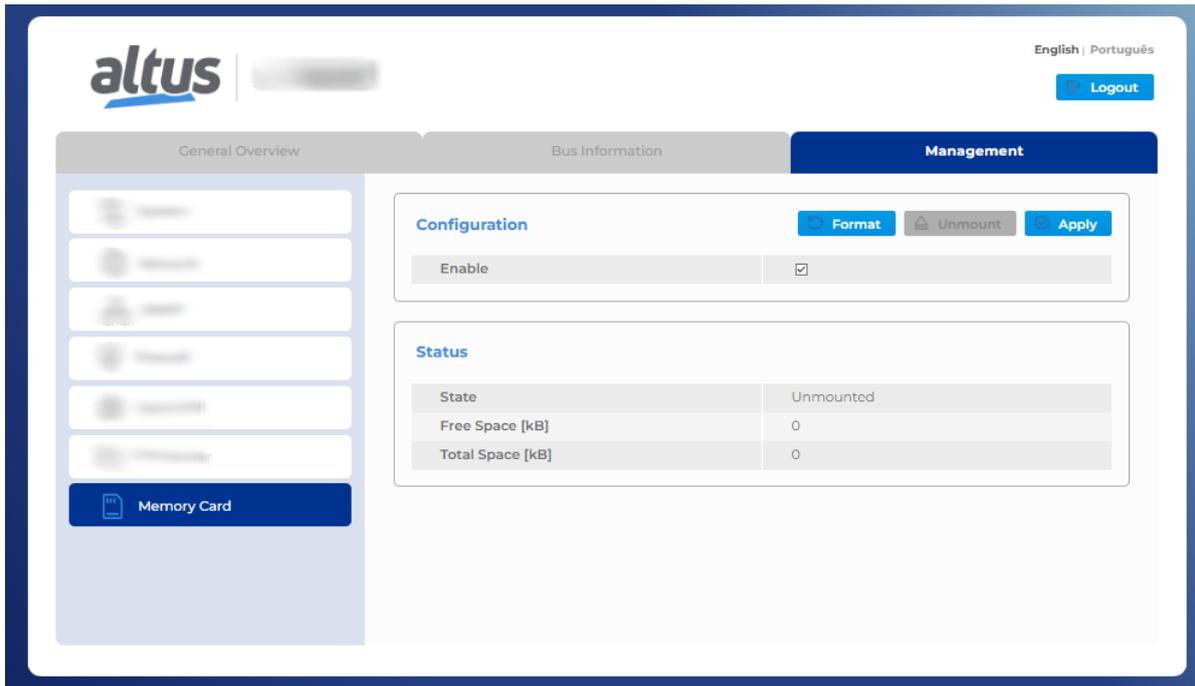


Figure 161: Memory Card Unmounted

5.13.1.3. Memory Card Interface Management

A setting was developed on the card’s web page to enable and disable the memory card interface, this functionality is part of the level one cybersecurity requirements according to IEC 62443. To enable, check the **Enable** checkbox in the **Configuration** table. Then use the **Apply** button to submit the new configuration. To disable, uncheck the **Enable** checkbox and use the same button to apply the setting. Clicking the **Apply** button will display a *pop-up* message asking you to confirm the operation. The image below shows the message.

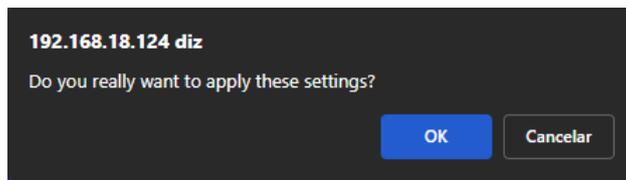


Figure 162: Confirmation Message to Apply Configuration

After confirming by clicking the **OK** button, the new configuration is sent to the CPU. If the interface has been enabled, the information displayed on the web page depends on whether or not a memory card is inserted for mounting. If there is no device, the page will display the information shown in figure [Memory Card Home Page](#). When a device is connected, the information displayed will be as shown in figure [Memory Card Device Mounted](#), after the card has been properly mounted.

If the new configuration disables the interface, the information displayed will be as shown in the image below.

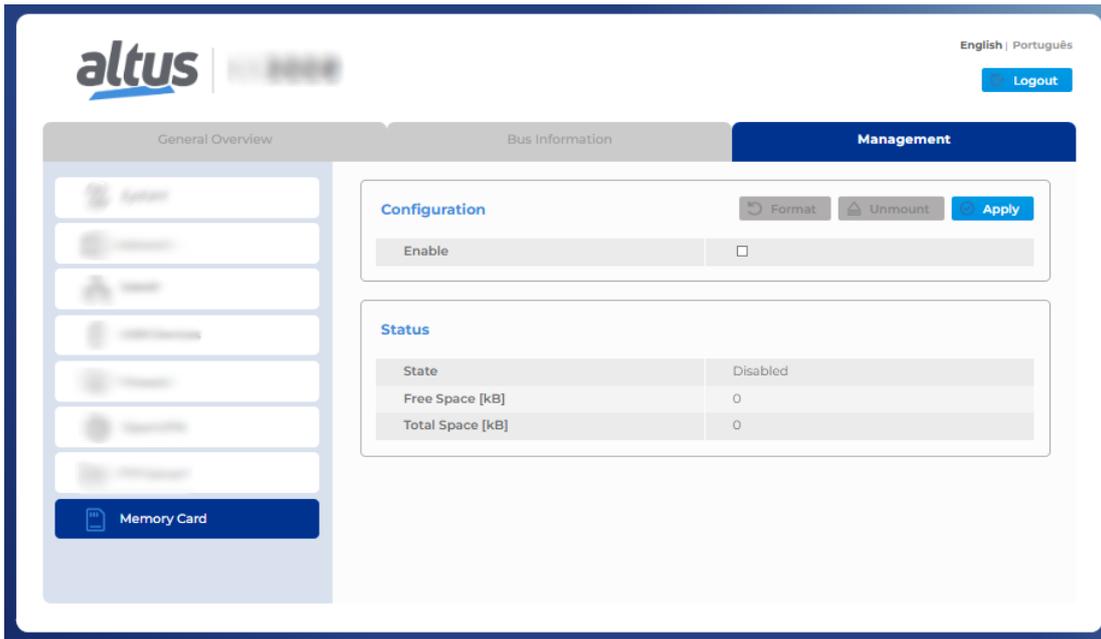


Figure 163: Memory Card Disabled Interface

ATTENTION

If the memory card deactivation is in effect, the MemoryCard folder will not be mounted.

5.13.1.4. Memory Card Interface Management by Application

To facilitate the management of the memory card interface, a function was developed that can be called directly by the user’s application code. The **SetMemCardState** function was implemented within the **NextoStandard** library. The image below shows the library information, as presented in the *Library Manager*.

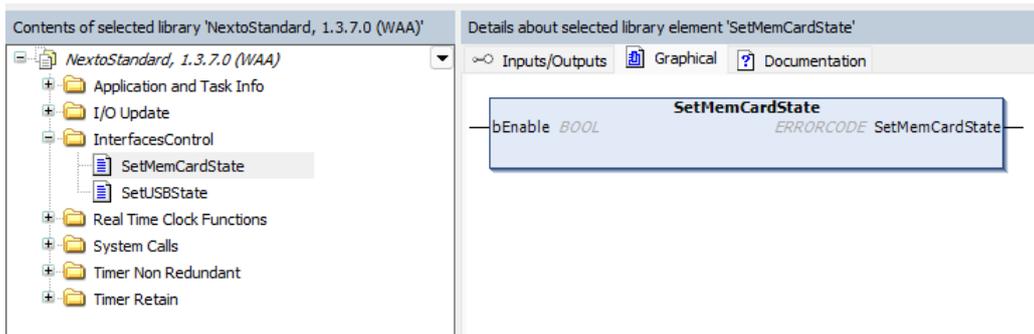


Figure 164: SetMemCardState information in Library Manager

The function has an input variable of type *bool*, **bEnable**, which receives the value to enable or disable the card interface. The function has three return values: *NoError* on success, *SetMemCardStateFail* on failure, or *ImportFunctionNotFound* if the function is not supported. The image below shows a basic example of variable declaration and function call.

```

PROGRAM UserPrg
VAR
  bSetMemoryCardInterfaceState : BOOL;
  stErrorCode : NextoStandard.ERRORCODE;
END_VAR

-----
// Function call example to configurate memory card's interface
stErrorCode:= NextoStandard.SetMemCardState (bEnable :=
  bSetMemoryCardInterfaceState);
    
```

ATTENTION

The function executes the command to set the desired value for the memory card interface. It is neither necessary nor recommended that the function be called cyclically.

5.14. CPU’s Informative and Configuration Menu

The access to the *Informative Menu*, the *Nexto CPU Configuration* and the detailed diagnostics, are available through levels and to access the menu information, change level and modify any configuration, a long touch is required on the diagnostic button and to navigate through the items on the same level, a short touch on the diagnostic button is required. See [One Touch Diag](#) section to verify the functioning and the difference between the diagnostics button touch types.

The table below shows the menu levels and each screen type available in the CPUs, if they are informative, configurable or to return a level.

Level 1	Level 2	Level 3	Type
HARDWARE	TEMPERATURE	-	Informative
	CONTRAST	CONTRAST LEVEL	Configurable
	DATE AND TIME	-	Informative
	BACK	-	Return level
LANGUAGES	ENGLISH	>ENGLISH	Configurable
	PORTUGUES	>PORTUGUES	Configurable
	BACK	-	Return level
NETWORK	NET 1 IP ADDR.	-	Informative
	NET 1 MASK		Informative
	BACK		Return level
SOFTWARE	FIRMWARE	-	Informative
	BOOTLOADER		Informative
	AUX. PROC.		Informative
	BACK		Return level
MEM. CARD	UNMOUNT	-	Configurable
	FORMAT	CONFIRM?	Configurable
	BACK	-	Return level
BACK	-	-	Return level

Table 165: CPU Menu Levels

Memory Card: The memory card will only be available in the menu if it is inserted in the Nexto CPU. As shown on [Table 165](#), between the available options to visualize and modify are the main data necessary to user, as:

- Information about the hardware resources:
 - TEMPERATURE – CPU Internal temperature (Ex.: 36 C 97 F)
 - CONTRAST – Contrast setting of the CPU frontal display
 - DATE AND TIME – Date and time set in the CPU (Ex.: 2001.01.31 00:00)
- Changing the menu language on the CPU:
 - PORTUGUES – Changes the language to Portuguese
 - ENGLISH – Changes the language to English
- Visualization of information about the network set in the device:
 - NET 1 IP ADDR. – Address (Ex.: 192.168.0.1)
 - NET 1 MASK – Subnet mask (Ex.: 255.255.255.0)
- Information about the software versions:
 - FIRMWARE – CPU software version (Ex.: 1.0.0.0)
 - BOOTLOADER – CPU bootloader version (Ex.: 1.0.0.0)
 - AUX. PROC. – CPU auxiliary processor version (Ex.: 1.0.0.0)

The figure below describes an example of how to operate the Nexto CPUs menu through the contrast adjust menu procedure from the *Status* screen. Besides making the configuration easier, it is possible to identify all screen levels and the touch type to navigate through them, and to modify other parameters as change the *Language*, using the same access logic. The short touch shows the contrast is being incremented (clearer) and in the next touch after its maximum value, it returns to the minimum value (less clear). The long touch shows the confirmation of the desired contrast and its return to the previous level.

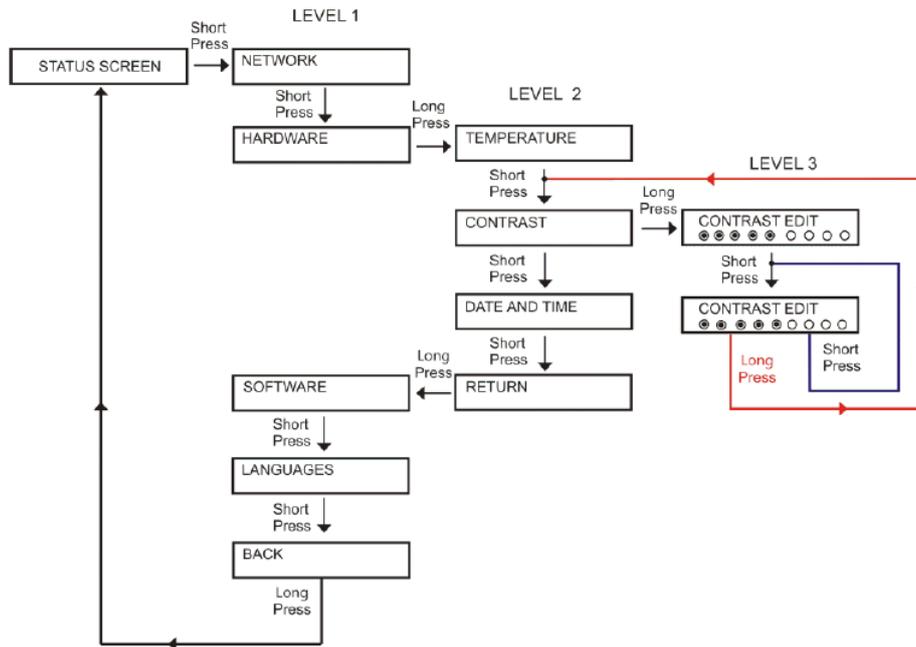


Figure 165: Contrast Adjust

Besides the possibility of the Nexto CPUs menu to be closed through a long touch on the screen diagnostic button *BACK* from level 1, there are also other output conditions that are described below:

- Short touch, at any moment, in the other modules existent on the bus, make the CPU disconnect from the menu and show the desired module diagnostic.
- Idle time, at any level, superior to 5 s.

5.15. Function Blocks and Functions

5.15.1. Special Function Blocks for Serial Interfaces

The special function blocks for serial interfaces make possible the local access (COM 1 and COM 2 - if available) and also access to remote serial ports (expansion modules). Therefore, the user can create his own protocols and handle the serial ports as he wishes, following the IEC 61131-3 languages available in the MasterTool IEC XE software. The blocks are available inside the *NextoSerial* library which must be added to the project so it's possible to use them (to execute the library insertion procedure, see MasterTool IEC XE Programming Manual – MP399609, section Library).

The special function blocks for serial interfaces can take several cycles (consecutive calls) to complete the task execution. Sometimes a block can be completed in a single cycle, but in the general case, needs several cycles. The task execution associated to a block can have many steps which some depend on external events, that can be significantly delayed. The function block cannot implement routines to occupy the time while waits for these events, because it would make the CPU busy. The solution could be the creation of blocking function blocks, but this is not advisable because it would increase the user application complexity, as normally, the multitask programming is not available. Therefore, when an external event is waited, the serial function blocks are finished and the control is returned to the main program. The task treatment continues in the next cycle, in other words, on the next time the block is called.

Before describing the special function blocks for serial interfaces, it is important to know the *Data types*, it means, the data type used by the blocks.

Data type	Options	Description
SERIAL_BAUDRATE	BAUD2400	Lists all baud rate possibilities (bits per second)
	BAUD4800	
	BAUD9600	
	BAUD19200	
	BAUD38400	
	BAUD57600	
	BAUD115200	
SERIAL_DATABITS	DATABITS_7	Lists all data bits possibilities.
	DATABITS_8	
SERIAL_MODE	NORMAL_MODE	Serial Communication Normal Operation mode.
	EXTENDED_MODE	Serial Communication Extended Operation mode in which are provided information about the received data frame.
SERIAL_PARAMETERS	Defines all modem signal possibilities for the configurations:	
	BAUDRATE	Defined in SERIAL_BAUDRATE.
	DATABITS	Defined in SERIAL_DATABITS.
	STOPBITS	Defined in SERIAL_STOPBITS.
	PARITY	Defined in SERIAL_PARITY.
	UART_RX_THRESHOLD	Byte quantity which must be received to generate a new UART interruption. Lower values make the TIMESTAMP more precise when the EXTENDED MODE is used and minimizes the overrun errors. However, values too low may cause too many interruptions and delay the CPU.
	MODE	Defined in SERIAL_MODE.

Data type	Options	Description
	ENABLE_RX_ON_TX	When true, all the received byte during the transmission will be discharged instead going to the RX line. Used to disable the full-duplex operation in the RS-422 interface.
SERIAL_PARITY	PARITY_NONE	List all parity possibilities.
	PARITY_ODD	
	PARITY_EVEN	
SERIAL_PORT	COM 1	List all available serial ports (COM 10, COM 11, COM 12, COM 13, COM 14, COM 15, COM 16, COM 17, COM 18 and COM 19 – expansion modules).
SERIAL_RX_CHAR_ EXTENDED	Defines a character in the RX queue in extended mode.	
	RX_CHAR	Data byte.
	RX_ERROR	Error code.
	RX_TIMESTAMP	Silence due to the previous character or due to another event which has happen before this character (serial port configuration, transmission ending).
SERIAL_RX_QUEUE_ STATUS	It has some fields which deliver information regarding RX queue status/error, used when the normal format is utilized (no error and timestamp information):	
	RX_FRAMING_ERRORS	Frame errors counter: character incorrect formation – no stop bit, incorrect baud rate, among other – since the serial port configuration. Returns to zero when it reaches the maximum value (65535).
	RX_PARITY_ERRORS	Parity errors counter, since the serial port configuration. Returns to zero when it reaches the maximum value (65535).
	RX_BREAK_ERRORS	Interruption errors counter, since the serial port configuration, in other words, active line higher than the character time. Returns to zero when it reaches the maximum value (65535).
	RX_FIFO_OVERRUN_ ERRORS	FIFO RX overrun errors counter, since the serial port configuration, in other words, error in the FIFO RX configured threshold. Returns to zero when it reaches the maximum value (65535).
	RX_QUEUE_OVERRUN_ ERRORS	RX queue overrun errors counter, in other words, the maximum characters number (1024) was overflowed and the data are being overwritten. Returns to zero when it reaches the maximum value (65535).

Data type	Options	Description
	RX_ANY_ERRORS	Sum the last 5 error counters (frame, parity, interruption, RX FIFO overrun, RX queue overrun).
	RX_REMAINING	Number of characters in the RX queue.
SERIAL_STATUS	List of critic error codes that can be returned by the serial function block. Each block returns specific errors, which will be described below:	
	NO_ERROR	No errors.
	ILLEGAL_*	Return the parameters with invalid values or out of range: - SERIAL_PORT - SERIAL_MODE - BAUDRATE - DATA_BITS - PARITY - STOP_BITS - HANDSHAKE - UART_RX_THRESHOLD - TIMEOUT - TX_BUFF_LENGTH - HANDSHAKE_METHOD - RX_BUFF_LENGTH
	PORT_BUSY	Indicates the serial port is being used by another instance
	HW_ERROR_UART	Hardware error detected in the UART.
	HW_ERROR_REMOTE	Hardware error at communicating with the remote serial port.
	CTS_TIMEOUT_ON	Time-out while waiting for the CTS enabling, in the RS-232 RTS/CTS handshake, in the SERIAL_TX block.
	CTS_TIMEOUT_OFF	Time-out while waiting for the CTS disabling, in the RS-232 RTS/CTS handshake, in the SERIAL_TX block.
	TX_TIMEOUT_ERROR	Time-out while waiting for the transmission ending in the SERIAL_TX.
	RX_TIMEOUT_ERROR	Time-out while waiting for all characters in the SERIAL_RX block or the SERIAL_RX_EXTENDED block.
	FB_SET_CTRL_NOT_ALLOWED	The SET_CTRL block can't be used in case the handshake is different from RS232_MANUAL.
	FB_GET_CTRL_NOT_ALLOWED	The GET_CTRL block can't be used in case the handshake is different from RS232_MANUAL.
FB_SERIAL_RX_NOT_ALLOWED	The SERIAL_RX isn't available for the RX queue, extended mode.	

Data type	Options	Description
	FB_SERIAL_RX_EXTENDED_NOT_ALLOWED	The SERIAL_RX_EXTENDED isn't available for the RX queue, normal mode.
	DCD_INTERRUPT_NOT_ALLOWED	The interruption by the DCD signal can't be enabled in case the serial port doesn't have the respective pin.
	CTS_INTERRUPT_NOT_ALLOWED	The interruption by the CTS signal can't be enabled in case the handshake is different from RS232_MANUAL or in case the serial port doesn't have the respective pin.
	DSR_INTERRUPT_NOT_ALLOWED	The interruption by the DSR signal can't be enabled in case the serial port doesn't have the respective pin. (Nexto CPUs don't have this signal in integrated ports)
	NOT_CONFIGURED	The function block can't be used before the serial port configuration.
	INTERNAL_ERROR	Indicates that an internal problem has occurred in the serial port.
SERIAL_STOPBITS	STOPBITS_1	List all Stop Bits possibilities.
	STOPBITS_2	
	STOPBITS_1_5	

Table 166: Serial Function Blocks Data types

5.15.1.1. SERIAL_CFG

This function block is used to configure and initialize the desired serial port. After the block is called, every RX and TX queue associated to the serial ports and the RX and TX FIFO are restarted.



Figure 166: Serial Configuration Block

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.
PARAMETERS	SERIAL_PARAMETERS	This structure defines the serial port configuration parameters, as described in the SERIAL_PARAMETERS data type.

Table 167: SERIAL_CFG Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It is false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It is false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It is false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - ILLEGAL_SERIAL_MODE - ILLEGAL_BAUDRATE - ILLEGAL_DATA_BITS - ILLEGAL_PARITY - ILLEGAL_STOP_BITS - ILLEGAL_HANDSHAKE - ILLEGAL_UART_RX_THRESHOLD - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - DCD_INTERRUPT_NOT_ALLOWED - CTS_INTERRUPT_NOT_ALLOWED - DSR_INTERRUPT_NOT_ALLOWED

Table 168: SERIAL_CFG Output Parameters

Utilization example in ST language, after the library Nexto Serial is inserted in the project:

```

PROGRAM UserPrg
VAR
Config: SERIAL_CFG;
Port: SERIAL_PORT := COM1;
Parameters: SERIAL_PARAMETERS := (BAUDRATE := BAUD9600,
DATABITS := DATABITS_8,
STOPBITS := STOPBITS_1,
PARITY := PARITY_NONE,
HANDSHAKE := RS232_RTS,
UART_RX_THRESHOLD := 8,
MODE :=NORMAL_MODE,
ENABLE_RX_ON_TX := FALSE,
ENABLE_DCD_EVENT := FALSE,
ENABLE_CTS_EVENT := FALSE);
Status: SERIAL_STATUS;
END_VAR
//INPUTS:
Config.REQUEST := TRUE;
Config.PORT := Port;
    
```

```

Config.PARAMETERS := Parameters;
//FUNCTION:
Config();
//OUTPUTS:
Config.DONE;
Config.EXEC;
Config.ERROR;
Status := Config.STATUS;    //If it is necessary to treat the error.
    
```

5.15.1.2. SERIAL_GET_CFG

The function block is used to capture the desired serial port configuration.



Figure 167: Block to Capture the Serial Configuration

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.

Table 169: SERIAL_GET_CFG Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It is false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It is false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It is false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.

Output parameters	Type	Description
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - NOT_CONFIGURED
PARAMETERS	SERIAL_PARAMETERS	This structure receives the serial port configuration parameters, as described in the SERIAL_PARAMETERS data type.

Table 170: SERIAL_GET_CFG Output Parameters

Utilization example in ST language, after the library is inserted in the project:

```

PROGRAM UserPrg
VAR
GetConfig: SERIAL_GET_CFG;
Port: SERIAL_PORT := COM1;
Parameters: SERIAL_PARAMETERS;
Status: SERIAL_STATUS;
END_VAR
//INPUTS:
GetConfig.REQUEST := TRUE;
GetConfig.PORT := Port;
//FUNCTION:
GetConfig();
//OUTPUTS:
GetConfig.DONE;
GetConfig.EXEC;
GetConfig.ERROR;
Status := GetConfig.STATUS; //If it is necessary to treat the error.
Parameters := GetConfig.PARAMETERS; //Receive the parameters of desired serial
port.
    
```

5.15.1.3. SERIAL_GET_RX_QUEUE_STATUS

This block is used to read some status information regarding the RX queue, specially developed for the normal mode, but it can also be used in the extended mode.



Figure 168: Block Used to Visualize the RX Queue Status

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.

Table 171: SERIAL_GET_RX_QUEUE_STATUS Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It is false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It is false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It is false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - NOT_CONFIGURED
RXQ_STATUS	SERIAL_RX_QUEUE_STATUS	Returns the RX queue status/error, as described in the SERIAL_RX_QUEUE_STATUS data type.

Table 172: SERIAL_GET_RX_QUEUE_STATUS Output Parameters

Utilization example in ST language, after the library is inserted in the project and the serial port configured:

```

PROGRAM UserPrg
VAR
Get_Status: SERIAL_GET_RX_QUEUE_STATUS;
Port: SERIAL_PORT := COM1;
Status: SERIAL_STATUS;
Status_RX: SERIAL_RX_QUEUE_STATUS;
END_VAR
//INPUTS:
Get_Status.REQUEST := TRUE;
Get_Status.PORT := Port;
//FUNCTION:
Get_Status();
//OUTPUTS:
Get_Status.DONE;
Get_Status.EXEC;
Get_Status.ERROR;
Status := Get_Status.STATUS; //If it is necessary to treat the error.
Status_RX := Get_Status.RXQ_STATUS; //If it is necessary to treat the error of
the RX.
    
```

5.15.1.4. SERIAL_PURGE_RX_QUEUE

This function block is used to clean the serial port RX queue, local and remote. The UART RX FIFO is restarted too.

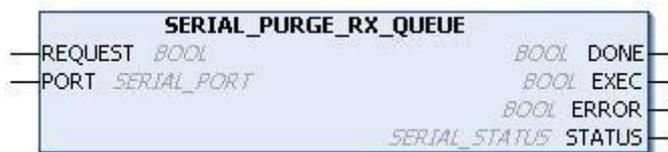


Figure 169: Block Used to Clean the RX Queue

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.

Table 173: SERIAL_PURGE_RX_QUEUE Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It's false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It's false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It's false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - NOT_CONFIGURED

Table 174: SERIAL_PURGE_RX_QUEUE Output Parameters

Utilization example in ST language, after the library is inserted in the project and the serial port configured:

```

PROGRAM UserPrg
VAR
Purge_Queue: SERIAL_PURGE_RX_QUEUE;
Port: SERIAL_PORT := COM1;
Status: SERIAL_STATUS;
END_VAR
//INPUTS:
Purge_Queue.REQUEST := TRUE;
Purge_Queue.PORT := Port;
//FUNCTION:
Purge_Queue();
//OUTPUTS:
Purge_Queue.DONE;
Purge_Queue.EXEC;
Purge_Queue.ERROR;
Status := Purge_Queue.STATUS; //If it is necessary to treat the error.

```

5.15.1.5. SERIAL_RX

This function block is used to receive a serial port buffer, using the RX queue normal mode. In this mode, each character in the RX queue occupy a single byte which has the received data, storing 5, 6, 7 or 8 bits, according to the serial interface configuration.



Figure 170: Block Used to Read the Reception Buffer Values

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.
RX_BUFFER_POINTER	POINTER TO BYTE	Pointer of a byte array to receive the buffer values.
RX_BUFFER_LENGTH	UINT	Specify the expected character number in the byte array. In case more than the expected bytes are available, only the expected quantity will be read from the byte array, the rest will be leaved in the RX queue (maximum size equal to 1024 characters).
RX_TIMEOUT	UINT	Specify the time-out to receive the expected character quantity. In case it is smaller than the necessary to receive the characters, the RX_TIMEOUT_ERROR output from the STATUS parameter will be indicated. When the specified value, in ms, is equal to zero, the function will return the data within the buffer.

Table 175: SERIAL_RX Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It is false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It is false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It is false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.

Output parameters	Type	Description
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - ILLEGAL_RX_BUFF_LENGTH - RX_TIMEOUT_ERROR - FB_SERIAL_RX_NOT_ALLOWED - NOT_CONFIGURED
RX_RECEIVED	UINT	Returns the received characters number. This number can be within zero and the configured value in RX_BUFFER_LENGTH. In case it is smaller, an error will be indicated by the function block.
RX_REMAINING	UINT	Returns the number of characters which are still in the RX queue after the function block execution.

Table 176: SERIAL_RX Output Parameters

Utilization example in ST language, after the library is inserted in the project and the serial port configured:

```

PROGRAM UserPrg
VAR
Receive: SERIAL_RX;
Port: SERIAL_PORT := COM1;
Buffer_Pointer: ARRAY [0..1023] OF BYTE; //Max size.
Status: SERIAL_STATUS;
END_VAR
//INPUTS:
Receive.REQUEST := TRUE;
Receive.PORT := Port;
Receive.RX_BUFFER_POINTER := ADR(Buffer_Pointer);
Receive.RX_BUFFER_LENGTH := 1024; //Max size.
Receive.RX_TIMEOUT := 10000;
//FUNCTION:
Receive();
//OUTPUTS:
Receive.DONE;
Receive.EXEC;
Receive.ERROR;
Status := Receive.STATUS; //If it is necessary to treat the error.
Receive.RX_RECEIVED;
Receive.RX_REMAINING;
    
```

5.15.1.6. SERIAL_RX_EXTENDED

This function block is used to receive a serial port buffer using the RX queue extended mode as shown in the [Serial Interfaces Configuration](#) section.



Figure 171: Block Used for Reception Buffer Reading

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.
RX_BUFFER_POINTER	POINTER TO SERIAL_RX_CHAR_EXTENDED	Pointer of a SERIAL_RX_CHAR_EXTENDED array to receive the buffer values.
RX_BUFFER_LENGTH	UINT	Specify the expected character number in the SERIAL_RX_CHAR_EXTENDED array. In case more than the expected bytes are available, only the expected quantity will be read from the byte array, the rest will be leaved in the RX queue (maximum size equal to 1024 characters).
RX_TIMEOUT	UINT	Specify the time-out to receive the expected character quantity. In case it is smaller than the necessary to receive the characters, the RX_TIMEOUT_ERROR output from the STATUS parameter will be indicated. When the specified value, in ms, is equal to zero, the function will return the data within the buffer.

Table 177: SERIAL_RX_EXTENDED Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It is false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It is false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It is false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.

Output parameters	Type	Description
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - ILLEGAL_RX_BUFF_LENGTH - RX_TIMEOUT_ERROR - FB_SERIAL_RX_EXTENDED_NOT_ALLOWED - NOT_CONFIGURED
RX_RECEIVED	UINT	Returns the received characters number. This number can be within zero and the configured value in RX_BUFFER_LENGTH. In case it is smaller, an error will be indicated by the function block.
RX_REMAINING	UINT	Returns the number of characters which are still in the RX queue after the function block execution.
RX_SILENCE	UINT	Returns the silence time in the RX queue, measured since the last received character is finished. The time unit is 10 μ s. This output parameter type is important to detect the silence time in protocols as MODBUS RTU. It might not be the silence time after the last received character by this function block, as it is only true if RX_REMAINING = 0.

Table 178: SERIAL_RX_EXTENDED Output Parameters

Utilization example in ST language, after the library is inserted in the project and the serial port configured:

```

PROGRAM UserPrg
VAR
Receive_Ex: SERIAL_RX_EXTENDED;
Port: SERIAL_PORT := COM1;
Buffer_Pointer: ARRAY [0..1023] OF SERIAL_RX_CHAR_EXTENDED;
Status: SERIAL_STATUS;
END_VAR
//INPUTS:
Receive_Ex.REQUEST := TRUE;
Receive_Ex.PORT := Port;
Receive_Ex.RX_BUFFER_POINTER := ADR(Buffer_Pointer);
Receive_Ex.RX_BUFFER_LENGTH := 1024; //Max size.
Receive_Ex.RX_TIMEOUT := 10000;
//FUNCTION:
Receive_Ex();
    
```

```
//OUTPUTS:
Receive_Ex.DONE;
Receive_Ex.EXEC;
Receive_Ex.ERROR;
Status := Receive_Ex.STATUS; //If it is necessary to treat the error.
Receive_Ex.RX_RECEIVED;
Receive_Ex.RX_REMAINING;
Receive_Ex.RX_SILENCE;
```

5.15.1.7. SERIAL_SET_CTRL

This block is used to write on the control signals (RTS and DTR), when they are available in the serial port. It can also set a busy condition for the transmission, through BREAK parameter and it can only be used if the modem signal is configured for RS232_MANUAL.

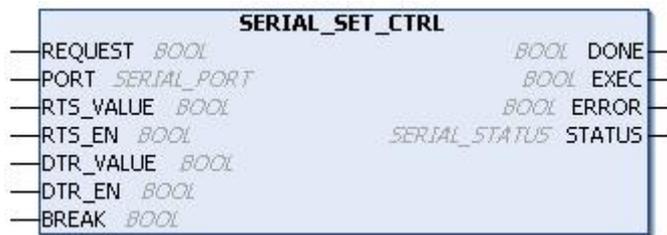


Figure 172: Block for Control Signals Writing

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.
RTS_VALUE	BOOL	Value to be written on RTS signal.
RTS_EN	BOOL	Enables the RTS_VALUE parameter writing.
DTR_VALUE	BOOL	Value to be written on DTR signal.
DTR_EN	BOOL	Enables the DTR_VALUE parameter writing.
BREAK	BOOL	In case it's true, enables logic 0 (busy) in the transmission line.

Table 179: SERIAL_SET_CTRL Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It is false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It is false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It is false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - FB_SET_CTRL_NOT_ALLOWED - NOT_CONFIGURED

Table 180: SERIAL_SET_CTRL Output Parameters

Utilization example in ST language, after the library is inserted in the project and the serial port configured:

```

PROGRAM UserPrg
VAR
Set_Control: SERIAL_SET_CTRL;
Port: SERIAL_PORT := COM1;
Status: SERIAL_STATUS;
END_VAR

//INPUTS:
Set_Control.REQUEST := TRUE;
Set_Control.PORT := Port;
Set_Control.RTS_VALUE := FALSE;
Set_Control.RTS_EN := FALSE;
Set_Control.DTR_VALUE := FALSE;
Set_Control.DTR_EN := FALSE;
Set_Control.BREAK := FALSE;
//FUNCTION:
Set_Control();
//OUTPUTS:
Set_Control.DONE;
Set_Control.EXEC;
Set_Control.ERROR;
Status := Set_Control.STATUS; //If it is necessary to treat the error.
    
```

5.15.1.8. SERIAL_TX

This function block is used to transmit a data buffer through serial port and it is only finalized after all bytes were transmitted or after time-out (generating errors).

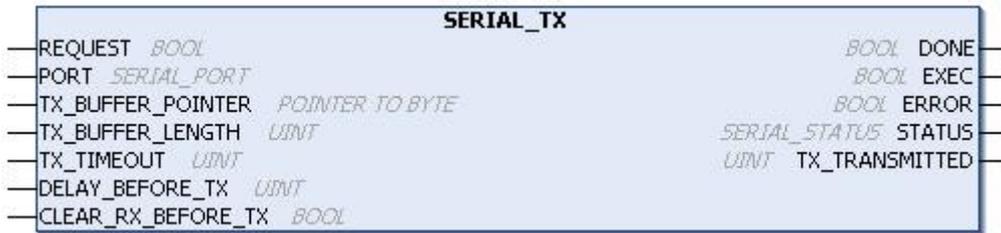


Figure 173: Block for Values Transmission by the Serial

Input parameters	Type	Description
REQUEST	BOOL	This variable, when true, enables the function block use.
PORT	SERIAL_PORT	Select the serial port, as described in the SERIAL_PORT data type.
TX_BUFFER_POINTER	POINTER TO BYTE	Pointer of a byte array to transmit the buffer values.
TX_BUFFER_LENGTH	UINT	Specify the expected character number in the byte array to be transmitted (TX queue maximum size is 1024 characters).
TX_TIMEOUT	UINT	Specify the time-out to complete the transmission including the handshake phase. The specified value, in ms, must be positive and different than zero.
DELAY_BEFORE_TX	UINT	Specify the delay, in ms, between the function block call and the transmission beginning. This variable can be used in communications with some modems.
CLEAR_RX_BEFORE_TX	BOOL	When true, the RX queue and the UART FIFO RX are erased before the transmission beginning. This behavior is typical in half-duplex master/slave protocols.

Table 181: SERIAL_TX Input Parameters

Output parameters	Type	Description
DONE	BOOL	This variable is true when the block is completely executed. It is false otherwise.
EXEC	BOOL	This variable is true while the block is being executed. It is false otherwise.
ERROR	BOOL	This variable is true when the block concludes the execution with an error. It is false otherwise. It is connected to the variable DONE, as its status is showed after the block conclusion.

Output parameters	Type	Description
STATUS	SERIAL_STATUS	In case the ERROR variable is true, the STATUS structure will show the error found during the block execution. The possible states, already described in the SERIAL_STATUS data type, are: - NO_ERROR - ILLEGAL_SERIAL_PORT - PORT_BUSY - HW_ERROR_UART - HW_ERROR_REMOTE - ILLEGAL_TX_BUFF_LENGTH - ILLEGAL_TIMEOUT - CTS_TIMEOUT_ON - CTS_TIMEOUT_OFF - TX_TIMEOUT_ERROR - NOT_CONFIGURED
TX_TRANSMITTED	UINT	Returns the transmitted byte number which must be equal to TX_BUFFER_LENGTH, but can be smaller in case some error has occurred during transmission.

Table 182: SERIAL_TX Output Parameters

Utilization example in ST language, after the library is inserted in the project and the serial port configured:

```

PROGRAM UserPrg
VAR
Transmit: SERIAL_TX;
Port: SERIAL_PORT := COM1;
Buffer_Pointer: ARRAY [0..9] OF BYTE := [0,1,2,3,4,5,6,7,8,9];
Status: SERIAL_STATUS;
END_VAR

//INPUTS:
Transmit.REQUEST := TRUE;
Transmit.PORT := Port;
Transmit.TX_BUFFER_POINTER := ADR(Buffer_Pointer);
Transmit.TX_BUFFER_LENGTH := 10;
Transmit.TX_TIMEOUT := 10000;
Transmit.DELAY_BEFORE_TX := 1000;
Transmit.CLEAR_RX_BEFORE_TX := TRUE;
//FUNCTION:
Transmit();
//OUTPUTS:
Transmit.DONE;
Transmit.EXEC;
Transmit.ERROR;
Status := Transmit.STATUS; //If it is necessary to treat the error.
Transmit.TX_TRANSMITTED;
    
```

5.15.2. Inputs and Outputs Update

By default, the local bus and CPU integrated I/O are updated on every execution cycle of MainTask. The Refresh functions allows to update these I/O points asynchronously at any point of user application code.

When the function blocks to update the inputs and outputs are not used, the update is performed every cycle of the Main-Task.

ATTENTION

At the startup of a CPU of this series, the inputs and outputs are only updated for reading and prepared for writing when the MainTask is performed.
All other system tasks that run before MainTask will be with the inputs and outputs invalid.

5.15.2.1. REFRESH_INPUT

This function block is used to update the specified module inputs without the necessity to wait for the cycle to be completed. It is important to notice that the filters configured in the MasterTool IEC XE and the update time of the module inputs will have to be considered in effective time of the inputs update in the application developed by the user.

ATTENTION

The *REFRESH_INPUT* function must only be used in MainTask.

ATTENTION

REFRESH_INPUT function does not support inputs that have been mapped to symbolic variables. For proper operation it is necessary that the input is mapped to a variable within the memory direct representation of input variables (%I).

ATTENTION

The *REFRESH_INPUT* function updates only the direct variables %I that are declared in the "Bus: I/O Mapping" tab of the module addressed in the respective rack/slot of the function. In the case of communication modules/interfaces (MODBUS, Profibus, etc.), the update does not include the direct variables of the device mappings.

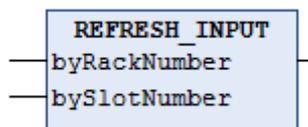


Figure 174: Block for Input Updating

Input parameters	Type	Description
byRackNumber	BYTE	Rack number.
bySlotNumber	BYTE	Position number where the module is connected.

Table 183: REFRESH_INPUT Input Parameters

Possible *TYPE_RESULT*:

- **OK_SUCCESS:** Execution success.
- **ERROR_FAILED:** This error is returned if the function is called for a module that has only outputs, or also if the option *Always update variables* (located in the module's configuration screen, tab *I/O Mapping*) is not checked.

- **ERROR_NOTSUPPORTED:** The called routine is not supported by the product.
- **ERROR_PARAMETER:** Invalid / unsupported parameter.
- **ERROR_MODULE_ABSENT:** The module is absent in the bus.
- **ERROR_MODULE_NOTCONFIGURED:** The module is not configured in the application.
- **ERROR_MODULE_NOTRUNNING:** The module is not running (is not in operational state).
- **ERROR_MODULE_COMMFAIL:** Failure in the communication with the module.
- **ERROR_MODULE_NOTFOUND:** The module was not found in the application or is not supported.

Utilization example in ST language:

```
PROGRAM UserPrg
VAR
Info: TYPE_RESULT;
byRackNumber: BYTE;
bySlotNumber: BYTE;
END_VAR
//INPUTS:
byRackNumber := 0;
bySlotNumber := 10;
//FUNCTION:
Info := REFRESH_INPUT (byRackNumber, bySlotNumber); //Function call.
//Variable "Info" receives possible function errors.
```

5.15.2.2. REFRESH_OUTPUT

This function block is used to update the specified module outputs. It is not necessary to wait until the cycle is finished. It is important to notice that the update time of the module outputs will have to be considered in the effective time of the outputs update in the application developed by the user.

ATTENTION

The *REFRESH_OUTPUT* function must only be used in MainTask.

ATTENTION

REFRESH_OUTPUT function does not support inputs that have been mapped to symbolic variables. For proper operation it is necessary that the input is mapped to a variable within the memory direct representation of input variables (%Q).

ATTENTION

The *REFRESH_OUTPUT* function updates only the direct variables %Q that are declared in the "Bus: I/O Mapping" tab of the module addressed in the respective rack/slot of the function. In the case of communication modules/interfaces (MODBUS, Profibus, etc.), the update does not include the direct variables of the device mappings.

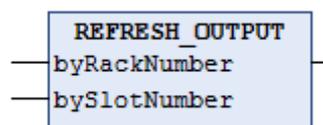


Figure 175: Block for Output Updating

Input parameters	Type	Description
byRackNumber	BYTE	Rack number.
bySlotNumber	BYTE	Position number where the module is connected.

Table 184: REFRESH_OUTPUT Input Parameters

Possible *TYPE_RESULT*:

- **OK_SUCCESS:** Execution success.
- **ERROR_FAILED:** This error is returned if the function is called for a module that has only inputs, or also if the option *Always update variables* (located in the module's configuration screen, tab *I/O Mapping*) is not checked.
- **ERROR_NOTSUPPORTED:** The called routine is not supported by the product.
- **ERROR_PARAMETER:** Invalid / unsupported parameter.
- **ERROR_MODULE_ABSENT:** The module is absent in the bus.
- **ERROR_MODULE_NOTCONFIGURED:** The module is not configured in the application.
- **ERROR_MODULE_NOTRUNNING:** The module is not running (is not in operational state).
- **ERROR_MODULE_COMMFAIL:** Failure in the communication with the module.
- **ERROR_MODULE_NOTFOUND:** The module was not found in the application or is not supported.

Utilization example in ST language:

```
PROGRAM UserPrg
VAR
Info: TYPE_RESULT;
byRackNumber: BYTE;
bySlotNumber: BYTE;
END_VAR
//INPUTS:
byRackNumber := 0;
bySlotNumber := 10;
//FUNCTION:
//Function call.
Info := REFRESH_OUTPUT (byRackNumber, bySlotNumber);
//Variable "Info" receives possible function errors.
```

5.15.3. PID Function Block

ATTENTION

The PID function block described up to previous revision L of this manual became obsolete and was removed from this manual.

The PID, PID_INT and PID_REAL function blocks described up to revision C of MP399609, also became obsolete and were also removed from newer versions of that manual. Users that need description of these obsolete function blocks due to maintenance reasons must use revision C of MP399609.

Function blocks PID, PID_INT and PID_REAL must not be used in new projects. These function blocks were replaced by newer function blocks with additional resources, like auto-tuning and support to cascade, override and feed-forward controls. These new function blocks are described in MU214610, and are available after version 1.1.0.0 of library *Nex-toPID*.

5.15.4. Timer Retain

The timer retain is a function block developed for applications as production line clocks, that need to store its value and restart the counting from the same point in case of power supply failure. The values stored by the function block, are only zero in case of a *Reset Cold*, *Reset Origin* or a new application *Download* (see the MasterTool IEC XE User Manual - MU299609), when the counters keep working, even when the application is stopped (Stop Mode).

ATTENTION

It is important to stress that, for the correct functioning of the Timer Retain blocks, the variables must be declared as Retain (*VAR RETAIN*). It's also important to notice that in simulation mode, the Timer Retain function blocks do not run properly due to need the Nexto CPU for correct behavior.

The three blocks already available in the MasterTool IEC XE software *NextoStandard* library are described below (for the library insertion proceeding, see MasterTool IEC XE Programming Manual – MP399609, section Library).

5.15.4.1. TOF_RET

The function block *TOF_RET* implements a time delay to disable an output. When the input *IN* has its state changed from (TRUE) to (FALSE), or a falling edge, the specified time *PT* will be counted and the *Q* output will be driven to (FALSE) at the end of it. When the input *IN* is in logic level 1 (TRUE), the output *Q* remain in the same state (TRUE), even if this happened in the middle of the counting process. The *PT* time can be changed during the counting as the block assumes the new value if the counting hasn't finished. Figure 176 depicts the *TOF_RET* block and Figure 177 shows its graphic behavior.



Figure 176: TOF_RET Block

Input parameters	Type	Description
IN	BOOL	This variable, when receives a falling edge, enables the block counting.
PT	TIME	This variable specifies the block counting limit (time delay).

Table 185: TOF_RET Input Parameters

Output parameters	Type	Description
Q	BOOL	This variable executes a falling edge as the PT variable (time delay) reaches its maximum value.
ET	TIME	This variable shows the current time delay.

Table 186: TOF_RET Output Parameters

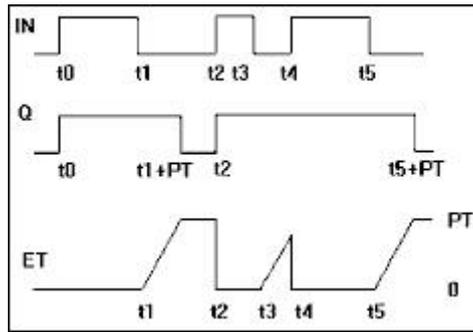


Figure 177: TOF_RET Block Graphic Behavior

Utilization example in ST language:

```
PROGRAM UserPrg
VAR RETAIN
bStart : BOOL := TRUE;
TOF_RET : TOF_RET;
END_VAR

// When bStart=FALSE starts counting
TOF_RET( IN := bStart,
PT := T#20S);

// Actions executed at the end of the counting
IF (TOF_RET.Q = FALSE) THEN
bStart := TRUE;
END_IF
```

5.15.4.2. TON_RET

The *TON_RET* implements a time delay to enable an output. When the input *IN* has its state changed from (FALSE) to (TRUE), or a rising edge, the specified time *PT* will be counted and the *Q* output will be driven to (TRUE) at the end of it. When the input *IN* is in logic level 0 (FALSE), the output *Q* remain in the same state (FALSE), even if it happens in the middle of the counting process. The *PT* time can be changed during the counting as the block assumes the new value if the counting hasn't finished. Figure 178 depicts the *TON_RET* block and Figure 179 shows its graphic behavior.



Figure 178: TON_RET Function Block

Input parameters	Type	Description
IN	BOOL	This variable, when receives a rising edge, enables the function block counting.
PT	TIME	This variable specifies the block counting limit (time delay).

Table 187: TON_RET Input Parameters

Output parameters	Type	Description
Q	BOOL	This variable executes a rising edge as the PT variable (time delay) reaches its maximum value.
ET	TIME	This variable shows the current time delay.

Table 188: TON_RET Output Parameters

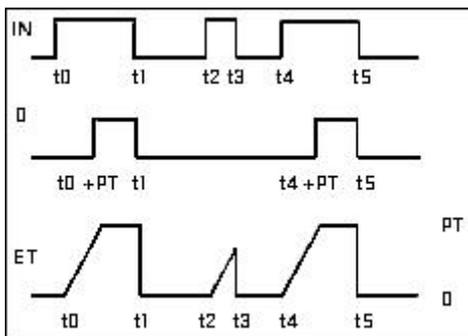


Figure 179: TON_RET Block Graphic Behavior

Utilization example in ST language:

```

PROGRAM UserPrg
VAR RETAIN
bStart : BOOL;
TON_RET : TON_RET;
END_VAR

// Quando bStart=TRUE starts counting
TON_RET( IN := bStart,
PT := T#20S);

// Actions executed at the end of the counting
IF (TON_RET.Q = TRUE) THEN
bStart := FALSE;
END_IF
    
```

5.15.4.3. TP_RET

The *TP_RET* function block works as a trigger. The timer which starts when the *IN* input has its state changed from (FALSE) to (TRUE), that is, a rising edge, it is increased until the *PT* time limit is reached. During the counting, the *Q* output is (TRUE), otherwise it is (FALSE). The *PT* time can be changed during the counting as the block assumes the new value if the counting has not finished. Figure 180 depicts the *TP_RET* and Figure 181 shows its graphic behavior.

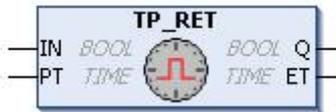


Figure 180: TP_RET Function Block

Input parameters	Type	Description
IN	BOOL	This variable, when receives a rising edge, enables the function block counting.
PT	TIME	This variable specifies the function block counting limit (time delay).

Table 189: TP_RET Input Parameters

Output parameters	Type	Description
Q	BOOL	This variable is true during the counting, otherwise is false.
ET	TIME	This variable shows the current time delay.

Table 190: TP_RET Output Parameters

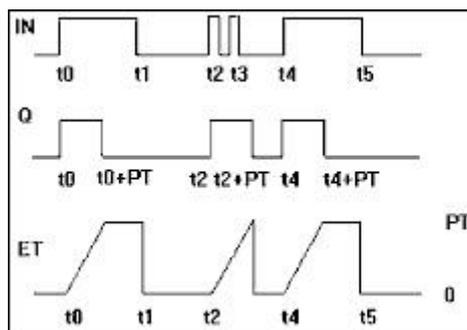


Figure 181: TP_RET Block Graphic Behavior

Utilization example in ST language:

```
PROGRAM UserPrg
VAR RETAIN
bStart : BOOL;
TP_RET : TP_RET;
END_VAR

// Configure TP_RET
```

```

TP_RET( IN := bStart,
PT := T#20S);

bStart := FALSE;

// Actions executed during the counting
IF (TP_RET.Q = TRUE) THEN
// Executes while the counter is activated
ELSE
// Executes when the counter is deactivated
END_IF

```

5.15.5. User Log

Feature that allows the user to create own records and write to log files on the memory card present in the CPU. The files are generated in a specific directory of the memory card in the CSV format, allowing viewing in text editors and spreadsheets. The separator was the semicolon character. For more information about the use of the memory card, see section [Memory Card](#).

There are two functions available, one for log information and another to remove all records. The following is a description of the types of data used by the functions:

Data type	Option	Description
USER_LOG_EVENT_TYPES	USER_LOG_EVENT_ERROR	The user is free to use the best indication according to log message severity.
	USER_LOG_EVENT_DEBUG	
	USER_LOG_EVENT_INFO	
	USER_LOG_EVENT_WARN	
USER_LOG_MESSAGE		Log message with 150-character max.
USER_LOG_ERROR_CODES	USER_LOG_OK	The operation was performed successfully.
	USER_LOG_FAILED	The operation was not performed successfully. The reason for the failure can be checked in the system logs – see section System Log .
	USER_LOG_BUFFER_FULL	Messages are being added beyond the processing capacity.
	USER_LOG_NO_MEMORY	At the time, there were no resources to perform the operation.
	USER_LOG_FILE_SYSTEM_ERROR	There was an error while accessing the memory card or there is no available space. Error information can be verified in the logs of system – see section System Log .
	USER_LOG_NO_MEMORY_CARD	There is a memory card present in the CPU.
	USER_LOG_MEMORY_CARD_FULL	There is no free space available on the memory card.
	USER_LOG_PROCESSING	The resource is busy executing the last operation, for example, deleting all log files.

Table 191: Data Type for User Log

The following are described the two functions available in the *LibLogs* library on MasterTool IEC XE. To perform the procedure of inserting a library, see the MasterTool IEC Programming Manual – MP399609, section Libraries.

ATTENTION

The User Logs are available only until version 1.3.0.20 of Nexto Series CPUs. In the same way to use this feature is necessary version 1.40 or higher of MasterTool IEC XE.

5.15.5.1. UserLogAdd

This function is used to add a new user log message, adding in a new line to the log file on the memory card. The message must have a maximum length of 150 characters, and the event type of the message. Application variables can be registered using conversion to string and concatenation with the main message. The date and time information in UTC (timestamp) is automatically added in the message with a resolution of milliseconds where the event was registered. The date and time information is also used in the formation of the names of the log files.

The *UserLogAdd* function can be used to enter multiple messages within a single task and also in different application tasks. However independent of each execution of the function in the application, being on the same task or on different tasks, all use the same feature to record the desired messages. For this reason it is recommended that the addition of messages using the *UserLogAdd* function in the application be held every 50 ms to prevent the return of buffer overload. If the function is performed in periods shorter than the indicated, but respect the average time of 50 ms between each message addition at the end of the interval for the task, also prevents the return of buffer overload. So that the logs are added correctly, it is important to respect time limits when the card is inserted and at startup of the CPU, mentioned in section [Memory Card](#). After the operation the function returns the options for the given type *USER_LOG_ERROR_CODES* as Table 191. When the function return is not *USER_LOG_OK*, the message was not registered and the function *UserLogAdd* should be re-executed with the desired message. In case of return of consecutive writing failures, the memory card can be damaged. The replacement by a healthy memory card ensures that the latest logged messages will be recorded on the card that is not damaged, since the CPU is not restarted.

The figure below represents the function *UserLogAdd* and table below the input parameters:

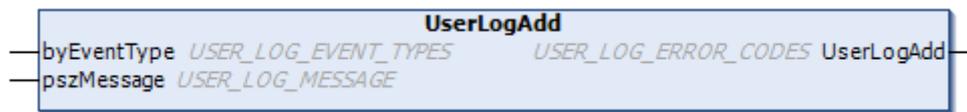


Figure 182: UserLogAdd Function

Input Parameters	Type	Description
byEventType	BYTE	This variable specifies the event type of the log being added as options for the <i>USER_LOG_EVENT_TYPES</i> data type.
pszMessage	USER_LOG_MESSAGE	This variable should contain the set of characters that compose the message to be added to the log file. The message must contain a maximum of 150 characters.

Table 192: UserLogAdd Input Parameters

The log files are generated and organized on the memory card in a specific directory path depending on the CPU serial number and the firmware version installed. For example, for a CPU with serial number 445627 and firmware version 1.4.0.4, the location where the log files should be written to the memory card is *MemoryCard/UserLog/445627/1.4.0.4/*.

The names of the log files are formed by the date and time (timestamp) of the first message. Except when there’s a problem to use this name, for example, another existing file with the same name, in this situation it is used the instant date and time. The file name follows the following pattern: *year/month/day/hour/minute/second/millisecond.CSV*. In case of file access problem due to defective sector not enabling to continue writing, will be added to the name of this file the extension “*corrupted*” and a new file will be created. The amount of logs per file is not fixed, varying depending on the size of messages. The amount of created files is limited to 1024 with maximum size of 1 MB each, so the memory card requires 1 GB of free space. When it

reaches the limit of 1024 files created on the memory card, during CPU operation, the oldest files are removed so that files with latest logs are preserved, even in cases of partial manual removal of the files in the directory where the files are being written.

The viewing of the log files can be performed through worksheets or conventional text editors. The concatenated information, for improved visualization, may use semicolons between the strings of the message to separate them. One must be careful in formatting cells with floating point values.

Utilization example in ST language:

```
PROGRAM UserPrg
VAR
  eLogError : USER_LOG_ERROR_CODES;
  sMessage : USER_LOG_MESSAGE;
END_VAR

IF (m_rTemperature > MAX_TEMPERATURE_ACCEPT) THEN
  sMessage := 'Temperature higher than expected: ';
  sMessage := concat(sMessage, REAL_TO_STRING(m_rTemperature));
  sMessage := concat(sMessage, '°');
  eLogError := UserLogAdd(USER_LOG_EVENT_WARN, sMessage);
  //eLogError variable gets possible function errors.
END_IF
```

Log file content example: (*UserLog-201308271506245738.csv*)

```
Model; NX3008
Serial number; 445627
Firmware version; 1.4.0.4

27/08/2013 15:06:24.5738; WARN; Overtemperature: 25°
27/08/2013 16:37:45.3476; WARN; Overtemperature: 25°
28/08/2013 09:10:55.4201; WARN; Overtemperature: 26°
```

5.15.5.2. UserLogDeleteAll

The *UserLogDeleteAll* function performs the deletion of log files present in the directory created specifically for the CPU in which is inserted the memory card, i.e. are only deleted the logs contained in the directory named with the CPU firmware version that exists within the directory with the CPU serial version. The log files deleted are only files that exist at the time of memory card mounting and the generated by the *UserLogAdd* function. Logs of other CPUs and files added manually by the user during execution are not deleted. The figure below represents the function *UserLogDeleteAll*.

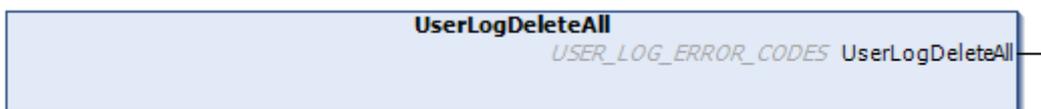


Figure 183: UserLogDeleteAll Function

Utilization example in ST language:

```

PROGRAM UserPrg
VAR
eLogError : USER_LOG_ERROR_CODES;
END_VAR

IF (m_DeleteLogs = TRUE) THEN
eLogError := UserLogDeleteAll();
m_DeleteLogs := FALSE;
//eLogError variable gets possibles function errors.
END_IF
    
```

ATTENTION

The *UserLogDeleteAll* function's return does not indicate operation completed, just confirmation of execution that can take a large amount of time if there are hundreds of log files in the directory. The function to record the new user log is unavailable right now, returning the *USER_LOG_PROCESSING* option for any operation. The result of the operation can also be checked in the system log.

5.15.6. ClearRtuDiagnostic

This function isn't supported by this CPUs' Series.

5.15.7. ClearEventQueue

The *ClearEventQueue* function available by the *LibRtuStandard* library can be used when it's needed to clear the CPU's event queue and of all instanced drivers.

According to table below the function's execution result is going to be showed in its output variable.

Name	ENUM (UDINT)	Result Description
OK_SUCCESS	0	Success
ERROR_FAILED	1	General error
ERROR_NOTSUPPORTED	2	The called routine is not supported by the product
ERROR_PARAMETER	3	Invalid/unsupported parameter
ERROR_MODULE_ABSENT	16	The module is absent in the bus
ERROR_MODULE_NOTCONFIGURED	17	The module is not configured in the application
ERROR_MODULE_NOTRUNNING	18	The module is not running (isn't in operational state)
ERROR_MODULE_COMMFAIL	19	Failure in the communication with the module
ERROR_MODULE_NOTFOUND	20	The module wasn't found in application or is not supported

Table 193: ClearEventQueue Function Results

Using example in ST language, where the function call is going to clear the events queue, and consequently, reset the communication drivers events queue usage diagnostics *T_DIAG_DNP_SERVER_1.tClient_*.tQueueDiags.wUsage*:

```

PROGRAM UserPrg
VAR
    ClearEventQueueStatus : TYPE_RESULT;
END_VAR

ClearEventQueueStatus := ClearEventQueue();
    
```

5.16. User Web Pages

Also called *Web Visualization*, or simply *Webvisu*, this feature allows to implement a simplified SCADA embedded into the PLC. The Visualization screens are developed on the same environment of the PLC application using MasterTool IEC XE. Once the application is downloaded, the PLC starts a web server hosting this special web page.

The complete information about this functionality can be found on Help of MasterTool IEC XE.

5.17. SNMP

SNMP (*Simple Network Management Protocol*) is a protocol widely used by network administrators to provide important information and diagnostic equipment present in a given Ethernet network.

This protocol uses the concept of agent and manager, in which the manager sends read requests or write certain objects to the agent. Through a MIB (*Management Information Base*) the manager is aware of existing objects in the agent, and thus can make requests of these objects, respecting the read permissions or writing the same. MIB is a collection of information organized hierarchically with each object of this tree is called *OID (Object Identifier)*.

For all equipment with SNMP, it is mandatory to support MIB-II. In this MIB are described key information for managing Ethernet networks.

5.17.1. SNMP on Nexto CPUs

The CPUs of the Nexto Series behave as agents in SNMP communication. The information made available through SNMP cannot be manipulated or accessed through the user application, requiring an external SNMP manager to perform access. The table below contains the objects available in the Nexto CPUs. The supported protocol versions are: SNMPv1, SNMPv2c and SNMPv3 (MIB-II supported objects are described in RFC-1213).

OID	Name	Description
1.3.6.1.2.1.1	System	Contains name, description, location and other equipment identification information.
1.3.6.1.2.1.2	Interfaces	Contains information of the machine's network interfaces. The ifTable (OID 1.3.6.1.2.1.2.2) has the indexes 8, 7 and 6 available, which can be viewed by the network interfaces statistics NET 1, NET 2 and NET 3, respectively, of the NX3008.
1.3.6.1.2.1.3	At	Contains information of the last required connections to the agent.
1.3.6.1.2.1.4	IP	Contains statistical connections using IP protocol.
1.3.6.1.2.1.5	ICMP	Contains statistical connections using ICMP protocol.
1.3.6.1.2.1.6	TCP	Contains statistical connections using TCP protocol.
1.3.6.1.2.1.7	UDP	Contains statistical connections using UDP protocol.
1.3.6.1.2.1.11	SNMP	Contains statistical connections using SNMP protocol.

Table 194: MIB II Objects – Nexto Series SNMP Agent

By default, the SNMP agent is activated, i.e., the service is initialized at the time the CPU is started. The access to the agent information is via the Ethernet interfaces of the Nexto Series CPUs on UDP port 161. So when the service is active, the agent information can be accessed through any one of the Ethernet interfaces available. It is only possible to provide agent information through CPU's Ethernet interfaces. In figure below, an example is shown where a SNMP manager presents some read values.

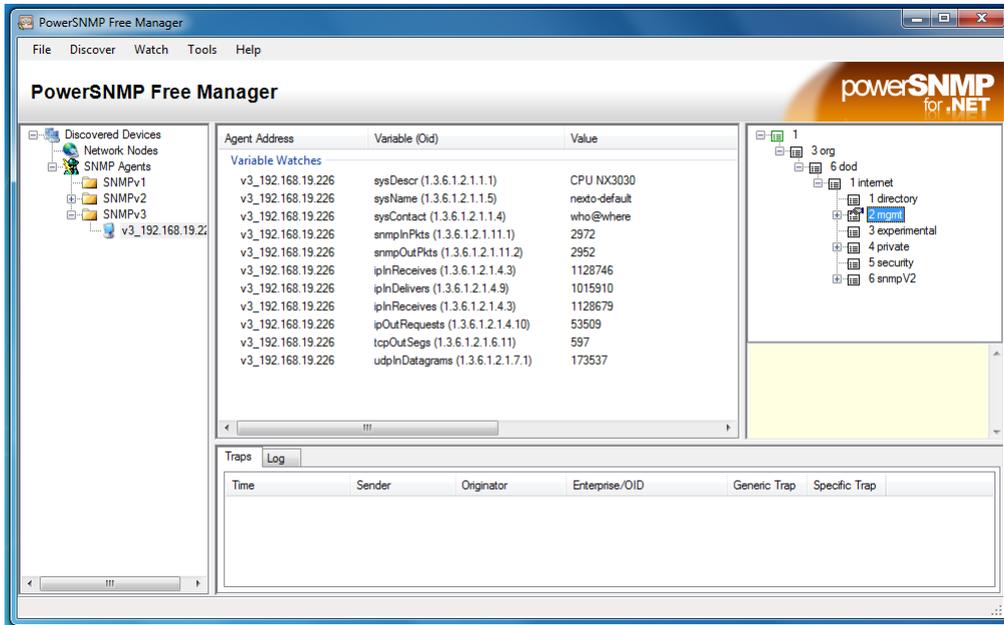


Figure 184: SNMP Manager Example

For SNMPv3, in which there is user authentication and password to requests via SNMP protocol, is provided a standard user described in the [User and SNMP Communities](#) section.

If you want to disable the service, change the SNMPv3 user or communities for SNMPv1 / v2c predefined, you must access the System Web Page of the CPU. For details, see the [SNMP Configuration](#) section.

5.17.2. SNMP Configuration

SNMP settings can be changed through the System Web Page, in the *CPU Management* tab, under the *SNMP* menu. After successful login, the current state of the service (enabled or disabled) as well as the user information SNMPv3 and communities for SNMPv1 / v2c can be viewed.

The user can enable or disable the service via a checkbox at the top of the screen.

It's also possible to change the SNMPv3 information by clicking the *Change* button just below the user information. This action will open a form where the user must fill the old username and old password, also the new username and the new password. Any other information can not be changed.

To change the information from the SNMPv1/v2c *Communities* group data, the process is similar, just click the *Change* button below the group information. In opened screen, new data can be filled in the *rocommunity* and *rwcommunity* fields. If any field is left blank, its correspondent *community* will be disabled. If both fields are left blank, the access to the SNMP agent will only be possible through SNMPv3.

If the user wants to return to the default settings, it must be manually reconfigured according to the available information in the [User and SNMP Communities](#) section. Therefore, all current SNMP configurations will be kept in the firmware update process. These options are shown in figure below.

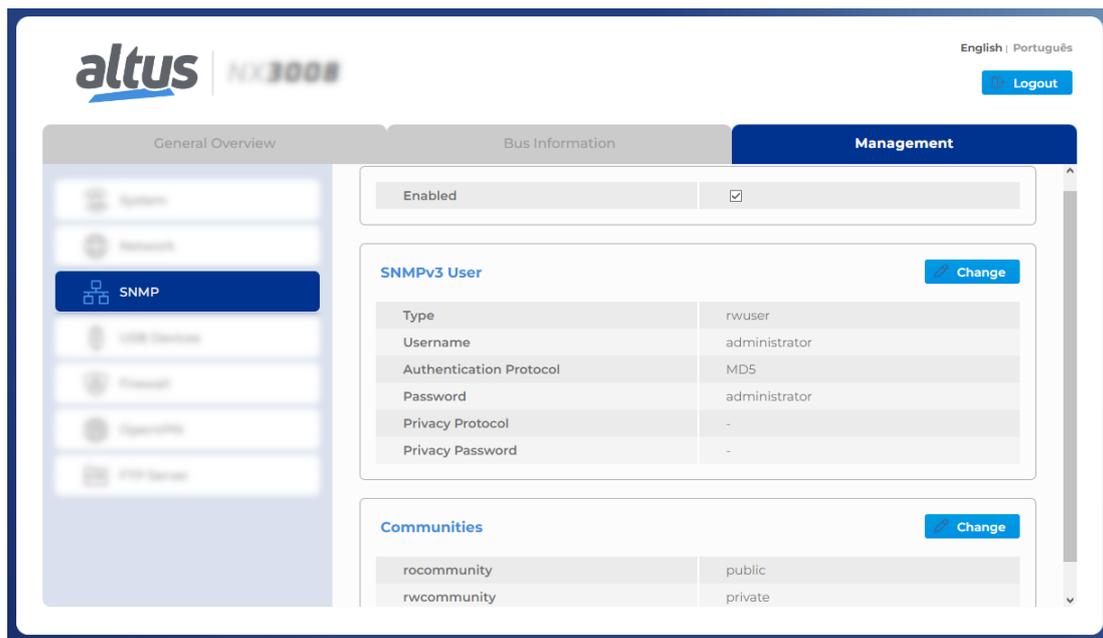


Figure 185: SNMP status configuration screen

5.17.3. User and SNMP Communities

Prior to access the SNMPv1 / v2c protocol informations, there are two *communities* settings to be configured, according to table below.

Communities	Default String	Type
rocommunity	Public	Only read
rwcommunity	Private	Read and Write

Table 195: SNMPv1/v2c Default Communities info

It's possible to access SNMPv3 using default user, see table below:

Username	Type	Authentication Protocol	Password	Privacy Protocol	Privacy Password
administrator	rwuser	MD5	administrator	-	-

Table 196: SNMPv3 Default User info

For *communities* settings, user and password, some limits must be respected, as described on the following table:

Configurable item	Minimum Size	Max Size	Allowed Characters
rocommunity	-	30	[0-9][a-z][A-Z]@\$*_
rwcommunity	-	30	[0-9][a-z][A-Z]@\$*_
V3 User	1	30	[0-9][a-z][A-Z]@\$*_
V3 Password	8	30	[0-9][a-z][A-Z]@\$*_

Table 197: SNMP settings limits

5.18. FTP Server

FTP (File Transfer Protocol) is a protocol that allows files to be transferred between devices. It operates in the client-server mode, where the CPU becomes a FTP Server, storing files that FTP Clients can access for transfer, download, and upload.

The controlling FTP connection is a TCP connection established through port 21 of the FTP Server. Through port 21, the Client and Server exchange commands and responses to manage the file transfer session.

Through the FTP protocol, the FTP Client can read and write files that are stored either in the internal memory of the CPU or in external memory (memory card, for example) if present in the architecture. The maximum file size that can be transferred varies according to the amount of memory available between internal and external memory. When the memory limit is reached, the transfer will stop, and if the file has not been transferred completely, it will become a corrupted file.

ATTENTION

Downloading and uploading large files through FTP, both from internal and external memory, can affect the performance of the CPU considerably.

ATTENTION

The FTP server does not support communication through Windows File Explorer, so an FTP Client software is required to access it.

5.18.1. Configuration

The FTP configuration is done through a dedicated section located in the *Management* tab of the controller's System Web Page, as shown below:

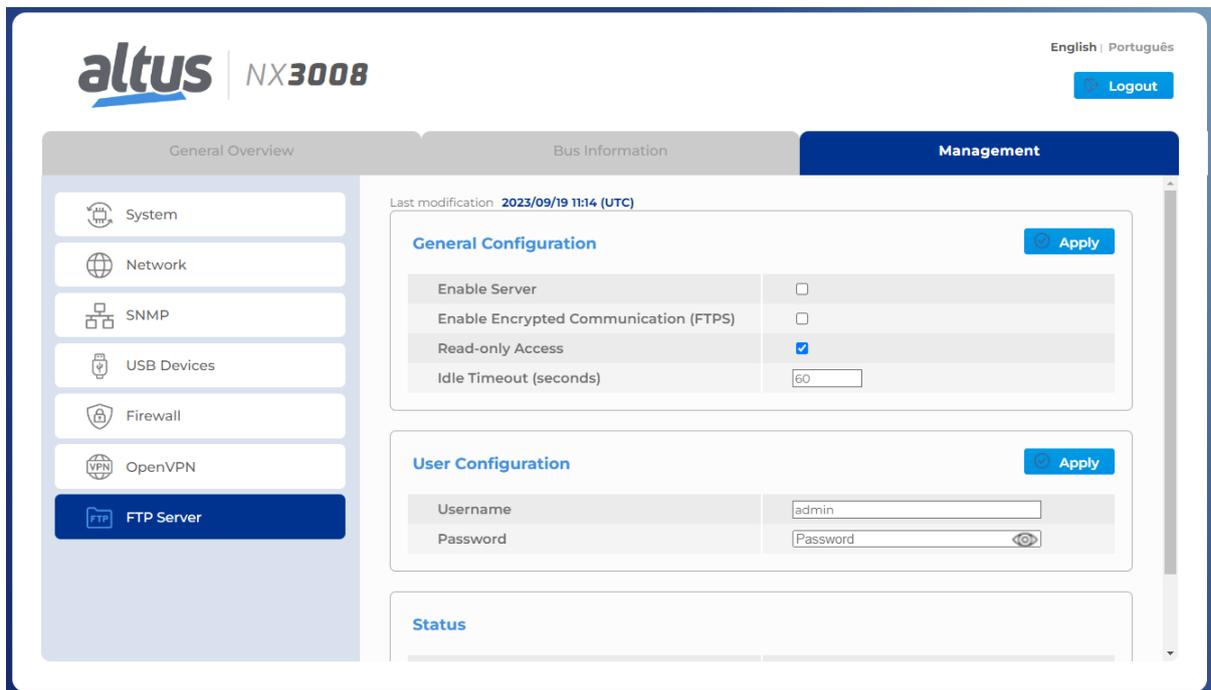


Figure 186: FTP Server Configuration Screen

FTP is a separate feature from MasterTool IEC XE, meaning it does not require any interaction with the programming tool. The settings applied on the *FTP Server* section take effect when confirmed through the *Apply* button and are automatically saved in the controller. As long as the functionality is enabled, it will resume operation even after the device is restarted.

ATTENTION

For the correct work of the FTP, the Clients must be configured in Active mode. Passive mode has been disabled for the NX3008.

5.18.1.1. General Configuration

5.18.1.1.1. Enable Server

Allows to activate or deactivate the functionality. When the FTP server is enabled, the settings made through the System Web Page are applied to the configuration files. That means the server is available according to the configuration made. If FTP is disabled, the configuration is still stored, but the service cannot be used.

5.18.1.1.2. Enable Encrypted Communication (FTPS)

Enables and disables encrypted communication. This communication is done through Explicit FTPS, also known as FTPES. This is a secure extension of the FTP protocol, which adds a layer of encryption to the transfer.

In this type of communication, when a client-server connection is established, instead of immediately starting the data transfer, the FTP Client sends an AUTH SSL command to request a secure connection. Then, when enabling encrypted communication, the UCP generates a self-signed certificate to guarantee communication using the SSL (Secure Sockets Layer) protocol.

When the FTP Client performs the authenticated connection, the certificate and its respective information will be displayed, allowing Explicit FTPS communication (FTP over SSL) to be established through port 21.

ATTENTION

The FTPES certificate is valid for one year from the date it was created. To generate a new certificate, simply reapply the configuration.

5.18.1.1.3. Read-only Access

Enables and disables limiting write and read access to the Server. By default, the parameter is enabled.

When the parameter is enabled, the FTP Client has read-only access without the possibility to add or remove any files from the FTP Server. In this case, the only operation allowed is uploading files, that is, transferring them from the Server to the Client. When the parameter is disabled, all operations can be performed.

5.18.1.1.4. Idle Timeout (Seconds)

Sets the maximum time the connection will be maintained before the FTP Server closes it due to inactivity. In other words, once the connection to a FTP Client is opened, if there is no activity after the Idle Timeout, the connection to the Client is closed by the Server.

The parameter can be configured with values between 10 to 60 seconds, the default being 60 seconds.

5.18.1.2. User Configuration

5.18.1.2.1. Username

User or *Username* required for the Client to connect to the Server.

If a new configuration is made, the previous one is removed. In other words, there is only one FTP user, but this one can be used for multiple connections.

5.18.1.2.2. Password

Manages the authentication key so the FTP Client can connect to the FTP Server.

There is no password recovery so, if the password has been lost, it is necessary to add a new user configuration.

Configurable Item	Minimum Size	Maximum Size	Allowed Characters	Default
Username	4	30	[a-z][A-Z][0-9]@\$*_	admin
Password	4	30	[a-z][A-Z][0-9]@\$*_	admin

Table 198: FTP User Settings

5.18.1.3. Status

5.18.1.3.1. Current State

Displays the current status of the FTP Server. The possible states are "Running", "Not Running", and "Restarting Service". Each configuration applied will restart the service.

5.18.1.3.2. Connected Clients

Shows the user the current number of active connections.

The FTP Server accepts a maximum of two active connections simultaneously. Some FTP Clients, such as *Filezilla*, use a feature called Multithread File Transfer to improve the efficiency and speed of the transfer. This feature allows the FTP Client to open more than one connection for the transfer of a file. Consequently, when using an FTP Client of this type, just one Client already counts as two active connections on the Server.

Other FTP Clients, such as the command terminal, only use one active connection, allowing two FTP Clients to connect to the Server simultaneously.

5.19. Firewall

The Firewall is designed to increase the security of the device while it is in use. The main function of the Firewall is to filter data packets coming into and leaving the device. The implemented filter uses information from each data packet to decide whether that packet is allowed. The main parameters used are the input/output interfaces, the port, the transport layer protocol, and the source and destination addresses.

5.19.1. Configuration

Firewall configuration is done through a dedicated section located in the *Management* tab of the controller's System Web Page, as shown below:

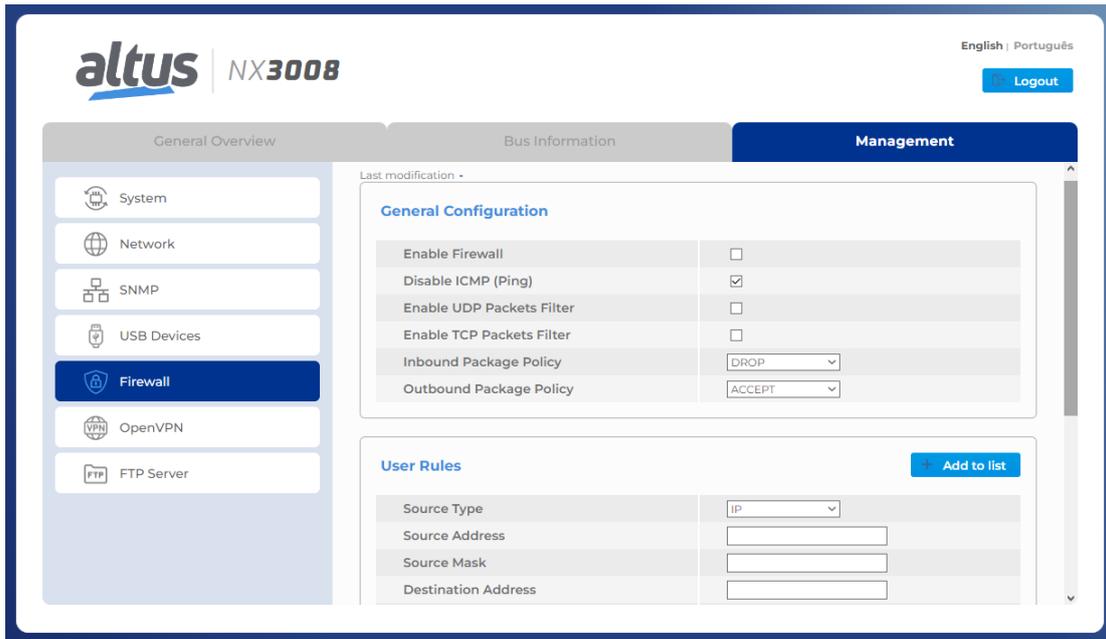


Figure 187: Firewall Configuration Screen

The Firewall is a separate feature from the MasterTool IEC XE, that is it doesn't require any interaction with the programming tool. Settings applied on the *Firewall* section take effect when confirmed with the *Apply* button, and are automatically saved in the controller. If the feature is enabled, it will operate again even after rebooting the device.

The following sections describe the possible settings for the Firewall, divided according to the tables of the *Firewall* section.

5.19.2. General Configuration

The image below shows all the settings in the *General Configuration* table:

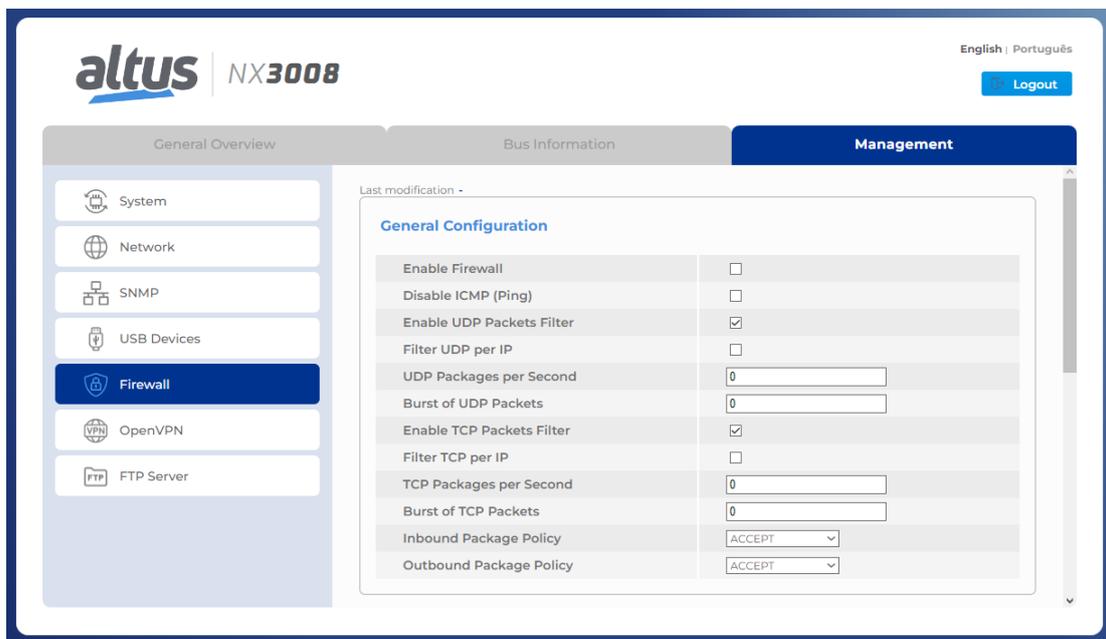


Figure 188: Firewall General Settings Table

This table expands dynamically by selecting the options to enable UDP and TCP packet filters, revealing all the items that can be configured. The first item in this table, *Enable Firewall*, is used to enable and disable this functionality. When the

Firewall is enabled, the web page settings, when submitted to the device, will be applied to the configuration files, and then the Firewall will filter what has been configured. If the Firewall is disabled, the configuration that was made is stored, but the rules are not applied in the controller.

The field *Disable ICMP (Ping)* enables or disables protection against the ICMP protocol. When protection is enabled, the controller will not respond to *Ping* requests, since it will drop packets that use the ICMP protocol. When disabled, the operation of the device for *Ping* responses maintains its normal behavior.

When enabled, the fields that enable UDP and TCP packet filtering, filter these protocols according to the limits configured in their respective fields. The packet filtering rule works like this: for a packet to be accepted, there must be "credits" available, and one credit is used to accept a data packet.

The setting of the field *Burst of XXX Packages* sets the initial value of packages (credits), which will be accepted. In this way, it is possible to set an overflow limit for these packets, where if there is a large flow of packets, only the configured amount will be accepted. The *XXX Packages per Second* field sets how many credits that rule will earn per second. For example, if the value is 5, each second, the rule will receive five new credits, so it will be able to accept five more packages. The limitation for this increment in the number of credits is the configuration of *Burst of XXX Packages* itself, and the limit set here is not exceeded, even with the increment of packets every second. These settings are applied as a *stock*, where upon receiving a data packet, it is first checked if there is any credit available in the stock, and then a decision is made whether or not to accept the package. If the packet is accepted in this quantity filter, it is forwarded to the filter of the other firewall rules.

The setting *Filter XXX per IP* causes the rule to differentiate the source addresses of each packet and apply the packet per second and packet overflow filters individually to each IP address. So, going back to the previous example, it can be considered that each source address has its *stock* of credits, and one address cannot use the credits that are in the *stock* reserved for others.

ATTENTION

Negative values are not allowed for the *XXX Packages per Second* and *Burst of XXX Packages* fields. If negative values are set, when applying the settings an error message will appear on the screen indicating the field that had a conflict. If the filter is enabled, but the values in these fields are left at 0, the filter is not applied.

The settings in this table are applied with the *Apply* button that appears in figure 190.

The fields for selecting both incoming and outgoing policies have options to accept and drop. if the Firewall is active, when data packets arrive, all the rules that have been configured are checked, and then the policy configured for these packets is applied, whether *Accept* or *Drop*. So if an accept policy is set, *Accept*, all packets that do not match any configured rule will be accepted by the firewall, and if a reject policy is set, *Drop*, they would all be dropped.

5.19.3. User Rules

The *User Rules* table was created to allow greater control over the firewall's rule settings. With it, you can configure different rules dynamically and with more precise filters.

User Rules	
Source Type	IP
Source Address	
Source Mask	
Destination Address	
Destination Mask	
Interface	NET1
Action	ACCEPT
Service Port	Other... 1
Protocol	UDP TCP
Direction	INPUT OUTPUT

Figure 189: Firewall User Rules Configuration Table

This table changes its format according to the selected *Source Type*, which can be IP or MAC. When the type is *IP*, the table has the items shown in figure above, but when the type is selected as *MAC*, the source and destination mask fields disappear, as well as the *Destination Address* field. The item *Source Address* now accepts a MAC address as input in a format of six groups of two hexadecimal digits separated by colons, e.g. "1A:2B:3C:4D:5E:6F". Also, an address-based *MAC* rule can only be configured as an input rule. In other words, the *Direction* field will be forced with the value *INPUT*.

With the *Source Address* and *Destination Address* fields, you can enter the addresses that will be configured for that specific rule, and using the *Source Mask* and *Destination Mask* fields, you can configure a network range for this rule. If you only configure the address, only the address will be assigned to the rule but with different netmask configurations, you can get IP groups of various sizes to be applied to the rule.

Interface configuration makes it possible to individually select each physical or virtual interface available to the controller. Based on which interface you select for a given rule, only data packets entering or leaving the interface will be filtered by the Firewall. If you use the option *Any*, this rule will have no interface filter. So the filtering rule will be valid for all available interfaces.

The *Action* field has three configuration options: *ACCEPT*, *DROP*, and *REJECT*. The action sets up what should be done with the package whose characteristics match the rule applied. If the chosen action is *ACCEPT*, the data packet having characteristics according to the rule will be accepted. If it is *DROP*, the packet will be dropped, and no reply will be sent to the sender of the package. Finally, if it is set to *REJECT*, the packet will be rejected, and a reply will be sent to the sender, stating that the requested *host* is inaccessible.

The *Service Port* field, is used to indicate which ports will be configured in this rule. All service ports that have a certain protocol or communication *standard* for the controller, such as the MODBUS protocol that has the standard port 502, are available with the service name and port used next to it. Thus, if you configure the rule for the MODBUS protocol, port 502 will be applied if you configure the rule for the WebVisu service, port 8080 will be applied, and so on for the other protocols listed in the checkbox.

This field also has two other settings, which are *Any* and *Other*. When you select the *Any* option, the rule is applied to all service ports except services except port 80 then two rules are created using the following port ranges: *1:79* and *81:65535*. If you select the *Other* option, a text box appears in which you can configure the port you want, except for port 80. To configure a port, you can type its number in the text box, but if you want to add more than a single port, you must use the "&" separator, and if you want to insert a range of ports, simply enter the start and end port using the separator ":".

Example of configuring ports 120, 144, and the range 1300 to 1450 in the same field: *120 & 144 & 1300:1450*.

This field doesn't accept values outside the range 1:65535, port 80, or port repeats.

The HTTP port 80 can only be set by selecting it from the list of known protocols and cannot be applied to the NET 1 interface. So if the HTTP protocol is chosen, the Interface field *NET 1* and *Any* won't be selectable.

In the *Protocol* field, you can select between UDP, TCP, and UDP|TCP protocols. If you select the UDP|TCP option, two rules will be created on the firewall, one for each transport protocol.

In the *Direction* field, you can select between *INPUT*, *OUTPUT*, and *INPUT|OUTPUT*. These options cause the rule to be applied to packets arriving at the device, option *INPUT*, or leaving it, option *OUTPUT*. If the joint option is configured, two

rules will be created, one with each direction option.

The figure below demonstrates how a rule is applied:

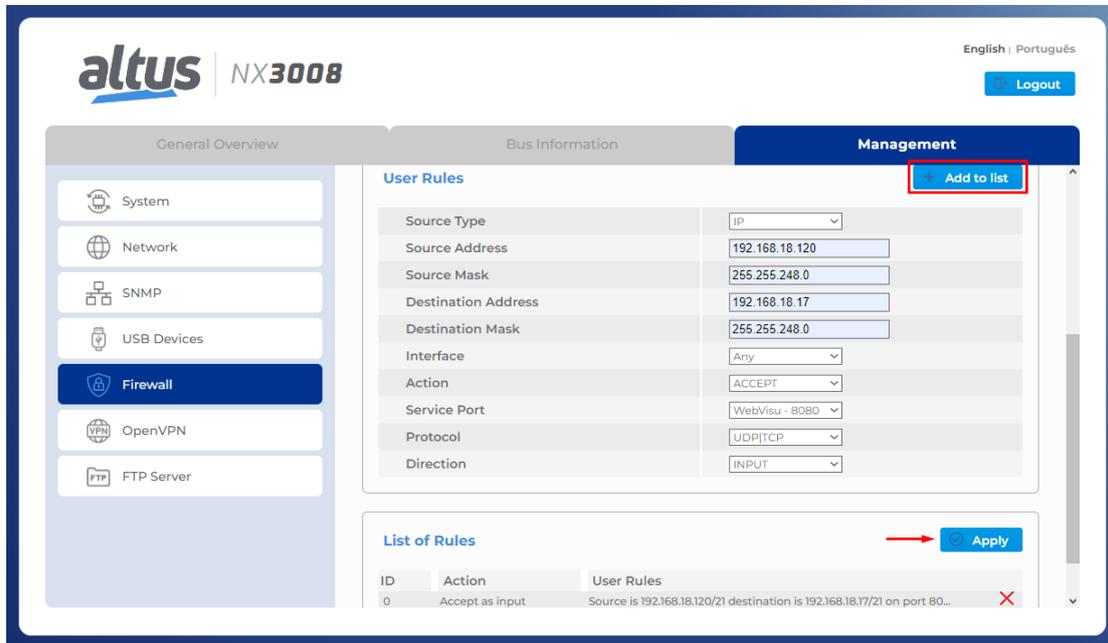


Figure 190: Firewall User Rules Enforcement Table

After filling in the fields as you wish to configure the firewall rule, you must click the *Add to list* button. By doing this, all the settings will be analyzed to check if there are invalid values or if there is any duplicate rule. It's impossible to add two rules with the same address, mask, interface, port, and direction parameters. If a conflict is found, a message will be displayed indicating the field that contains an invalid setting or the ID number of the rule in the table whose settings caused the conflict with the newly configured one.

After all, parameters are checked, the rule will be added to the list below the configuration table. This list expands automatically as rules are added or deleted. If you want to exclude a rule from the list, you can place the mouse over the one you want to exclude. When you do this, a red X button will appear on the right, as shown in the previous figure. By clicking it, the rule will be deleted from the table.

When adding new rules, or deleting an existing one, in the rules table, the *Apply* button below must be clicked for the configuration to be applied to the device.

ATTENTION

During the application of firewall rules, there may be a momentary instability in Ethernet communication.

5.20. OpenVPN

VPN (Virtual Private Network), used for surfing unsecured networks, transmitting data, or simply accessing the Internet with a high level of security and privacy. The VPN virtual network can be understood as a tunnel in which information travels securely, protected by security certificates and keys. OpenVPN is an *open-source* service, which means that it is free to use and distribute, and its source code is open for modifications if needed.

The main purpose of a VPN is to communicate securely over an unsecured network. To make this possible, data encryption is used based on certificates and keys generated using TLS, Transport Layer Security, a protocol that performs 256-bit encryption, one of the most secure.

To perform the configuration of the OpenVPN client or server, the OpenVPN page was created in the *Management* tab of the CPU's System Web Page. As shown in the figure below.

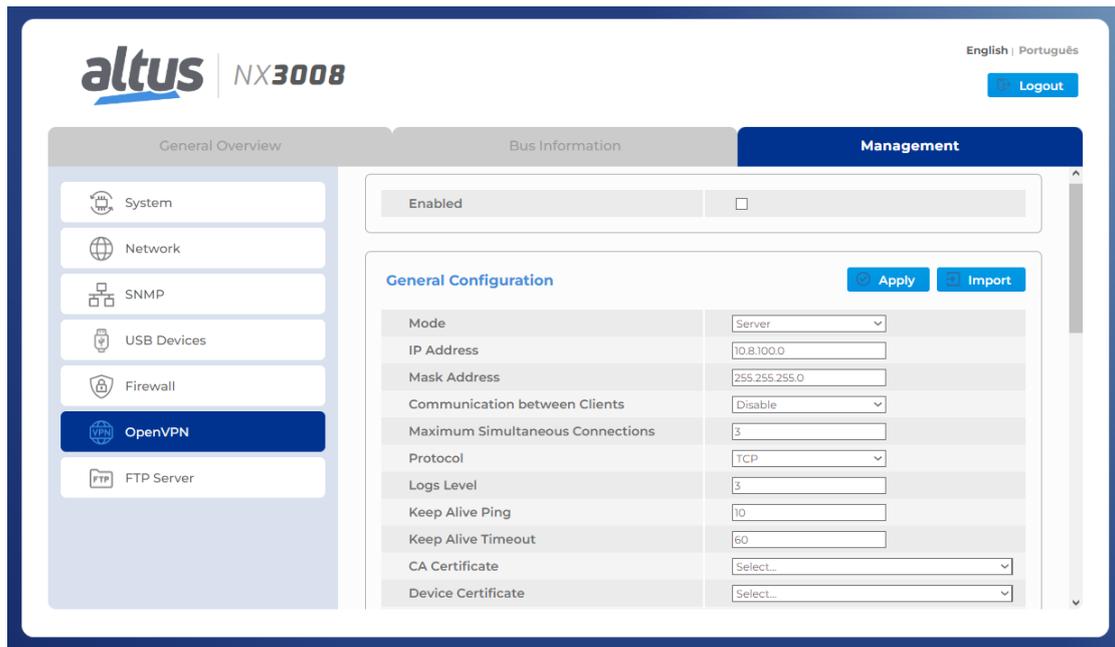


Figure 191: OpenVPN Configuration Screen

Because it is located within the *Management* tab, access to this page is password protected. The following sections describe the settings and functionality of this page.

5.20.1. Import Configuration

To quickly and easily configure the VPN on your device, you can use the *Import* button that appears in the picture 191 in the upper right corner of the page. Clicking on this button opens a file explorer window where you can select a configuration file. Files with extension *.conf* or *.ovpn* should be selected. When you select a file, its contents will be read and the configuration parameters present will fill their respective configuration fields on the web page.

For the file's parameters to be interpreted correctly, they must follow standard OpenVPN configuration file syntax.

If there are security files, certificates, or keys, written in the configuration file, along with the other parameters, they will be read and separated into separate files within the controller for use.

ATTENTION

Do not use spaces to separate the words in the name of the *.conf* files. Instead, use *"_"* to separate them.

5.20.2. OpenVPN Configuration

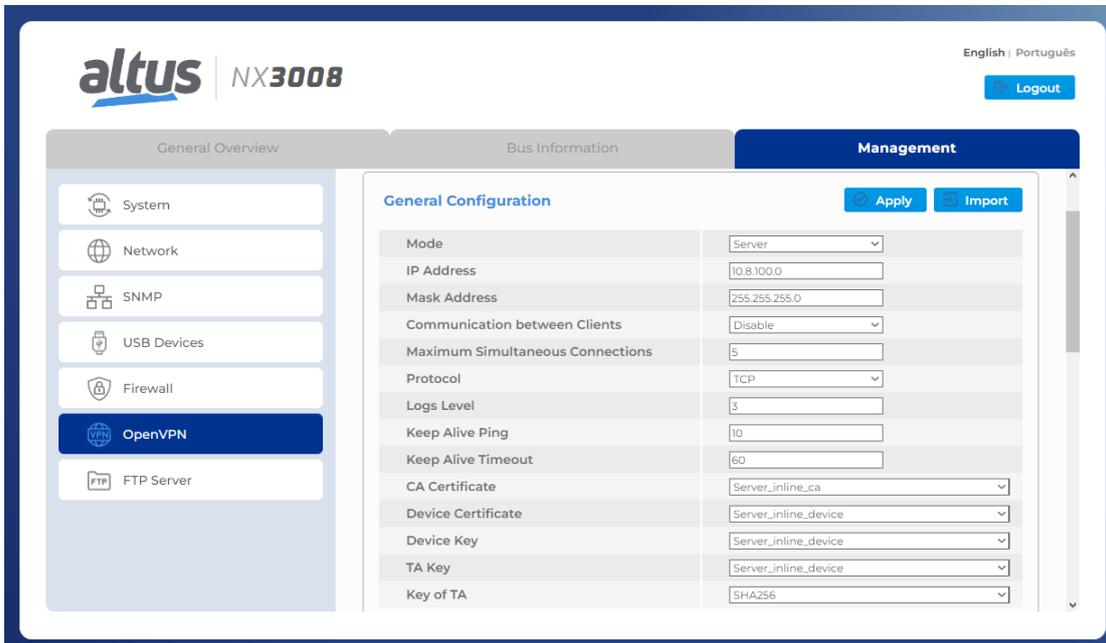


Figure 192: OpenVPN Server Configuration Table

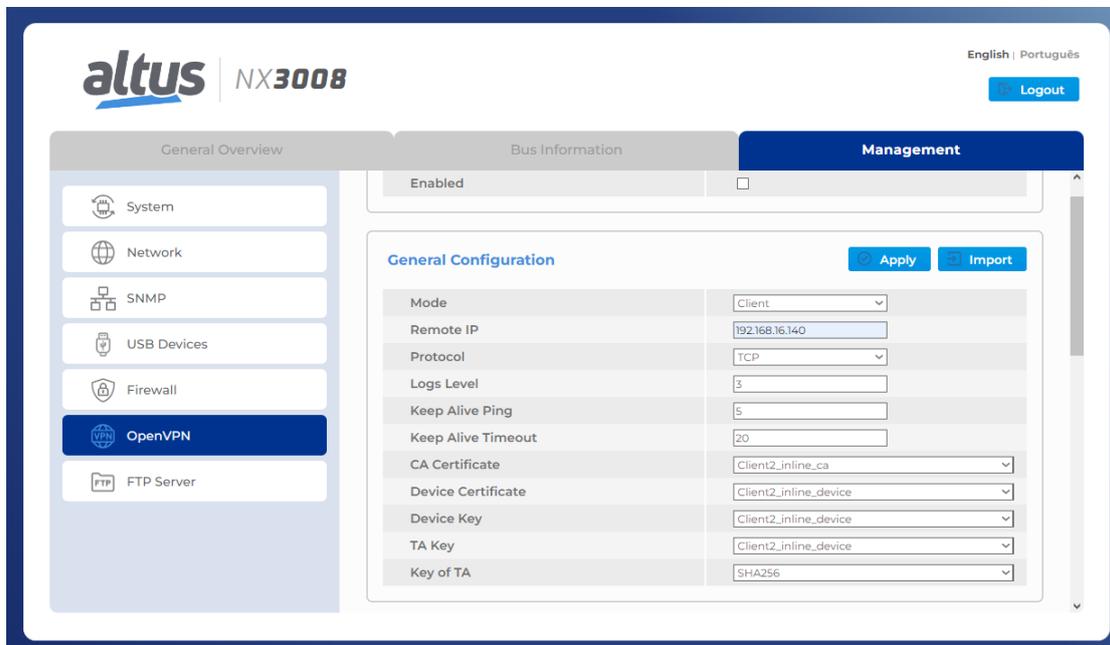


Figure 193: OpenVPN Client Configuration Table

This section shows how OpenVPN configuration is performed. The settings will be divided into three parts: settings common to both operating modes, settings unique to a server, and settings unique to a client.

5.20.2.1. Common Configurations

Looking at the figures with the client configurations, figure 193, and the server configuration, figure 192, you can identify that several parameters are the same for both configurations. These are:

5.20.2.1.1. Mode

With the configuration of the *Mode*, you can select between two options, client or server. When you select one of the two modes, the settings table changes automatically to allow the configuration of the necessary fields for each mode of operation.

5.20.2.1.2. Protocol

This field configures which transport protocol will be used for VPN communication. It can be set between UDP and TCP.

ATTENTION

The configuration of the server and all its clients must be the same. With a divergent configuration, OpenVPN is not able to perform communication.

5.20.2.1.3. Logs level

This field sets the level that the log file will receive. The setting ranges from 0 to 5, 0 being the most basic level and 5 being the most advanced.

Level 0 only displays logs about some critical failure in OpenVPN and levels 4 and above are used for debugging as there is a lot of information being written to the log file. For normal operation, it is recommended to use value 3.

This field only accepts numbers as input. You are not allowed to use letters or special characters.

5.20.2.1.4. Keep Alive Ping

This field sets the time, *in seconds* when the *Ping* request will be forwarded. This request serves to verify the connection between the server and the clients.

This parameter can be set on both the server and the OpenVPN clients, but if this parameter is set on the server, the clients will assume the server's value and not the value set on them. If the server doesn't have such a setting, each client assumes its setting normally. If you want to disable pinging between the server and the clients, set the value to 0.

This field only accepts numbers as input. You are not allowed to use letters or special characters.

5.20.2.1.5. Keep Alive Timeout

This field sets the time, *in seconds* when the timeout of the *Ping* request will occur. After the expiration of this time, without a response from the other VPN device, it will be considered disconnected.

This parameter can be set on both the server and the OpenVPN clients, but if this parameter is set on the server, the clients will assume half of the server's value and not the value set on them. Clients receive half the amount to ensure that they are disconnected in case the server disconnects. If the Server does not have such a setting, each client assumes its setting normally. If you wish to disable this feature, set the value to 0.

This field only accepts numbers as input. You are not allowed to use letters or special characters.

5.20.2.1.6. Security Files

In the fields *CA Certificate*, *Device Certificate*, *Device Key* and *TA Key*, you must select which security file, certificate, or key, will be used to establish the OpenVPN communication. The options in each field, *combobox*, are filtered according to the type of key file or certificate, although there is no differentiation between keys and certificates.

To be possible to select a file, it must first have been imported.

All security files are required for correct communication to be established between clients and the VPN server, except for *TAP Key*. This key is optional for communication, but if it is used on the server, it becomes mandatory for all clients on the server.

See the [TLS Key and Certificate Management](#) section for further information about generating certificates and security keys based on TLS.

5.20.2.1.7. TA Key

In the field *TA Key* it is set which type of encryption will be applied to the *TA Key*. This field stays hidden until you select a file for the TLS key because it is only used in conjunction with this key. The default value of this parameter is *SHA1*, but you can select from the following values: *SHA256*, *SHA512*, and *MD5*, in addition to the default *SHA1*.

ATTENTION

This configuration needs to be the same between the clients and the server in the same OpenVPN network. If the value of this field is different between the client and server, the connection will not be established.

5.20.2.2. Exclusive Server Configurations

The exclusive server configurations, seen in figure 192, are described below.

5.20.2.2.1. Network Address

The IP range that will be used to assign the server and client addresses for the VPN network is configured by the server by setting the *IP Address* and *Mask Address* fields. All IPs that will be assigned to the clients and the server will be taken from the specified range.

The server's IP address is always the first available value in the configured range, and for IP assignments to clients, the values still available in the range are used, so the first available value is assigned as clients make their connection. For example, if a network is configured with the addresses 10.8.12.4 and mask 255.255.255.248, the server will assume IP 10.8.12.5 which is the first available address in the configured range. However, if mask 255.255.255.255.0 is set, the server will assume IP 10.8.12.1, which is the first available address in the range.

The IP and Mask address fields only accept settings that have the syntax of an IP address and mask address, respectively. If anything out of the standard is configured, an alert message will be displayed, informing you that an error has occurred.

5.20.2.2.2. Communication between Clients

In this field, you can enable or disable communication between clients in the VPN network. When the option is selected as *Disabled*, only client-server communication can be performed directly. If the option selected is *Enabled*, it will allow communication between the clients themselves in addition to the client-server communication.

5.20.2.2.3. Maximum Connected Clients

In this field, you can set the maximum number of clients that can connect to the server simultaneously. This field accepts only numeric characters, and the minimum value is 1.

5.20.2.2.4. Private Networks

When you select OpenVPN's operating mode as a server, a table will be displayed, normally hidden, which allows the configuration of private networks that can be below the server and each client.

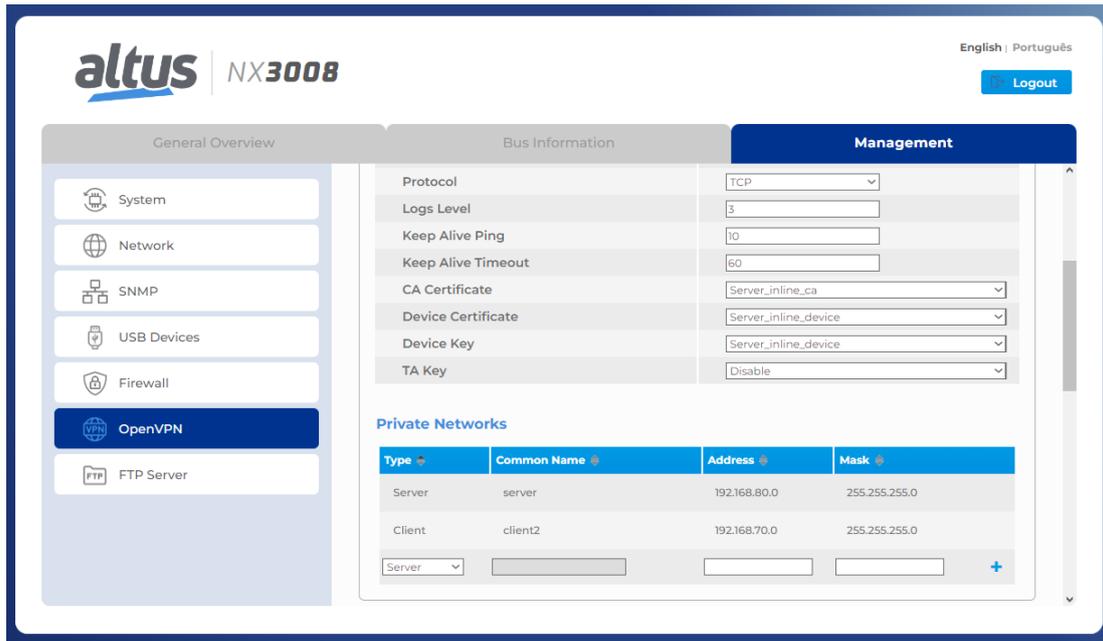


Figure 194: OpenVPN Private Network Configuration Table

To configure a private network that is below the server, simply select the network type as *Server* and configure the network addresses and mask. Configuring a private network for a client requires, in addition to setting the type as *Client*, to enter the *Common Name* of the client that owns the network being configured.

The Common Name of a client is set when generating the *Device Certificate*. This parameter is entered when creating the certificate and is unique for each client and server. The configuration of these private networks creates a routing table that will be checked when receiving or sending packets over the VPN.

Figure above, shows a configuration of a subnet *80* on the OpenVPN server, then a routing rule will be configured that will forward the data packets that will be received by the VPN to the device interface configured on this network. It also creates a rule, internal to the server, that if a data packet has the subnet *70*, this packet will be routed and forwarded through the VPN tunnel. The same behavior occurs with the *client2* client, but with the subnets switched, because below this client is the *70* subnet and it will forward packets with the *80* subnet to the VPN tunnel.

See the following figure for an example of architecture:

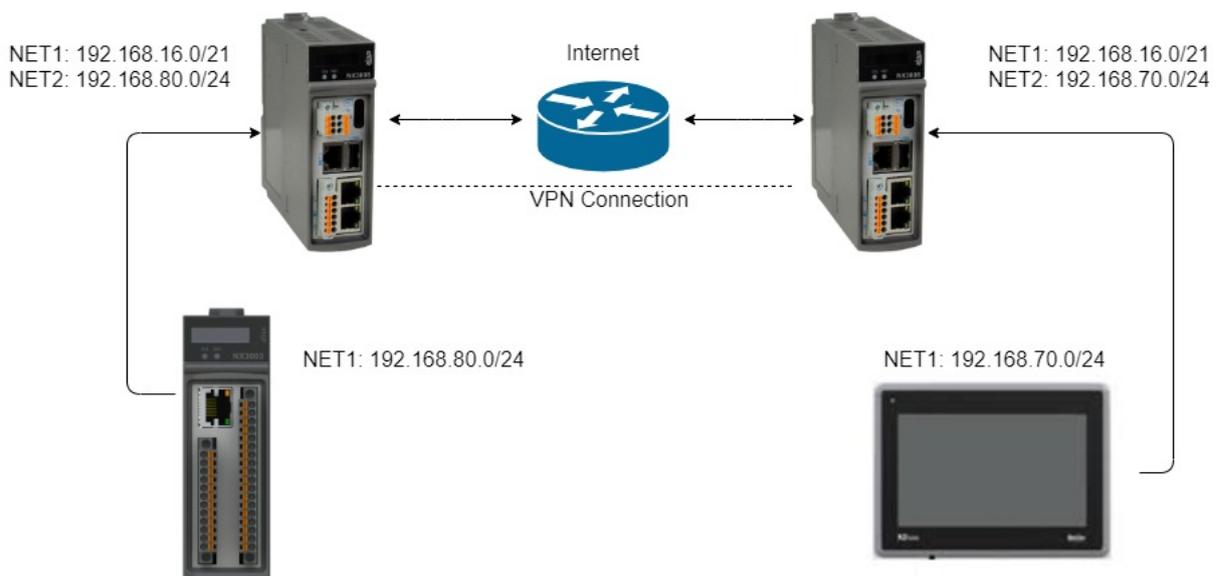


Figure 195: Architecture Example with Private Networks

In the example picture, the NX3008 on the left has a private network 80 configured on its NET 2, and connected to it is an NX3003 on the same network. The NX3008 on the right has a private network 70 configured on its NET 2 and connected to it is an HMI, on the same network. The example architecture realizes the communication between the NX3003 and HMI devices over VPN by configuring their respective private networks.

After filling the fields, shown in the figure 194, with the desired configuration, you must click on the blue + button that appears on the far right of the configuration fields, so that the rule is added to the table. If you want to delete a rule, drag your mouse over the rule you want to remove, and a red X will appear on the right, as shown in the image 194. By clicking on this X, the rule is removed from the table.

For the settings present in the table to be applied to the device you must click the *Apply* button and confirm the operation in the confirmation window that will appear. When the rules are applied, a message will be displayed indicating whether the operation was successful or not.

5.20.2.3. Exclusive Client Configurations

There is only one configuration unique to OpenVPN clients on the page, which you can see in the picture 193. This configuration is the *IP Remote*.

5.20.2.3.1. Remote IP

The Remote IP field sets the address where the VPN server is expecting communication from the clients. If an OpenVPN server is established on a computer, the remote IP configuration must be done according to the IP address of this computer. This field also accepts *host names* as the remote address, so you can set an IP or a hostname in this parameter.

ATTENTION

Because of the need to allow for such different parameters, IPs, and host names, the only check that exists in this field is whether or not data exists. Be careful when performing the configuration.

5.20.2.4. Application Settings

To enable the functionality, the checkbox *Enabled*, shown in the figure above, must be checked. If you just want to apply the settings you have made and not enable OpenVPN, uncheck this checkbox.

After you have made all the desired settings, the settings must be applied to the device, to do this use the *Apply* button. This button is shown in the figure 193 in the lower right corner. When the settings are applied and the VPN is enabled, the web page will perform an automatic *scroll* to the OpenVPN *status* table, displayed in the [Status Table](#) section.

5.20.3. Security Files

Security files are used to establish OpenVPN's communication securely by performing the role of encrypting and decrypting the data packets that will travel through the VPN tunnel. In the [TLS Key and Certificate Management](#) section, it is described how to generate TLS keys and certificates. Here is a screenshot that shows the section responsible for managing the security files:



Figure 196: OpenVPN Security Files Table

In this section of the System Web Page, you can manage the security files. You can import files, monitor the validity of certificates, download files uploaded to the device, and delete files that have been uploaded.

By clicking the *Choose files* button, you can import certificates and keys, these files must have the respective extensions *.cert* and *.key*. This button opens a file explorer window and allows the selection of one file, i.e. multiple files.

ATTENTION

There is a limit of 12 files that can be imported into the controller.

The control of the files is done in the table, which is shown in the picture 196. This table adds new items, or removes them, as the import or delete operations occur. You can identify whether the file is a key or a certificate by the second item in the list, the *Type*, which indicates what that file is. For the certificates, their *commons names* and their expiry dates, both start and expiry, are also displayed.

You can recover a file that has been imported into the part and also delete it. When you drag the mouse over a file in the table, two buttons appear, one for downloading and one for deleting. The download button is a black arrow pointing downwards, and the delete button is a red X.

5.20.4. Status Table

Designed to allow for data monitoring, OpenVPN’s status table automatically expands as you change settings and displays various data about the connection such as the state of the VPN, the VPN IP assigned to that device, the data being transmitted, and the security files being used for communication.

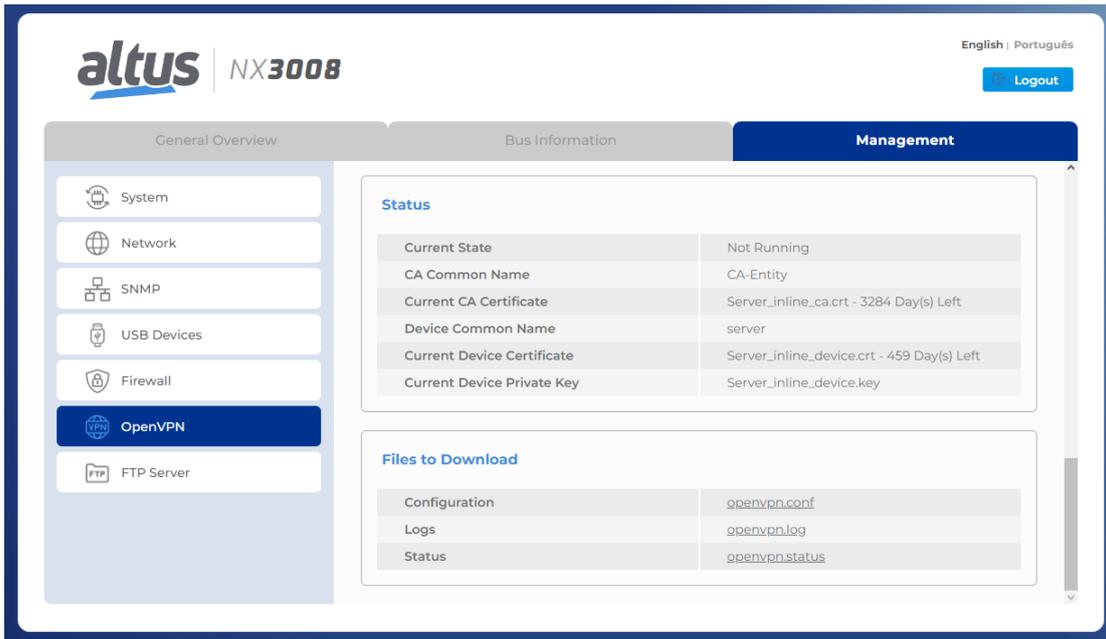


Figure 197: OpenVPN Status Table with Feature Disabled

When VPN is disabled, the table has few parameters. The field *Current State* indicates whether the VPN is enabled or not, and the other fields show which certificates and keys are configured for VPN communication. If one of the security files has not been selected, the character "-" will appear instead of its name, indicating that there is no file configured.

The common name fields for the CA and the device display the names given to the respective certificates, certificate authority, and device.

Next to the file name of each certificate is displayed the remaining time, *in days*, until its expiration date.

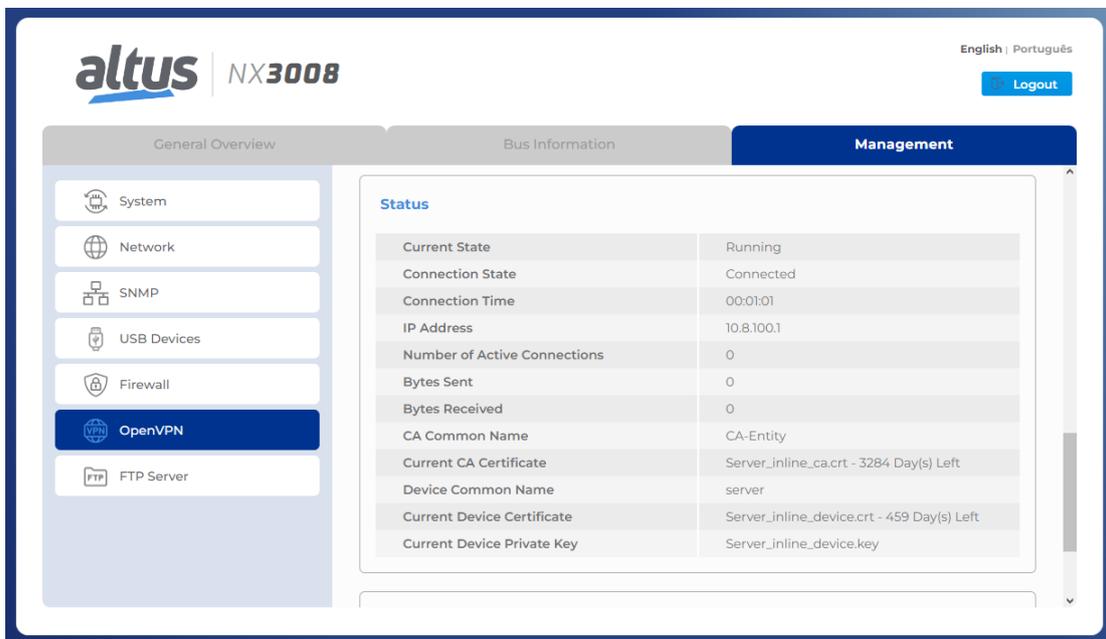


Figure 198: OpenVPN Status Table with Feature Enabled

When the functionality is enabled and the settings are applied on the device, the table has its cells dynamically modified so that the remaining information is displayed. Information about the OpenVPN connection status can be found in the first two topics of the list.

The item *Current State* has the states of *Not Running*, *Starting service...*, and *Running*, which indicate respectively that the VPN is disabled, is starting or is enabled.

The item *Connection State* has the states *Not connected*, *Connecting...*, and *Connected*.

The other information that can be obtained from this table is the total connection time, the device's IP address, and the amount of data sent and received, in bytes. The status of how many clients are currently connected is only displayed when OpenVPN is operating as a server.

5.20.5. Files to Download

You can check the information generated by OpenVPN through status and log files. The list of files to download is only displayed when there is a file to download. If there is none, the message "No file found in the controller!" is displayed. Clicking on any of the links will download the requested file through the browser.

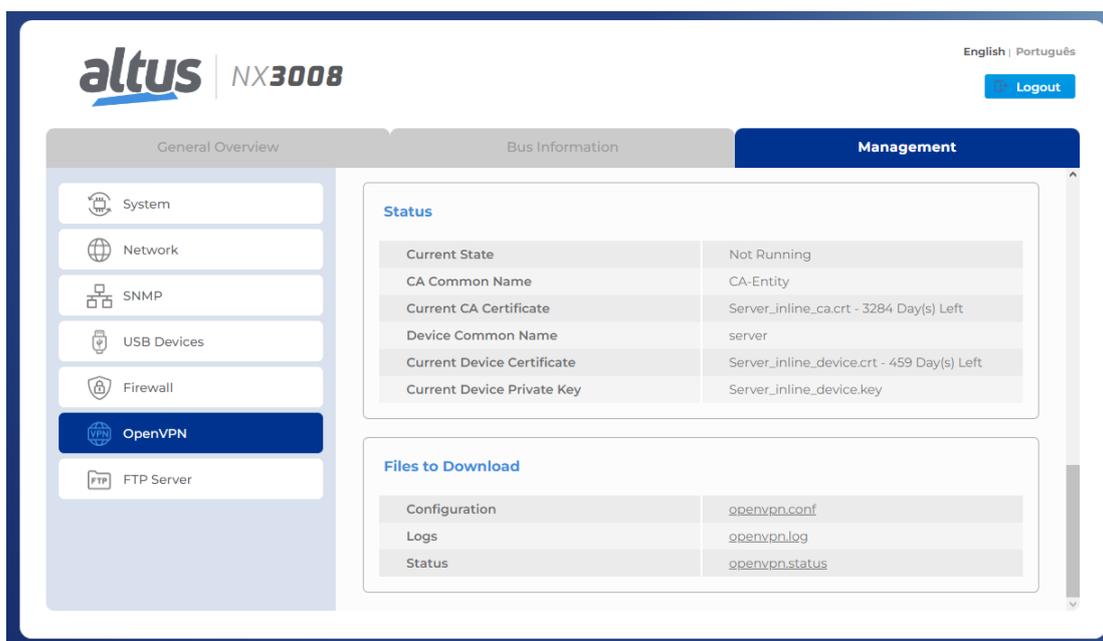


Figure 199: OpenVPN Download Section

5.20.6. Architectures Configuration

This section will cover some possible configurations for OpenVPN, such as Host-to-Host, Host-to-Site, and Site-to-Site architectures.

5.20.6.1. Host-to-Host



Figure 200: Example of Host-to-Host architecture

This topology allows the connection between two VPN hosts. Both hosts can be chosen to be configured as the server, then the other should be configured as the client, or both hosts can be configured as clients and have a third host that will be the server for the VPN network.

Setting up this type of architecture doesn't require any specific configuration. In other words, there is no restriction on the settings available on the OpenVPN web page.

5.20.6.2. Host-to-Site

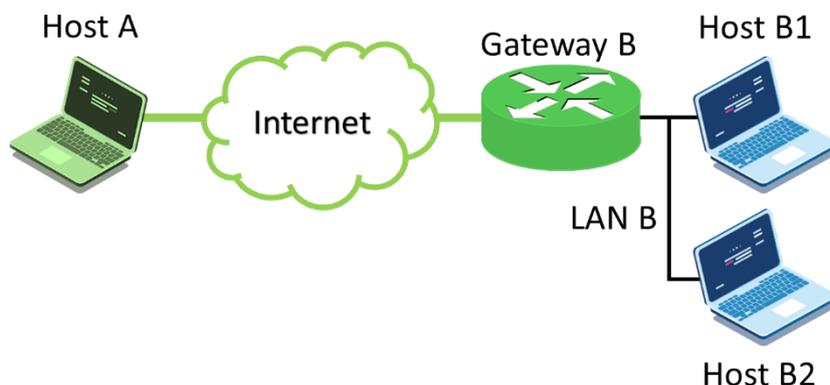


Figure 201: Example of Host-to-Site architecture

This topology allows the connection between two VPN hosts, but one of these hosts also acts as a gateway to the VPN network. Through this gateway, routing is performed to set up communication between hosts A, B1, B2, and Gateway B. In this scenario, either Host A or Gateway B can be the server. When one is the server on the network, the other will be the client.

The hosts, B1 and B2, that are on a private Lan B network below Gateway B, don't need to support OpenVPN to be able to communicate since all communication is handled by the VPN network gateway.

To enable communication between all devices on the network, you need to create routing rules for the VPN tunnel. Please refer to the section [Private Networks](#) to see how to create private network rules.

This VPN connection architecture requires some specific configurations. The server must have its topology configuration as a Subnet, this being the default configuration of the controller, to configure the private networks under Gateway B, as seen in the image above.

You also need to enter the address of the private network, Lan B, that will be communicating through the VPN. This configuration is done using the command `push "route Lan_B_IP Lan_B's_Mask"` and is required regardless of whether the private network is located below the client or the OpenVPN server, but if the private network is below the VPN client, you must add, in addition to this command, the following configuration: `route route Lan_B_IP Lan_B's_Mask`. These settings are written to the VPN server's configuration file.

5.20.6.3. Site-to-Site

Below is a picture that represents a Site-to-Site connection:

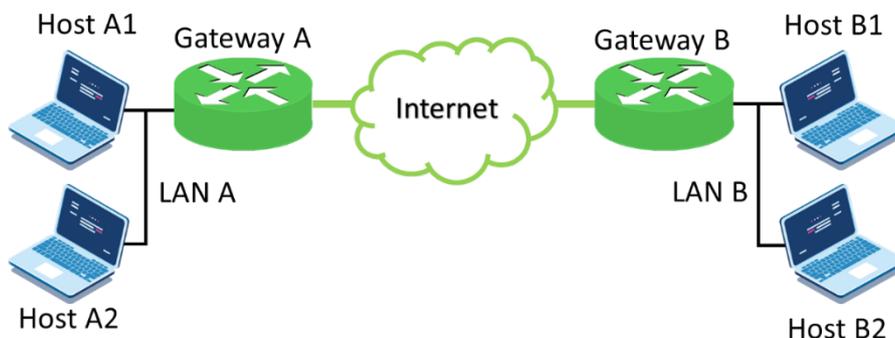


Figure 202: Example of Site-to-Site architecture

This topology allows the connection between two VPN hosts, both of which acts as a gateway to the VPN network. Through these gateways, access is provided to establish communication between hosts A1, A2, B1, B2, Gateway A, and Gateway B. In this scenario, any gateway can assume the role of a server, so the other will be the client.

None of the hosts that are in a private network below one of the two gateways need to support OpenVPN to be able to communicate, since all communication is handled by the VPN network gateways.

To enable communication between all devices on the network, you need to create routing rules for the VPN tunnel. Please refer to the section [Private Networks](#) to see how to create private network rules.

The configurations for this architecture need the same specific settings described in section [Host-to-Site](#), with the difference that now, there are two private networks, and both must follow the configuration that has been demonstrated. Assuming that Gateway A is the server on this connection, you should add the following commands to the configuration file: *push "route Lan_A_IP Lan_A's_Mask"*, *route Lan_B_IP Lan_B's_Mask*, and *push "route Lan_B_IP Lan_B's_Mask"*. If the server is Gateway B, in the configuration file it would be added: *push "route Lan_B_IP Lan_B's_Mask"*, *route Lan_A_IP Lan_A's_Mask*, and *push "route Lan_A_IP Lan_A's_Mask"*.

5.21. Docker

The Docker functionality was developed to expand and enhance the integration and operation of the CPU. The main purpose of Docker is to enable the execution and maintenance of Docker *Containers*. The installation, execution and maintenance of the *Container* are carried out through the *Portainer* management platform.

ATTENTION

There is a wide range of applications available as Containers and openly distributed on platforms such as *Docker Hub*. Altus does not provide specific technical support for the use and operation of these applications; this should be handled directly by the Container developer or maintainer. Furthermore, due to the processing and memory constraints of the programmable controller's CPU, many of these containers may not run properly. Therefore, we recommend to check the tutorials available on Altus website, which use previously tested containers compatible with the resources available on this platform.

5.21.1. How to access a Docker Container

The vast majority of Docker *Container* are accessible through an exposed port configured for the *Container*. The default exposed port can be discovered by searching in the documentation for that *Container*. It is expected that the *Container* will always be linked to the default port listed on those sources.

5.21.1.1. How to access Portainer

Our management platform of Docker Containers, *Portainer*, is a *Container*. Like most *Containers*, it is accessible through the exposed port in which it is linked to. In *Portainer's* case it is located in the CPU IP followed by ":9000". For example: "192.168.15.1:9000". After accessing the link, you will be prompted to create an account to access the Portainer platform. This account should have a username and a password of at least 12 characters.

CAUTION

This password is not in the *Altus* domain and is **NOT** recoverable! The password should be stored with caution!

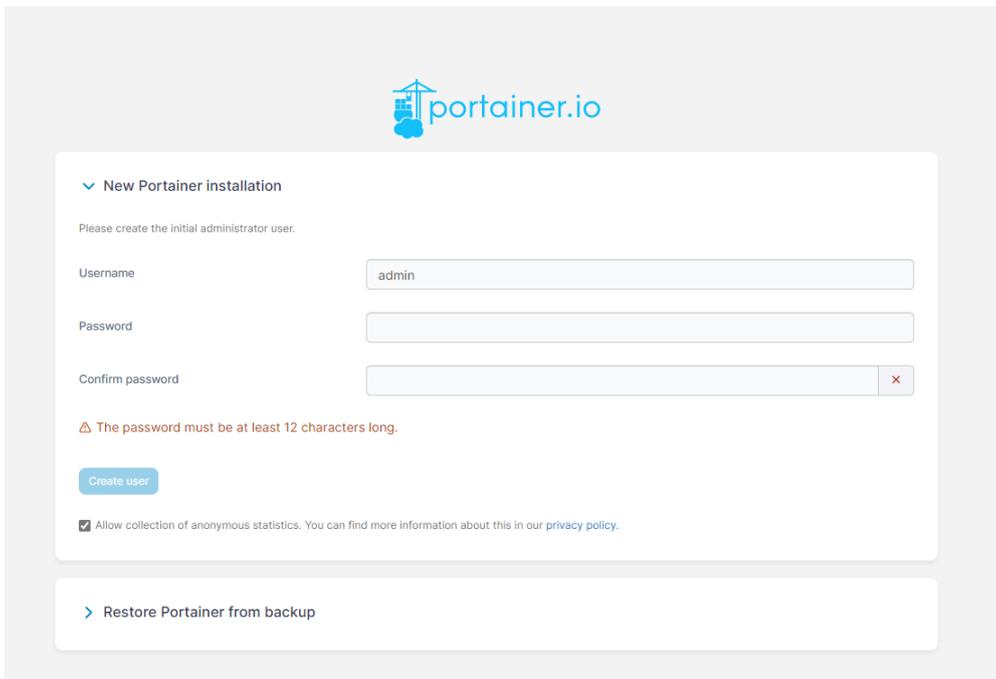


Figure 203: Portainer’s Login Screen

It is also possible to use the *"Restore Portainer from backup"* option to restore all configurations using a restoration file.

ATTENTION

It is recommended that the backup file be updated regularly.

5.21.2. Quick Setup

Once connected, the platform will redirect you to the home screen. This home screen will contain two options: proceed using the local environment in which Portainer is running or add an environment to connect to another available environment.

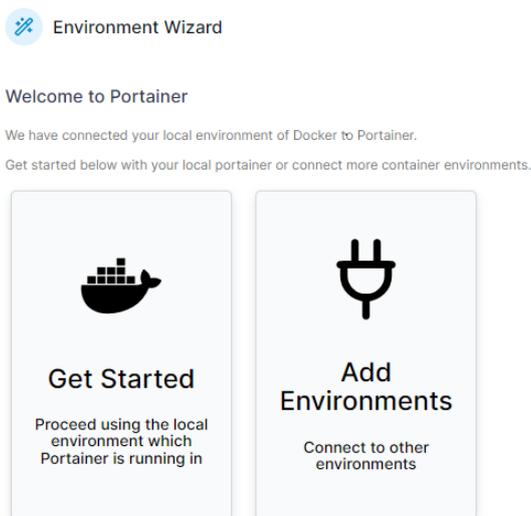


Figure 204: Portainer’s Initial Screen

The correct option to be chosen is "Get Started". Once picked, *Portainer* will redirect you to a screen that shows the available environments in your device. It will have only one environment, that is the Docker environment, easily identifiable by the whale logo that it has adopted.

5.21.2.1. Local Environment Informations

You can find information about the Docker environment running within the CPU on the home screen. Among this information are: the complete date, Docker server version, Stacks, and the number of *Containers* followed by their statuses. The number of created *Volumes*, and *Images* present in the UCP, the number of usable CPUs, and the maximum amount of memory available for all the *Containers*.



Figure 205: Environment Info Screen

CAUTION

It is important that the date in the environment is correct! It can be configured through the clock setting function on the CPU web page.

5.21.3. Environment's Dashboard

After accessing the *Dashboard* by clicking on the desired environment, you will encounter some of the information previously displayed in a table of basic information named "Environment info". These include the available hardware information and the Docker version. It is possible to access the menus listed above by interacting with them. From all the menus listed, the most relevant are the *Container menu* and the *Image menu*.

ATTENTION

The NX3008 does not support containers that require a dedicated graphics processor.

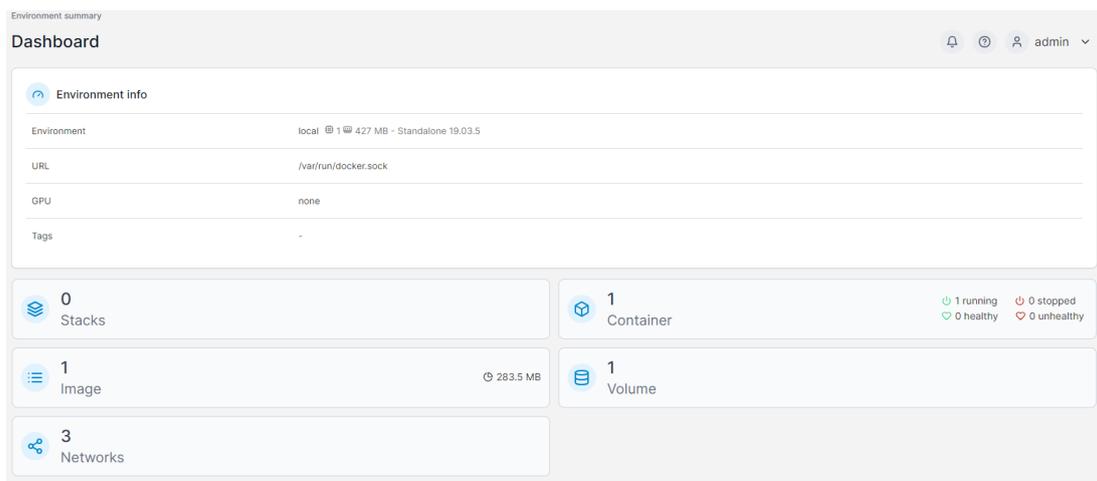


Figure 206: Dashboard

ATTENTION

For more information about the menus and/or Docker itself, you can access the *Portainer* documentation, which is available by clicking on the "(?)" symbol next to the user in the top right-hand corner of the screen.

5.21.3.1. Containers Menu

The *Container* menu is responsible for the comprehensive administration of *Container*. It allows access to the *Container*, the image, and some relevant quick actions. You can see the creation date, IP address, published ports, when applicable, and the *Container's* owner profile.

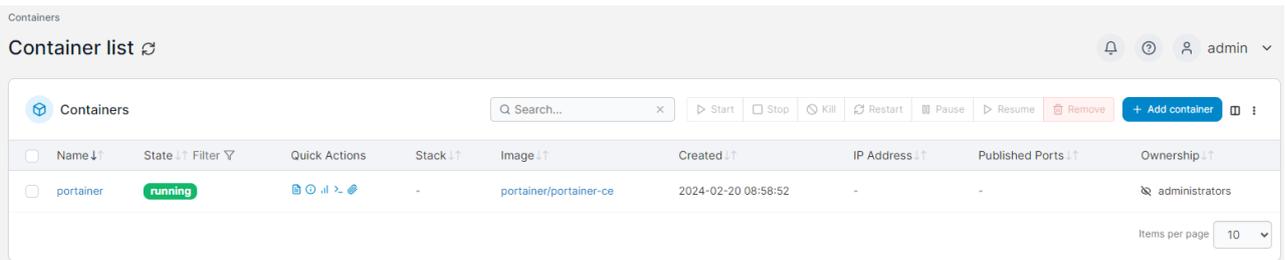


Figure 207: Containers Menu

CAUTION

No *Stop*, *Kill*, *Restart* or *Pause* commands should be performed on the *Container* of the *Portainer*. If any of these operations are performed, a reboot is required for the *Container* to function again.

5.21.3.2. Images Menu

The *Images* menu is responsible for the administration of downloaded images and their statuses. The name and tag of images can be obtained through the *Search* button located to the right of the Image input box. The *Pull the Image* button is responsible for obtaining the image. As indicated on this screen, there is a limitation on image *"pulls"*.

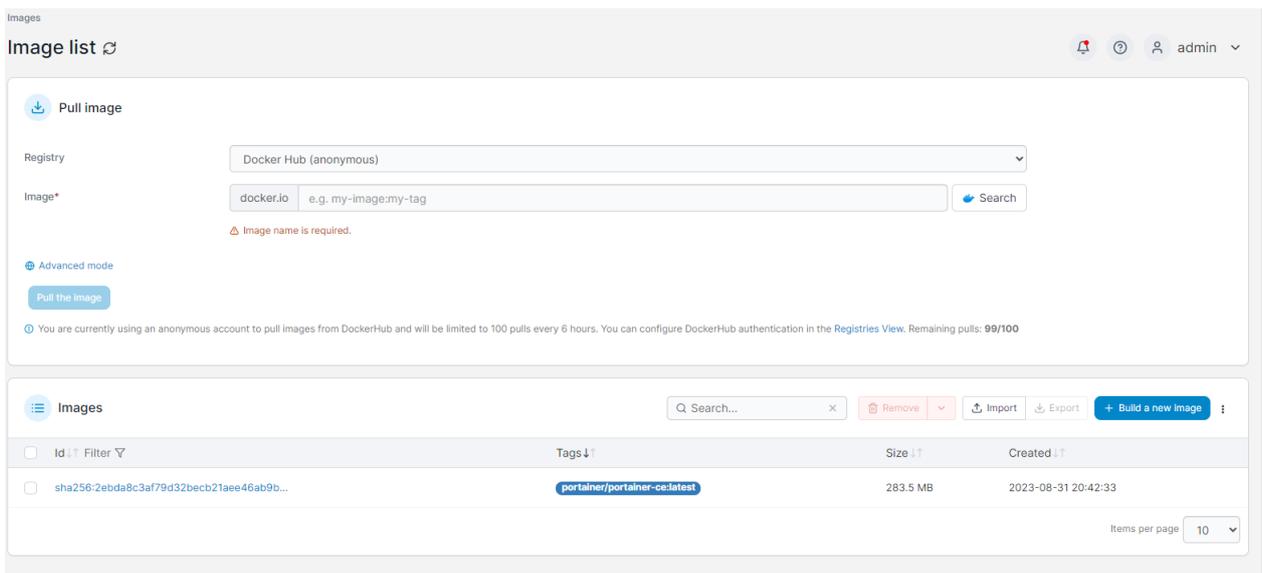


Figure 208: Images Menu

Below, in the *Images* menu, you can identify all the obtained images, their status, whether it is "Unused", their tag, the occupied size, and the creation date. Like the *Stack*, you can add images using a web editor through the "Import" and "Build a new Image" buttons.

5.21.4. Creating and Configuring a Container

A *Container* can be created through the *Container* menu, accessible from the *Dashboard*, or through the quick access menu on the left side of the *Portainer* web page. There is also the option to create a *Container* through *Stacks* and configure them later.

ATTENTION

Creating custom images using Portainer's *Build Image* feature is not supported on this platform.

ATTENTION

During the process of installation and configuration of a *Container*, it is highly recommended that the controller be stopped, with the application removed using the *Reset Origin* command. This is necessary because, due to the intrinsic characteristics of Docker technology, these operations perform low-level access to the controller's operating system which can temporarily affect the stability of the control function (temporary performance degradation and loss of determinism) and, in extreme cases, even cause the system to reboot.

Using the "Add Container" button, you can add a *Container* from images you have already obtained through the *Images* menu or images that will be obtained in the *Container* creation process.

Clicking on "Add Container" will take you to the "Create Container" screen.

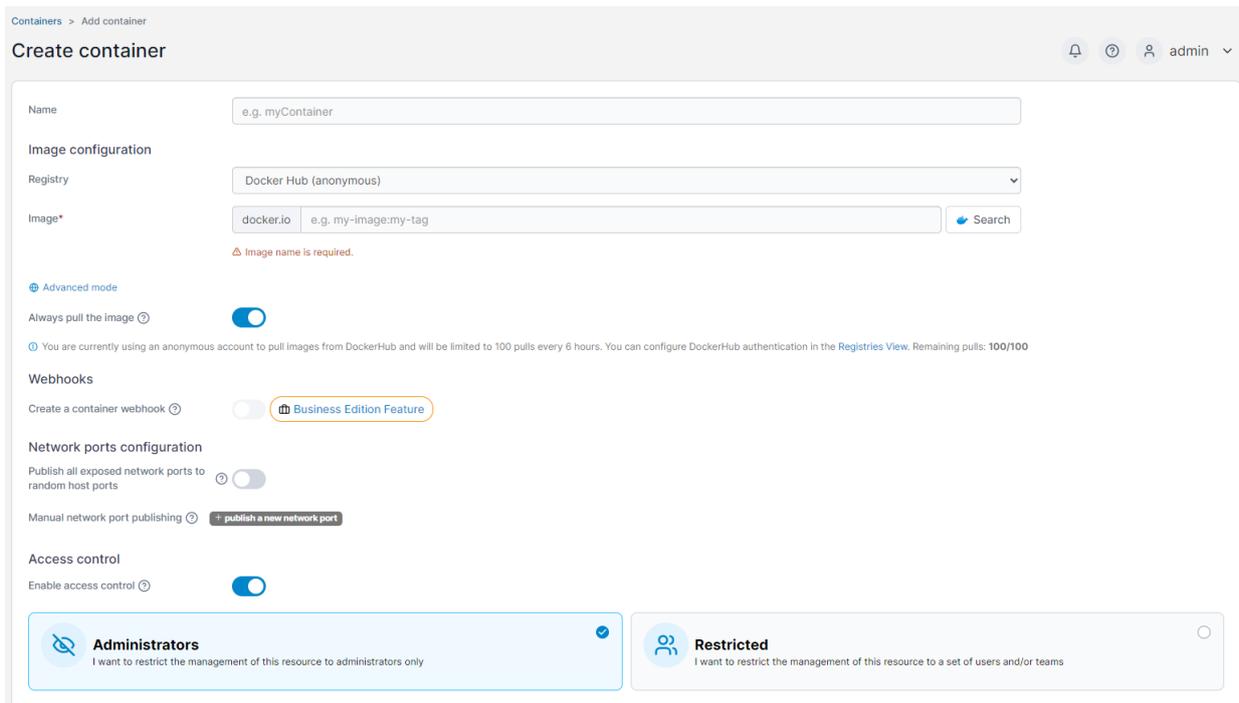


Figure 209: Create Container Screen

On this screen, you can name the *Container* being used and specify the image you want to use.

Like the *Images* menu, you can access Docker Hub to view available images and their respective names. There is an option for "Always pull the image". If activated, shouldn't be needed to add the image through the *Images* menu beforehand. It is **NOT** always the case. So the *Container* may not be created if the image is not available in the device. To add an image, you

can use the [Images Menu](#) as a guide. The options in this basic *Container* configuration box are case-sensitive and should be evaluated according to the specific requirements.

To create the *Container* definitively, you can use the *"Deploy the Container"* button. However, it is of paramount importance to perform the additional configurations present in the item below.

In case you are creating *Containers* through the *Stacks* method, it is important to notice that:

CAUTION

When using the *stacks* option (docker-compose) when passing the parameters for creating a volume, the following path must be used: `"/codesys/NextoUser/Files/docker/var-lib/"`. Otherwise, the startup of the *container* will be aborted.

5.21.4.1. Configuring a Container

5.21.4.1.1. Command & Logging Menu

The first available menu is the *Command & Logging* menu. In this initial menu, there is no need to change any parameters; however, it is recommended to activate the console configuration for *Container* that can take advantage of it.

The screenshot shows the 'Advanced container settings' dialog with the 'Command & logging' tab selected. The dialog has several tabs: 'Command & logging', 'Volumes', 'Network', 'Env', 'Labels', 'Restart policy', 'Runtime & Resources', and 'Capabilities'. The 'Command & logging' tab contains the following fields and options:

- Command:** A text input field with a 'Default' button and an 'Override' button. The value is `e.g. '-logtostderr' '--housekeeping_interval=5s' or '/usr/bin/nginx -t -c /mynginx.conf`.
- Entrypoint:** A text input field with a 'Default' button and an 'Override' button. The value is `e.g. '/bin/sh -c`.
- Working Dir:** A text input field with the value `e.g. /myapp`.
- User:** A text input field with the value `e.g. nginx`.
- Console:** Radio buttons for 'Interactive & TTY (-i -t)', 'TTY (-t)', 'Interactive (-i)', and 'None' (selected).
- Logging:** A dropdown menu for 'Driver' with the value 'Default logging driver'. A note below says: 'Logging driver that will override the default docker daemon driver. Select Default logging driver if you don't want to override it. Supported logging drivers can be found in the [Docker documentation](#).'
- Options:** A button labeled '+ add logging driver option'.

Figure 210: Command & logging Configuration Menu

5.21.4.1.2. Network Menu

The Network menu allows the configuration of the network in which this *Container* will operate. The use of network in *"Host"* mode is mandatory for the operation of the *Container*. This happens because our Docker does **not** support any other network's mode.

The screenshot shows the 'Advanced container settings' dialog with the 'Network' tab selected. The dialog has several tabs: 'Command & logging', 'Volumes', 'Network', 'Env', 'Labels', 'Restart policy', 'Runtime & Resources', and 'Capabilities'. The 'Network' tab contains the following fields and options:

- Network:** A dropdown menu with the value 'host'.
- Hostname:** A text input field with the value `e.g. web01`.
- Domain Name:** A text input field with the value `e.g. example.com`.
- Mac Address:** A text input field with the value `e.g. 12-34-56-78-9a-bc`.
- IPv4 Address:** A text input field with the value `e.g. 172.20.0.7`.
- IPv6 Address:** A text input field with the value `e.g. a:b:c:d:1234`.
- Primary DNS Server:** A text input field with the value `e.g. 1.1.1.1, 2606:4700:4700::1111`.
- Secondary DNS Server:** A text input field with the value `e.g. 1.0.0.1, 2606:4700:4700::1001`.

Figure 211: Network Configuration Menu

5.21.4.1.3. Runtime & Resources Menu

The *Runtime & Resources* menu is the most crucial among the menus present in a *Container*. In this menu, the user can configure the maximum CPU and RAM that a container can consume.

CAUTION
It is recommended that the total sum of RAM memory usage limits of all *Containers* don't surpass the 230 *MegaBytes* mark to ensure proper reserves of RAM for the PLC operation.

The figure below shows the recommended configurations for using just one *Container*:

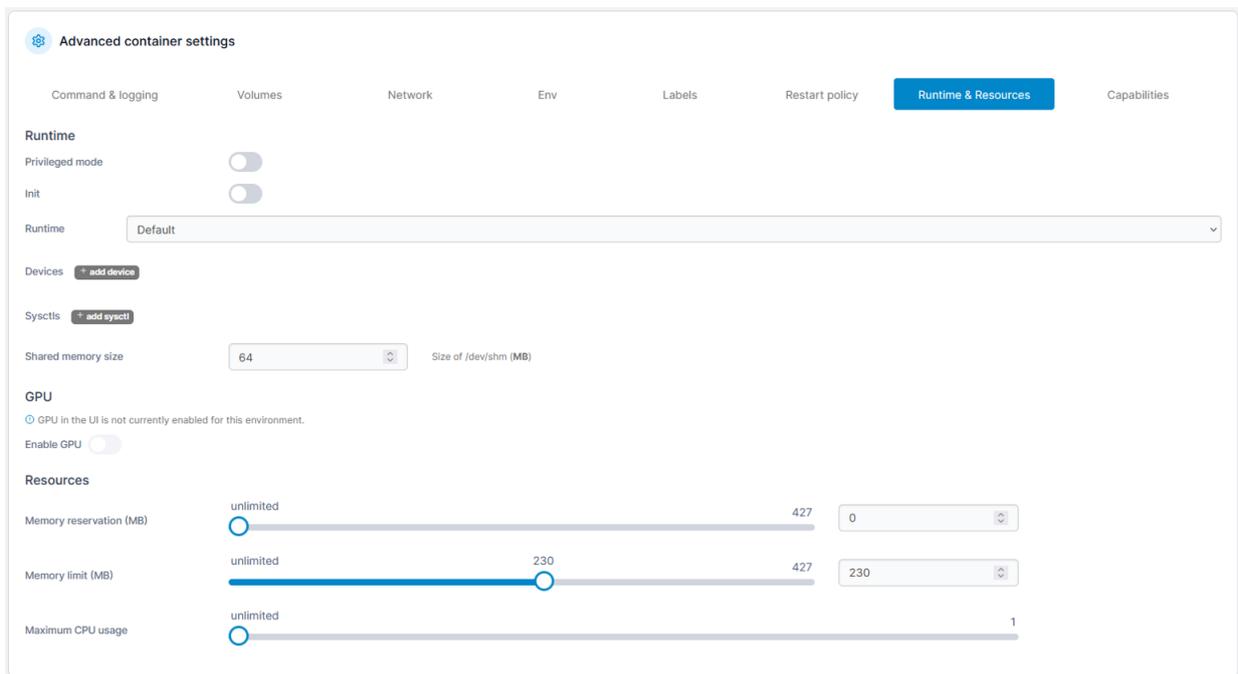


Figure 212: Runtime & Resources Configuration Menu

5.21.4.1.4. Capabilities Menu

Finally, there is the *capabilities* menu, which provides a large number of *Container* capabilities. Each one of them comes with a brief explanation of how it works, accessible through the small "(?)" symbol next to each configuration.

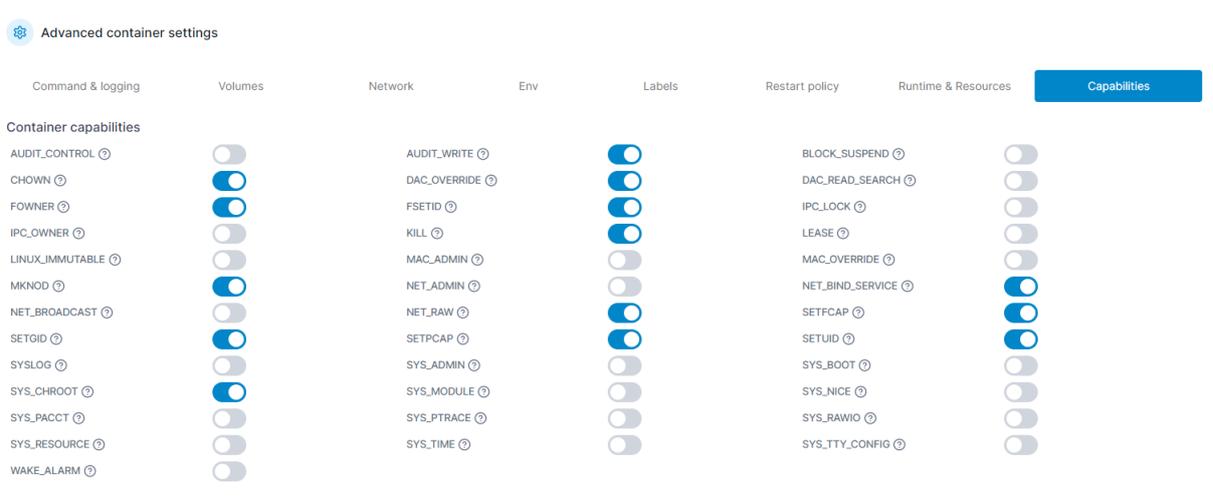


Figure 213: Capabilities Configuration Menu

CAUTION

We do not guarantee the desired system functionality in the case of activating certain parameters. Caution should be exercised when enabling or disabling sensitive capabilities.

5.21.4.2. Using a Container

As mentioned in section [How to access Portainer](#), most *Containers* can be accessed using the address “*IP.OF.YOUR.CPU:CONTAINER PORT*”, followed by a port address. One way to access a *Container* is through *Portainer* itself and in its case, the port address is “:9000”, meaning that to access it you would use “*IP.OF.YOUR.CPU:9000*”.

Once the *Container* is created, upon accessing it, two sections will be visible: an actions section and a status menu.

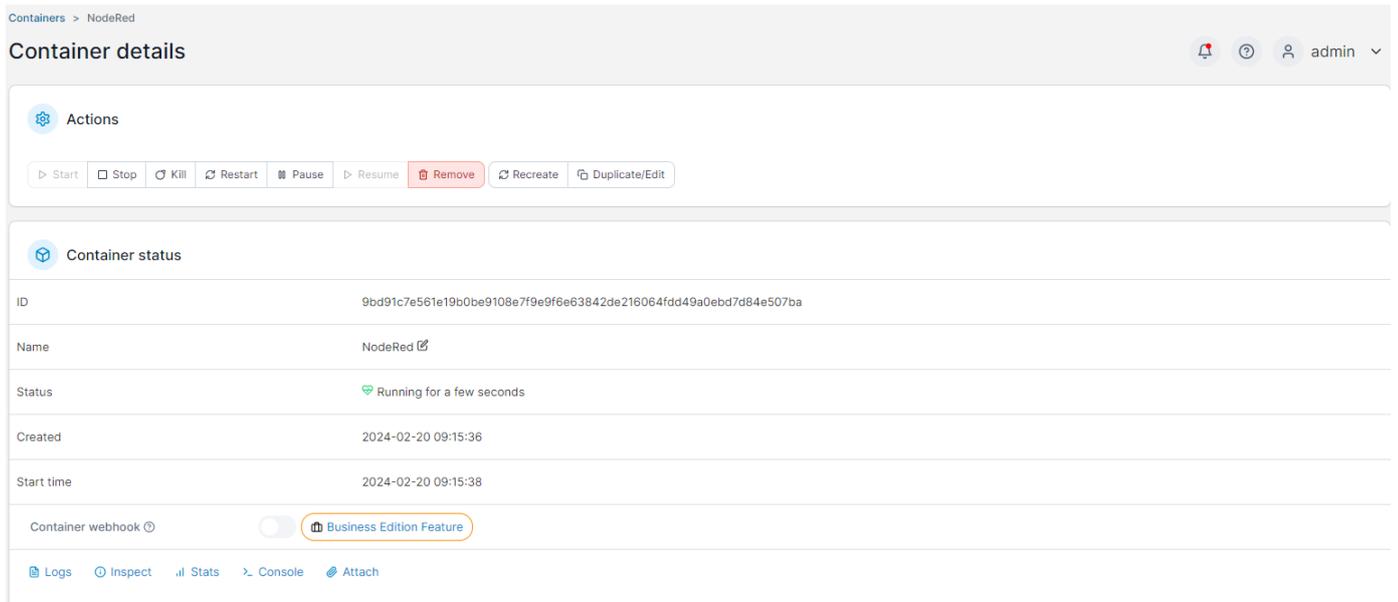


Figure 214: Container Details Table

This actions table enables the execution of some general actions that can be performed with the *Container*. The table below, called “*Container Status*”, presents some general information about the *Container*. At the end of this table, some functionalities can be accessed: The first one is the page of logs for the running *Container*, the second is a deep inspection of

parameters and configurations of the *Container*, the third provides relevant statistics of resource consumption generated during the *Container*'s operation, and the fourth is a console for interaction with the *Container* in relevant cases.

ATTENTION

You must know the type of console supported by the *Container* you are using. If the selected option is not supported, it will not be able to interact with it.

The next table is the access control table, where the owner of the *Container* can be selected.

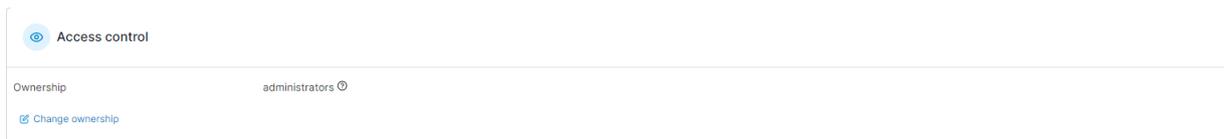


Figure 215: Access Control box

Following that is the *Container* health table, where it informs its state, failure count, and the last error code that was recorded.

The "Create Image" table allows the user to create an image of that Docker.

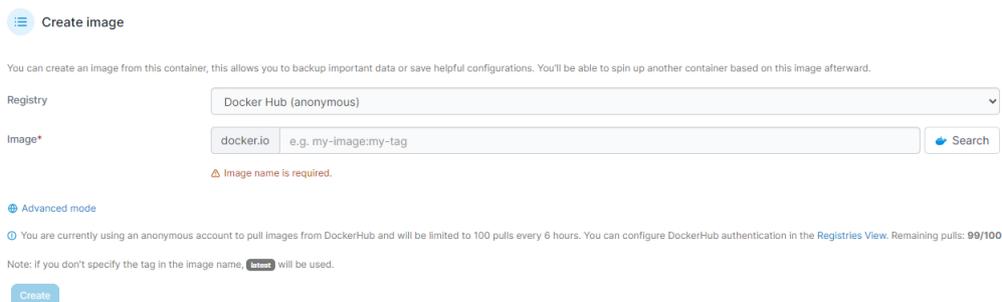


Figure 216: Create Image box Table

5.21.4.3. How to create an image of an existing container to backup its data

On the *Container Details* screen, accessed from the *Containers* menu and clicking on the *Container* name, it is possible to create an image of this container containing all the data and configurations already configured. This feature can be used to facilitate the distribution of examples, to perform backups, or to migrate the Docker application to another controller.

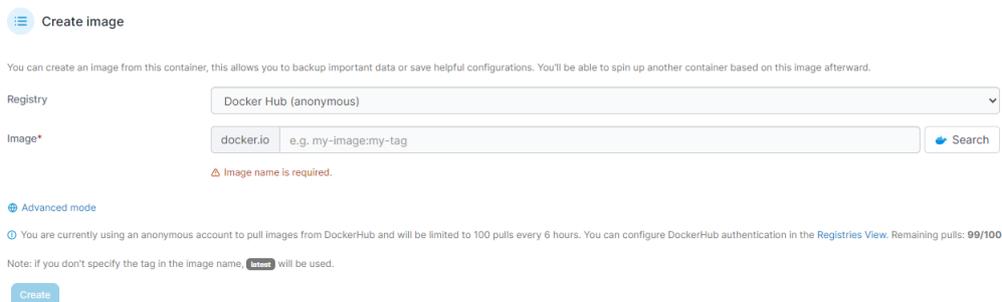


Figure 217: Creating an image of an existing Container

5.21.4.4. Monitoring a Container

To monitor a *Container*, you can use a tool within the *Portainer* itself. This tool is accessible both via the list of *Containers*, in an icon in the “*Quick Actions*” called “*Stats*” and via the “*Container Statistics*” screen. Once accessed, the user will see the menu shown in the figure below. It will be possible to see statistics on memory, CPU, and I/O consumption. The refresh rate of the memory, UCP, and I/O consumption statistics can be configured via the “*Refresh rate*” field. This tool only monitors one *Container*, and it is not possible to monitor the sum of all *Containers* via *Portainer*. However, there are CPU diagnostics that can be monitored using the *MasterTool* and are directly related to the use of the *Container*, such as the *byProcessorLoad* diagnostic, where it is possible to view the percentage of CPU processor use, and the *dwFreeSpacekB* and *dwTotalSizekB* diagnostics, which show the total amount of user memory available.

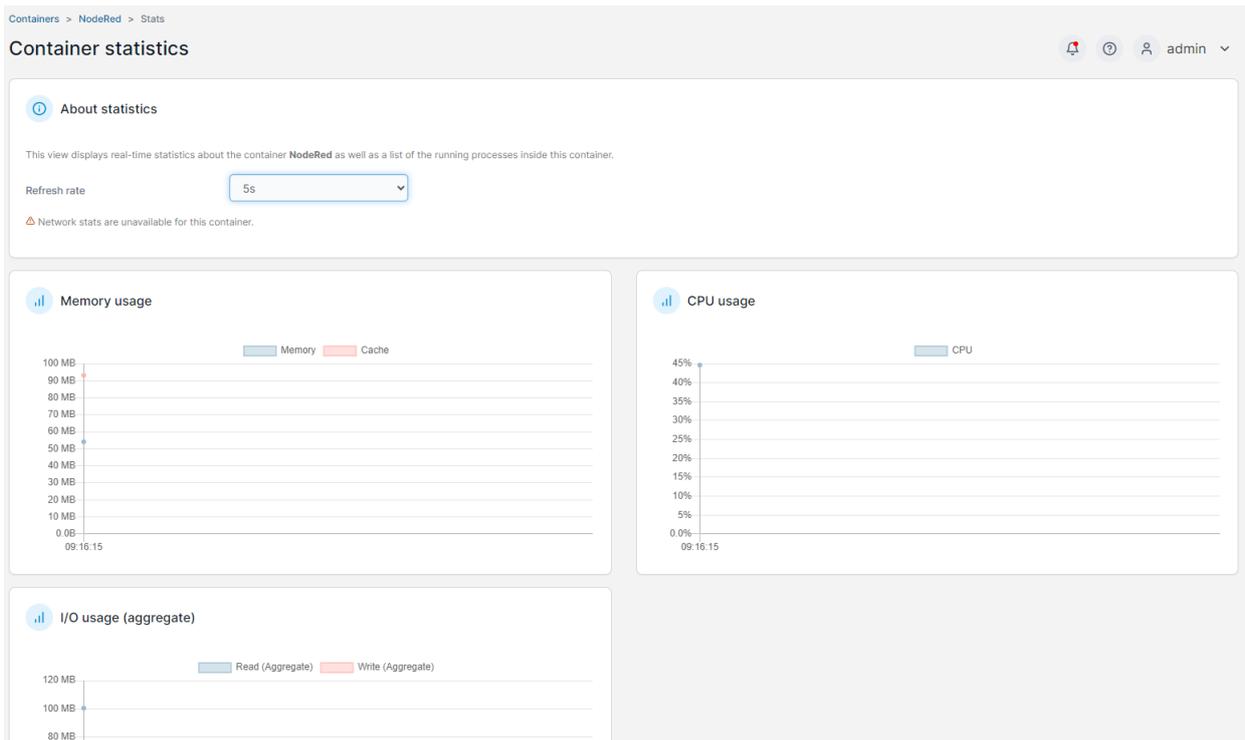


Figure 218: Stats Screen

5.21.4.5. Technical Characteristics

5.21.4.5.1. Flash Memory

The Docker *Containers* are located in the user’s storage folder, accessible via the *Files* menu of the *MasterTool*. Because Docker is stored in the user memory, the maximum storage available for both Docker and the Application is the total amount of the device’s user memory. *Containers* that use a large amount of storage can, in turn, take a long time to complete the process of obtaining the Image and deploying it.

5.21.4.5.2. RAM Memory

The Maximum RAM usage, among all Docker *Containers* **MUST** be inferior to 230 *MegaBytes*.

If an attempt is made to set a value higher than the one available, *Portainer* will display an error message. This can also result in the device malfunctioning. The option to use unlimited resources **NOT** should not be used, as this may result in the device malfunctioning.

DANGER

The memory is shared among **all** Docker *Containers* and Application. It should be carefully configured to avoid malfunctioning of the device. It is recommended that the sum of the RAM memory usage of all Docker *Containers* don’t surpass the mark of 230 *MegaBytes*.

5.21.4.5.3. CPU

The CPU limitation used by Docker should also be configured through menu mentioned in section [Runtime & Resources Menu](#). The configured value refers to the entire CPU. Therefore, if there is an application and/or *Container* consuming high processing power, this value should be modified accordingly. The device does not have a dedicated, integrated graphics processor or graphics drivers and may present instabilities in *Containers* that require this feature.

5.21.4.6. How to access the Docker’s folders

5.21.4.6.1. Mastertool

Through *MasterTool*, it is possible to check the files of Docker’s *Container* using the File access functionality under the device menu. The following image illustrates the menu and the folder that allows access to these files.

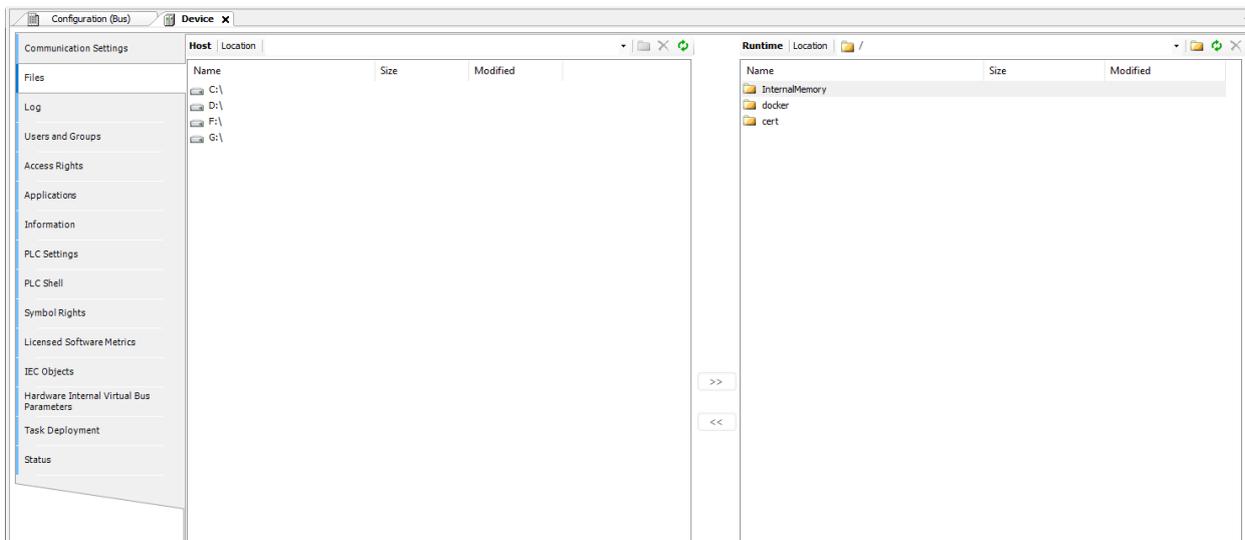


Figure 219: Docker’s Folder in MasterTool

5.21.4.7. Using External Memory as Docker Volumes

To expand Docker’s storage capacity using external memory devices like SD cards and USB flash drives, you must use volumes to mount the external file systems into the containers. This process is only supported via Portainer Stacks (Docker Compose).

Use the following host paths to configure volumes in your stack file:

External Device	Host Path
SD Card	/codesys/NextoUser/Files/MemoryCard
USB Mass Storage	/codesys/NextoUser/Files/Mass_Storage

Table 199: Host paths for external memory devices

To create a Docker Stack that uses external memory, you must configure volumes to mount the physical device paths into your container. This allows containerized services to access files on the external storage.

To deploy a new stack, navigate to the Stacks section in Portainer and click Add Stack. The [Figure 220](#) shows an example of a stack file that mounts both an SD card and a USB flash drive to a service:

The screenshot shows the Portainer.io 'Create stack' interface. The 'Name' field is set to 'mystack'. Below the name, it states 'This stack will be deployed using docker compose.'. There are two build method options: 'Web editor' (selected with a checkmark) and 'Upload' (with a radio button). The 'Web editor' section contains a text area with the following Docker Compose file content:

```

1 version: '3.8'
2 services:
3   my_service:
4     image: my_image
5     volumes:
6       - /codesys/NextoUser/Files/MemoryCard:/data/sd_card
7       - /codesys/NextoUser/Files/Mass_Storage:/data/usb_drive
8

```

Figure 220: Stack File Example for External Memory Devices

ATTENTION

If the external device is not mounted during the container's startup, the container will not be able to access the files on that device. Ensure that the external memory devices are properly mounted before starting the containers. In the same way, if the external device is removed while the container is running, the container will lose access to the files on that device, needing to be restarted to regain access.

5.21.4.8. Troubleshooting

This section aims to describe the most common problems, their causes and solutions.

5.21.4.8.1. Container Installation Failure due to expired or not valid Certificate

Cause: PLC time is invalid.

Solution: Adjust the PLC time.

5.21.4.8.2. Portainer is inaccessible, returning after CPU reboot

Cause: Container memory limits were not applied as per section [Runtime & Resources Menu](#)

Solution: Apply the memory limits as described in this manual.

6. Maintenance

One feature of the Nexto Series is the abnormality diagnostic generation, whether they are failures, errors or operation modes, allowing the operator to identify and solve problems which occurs in the system easily.

The Nexto CPUs permit many ways to visualize the diagnostics generated by the system, which are:

- [One Touch Diag](#)
- [Diagnostics via LED](#)
- [Diagnostics via System Web Page](#)
- [Diagnostics via Variables](#)
- [Diagnostics via Function Blocks](#)

The first one is an innovating feature of Nexto Series, which allows a fast access to the application abnormal conditions. The second is purely visual, generated through two LEDs placed on the panel (DG and WD) and also through the LEDs placed in the RJ45 connector (exclusive for Ethernet connection). The next feature is the graphic visualization in a WEB page of the rack and the respective configured modules, with the individual access allowed of the operation state and the active diagnostics. The diagnostics are also stored directly in the CPU variables, either direct representation (%Q) or attributed (AT variable), and can be used by the user application, for instance, being presented in a supervisory system. The last ones present specific conditions of the system functioning.

These diagnostics function is to point possible system installation or configuration problems, and communication network problems or deficiency.

6.1. Module Diagnostics

6.1.1. One Touch Diag

The One Touch Diag (OTD), or single touch diagnostics, is an exclusive feature the Nexto Series brings for the programmable controllers. With this new concept the user can verify the diagnostics of any module connected to the system straight on the CPU graphic display with a single touch on the module Diagnostic Switch. This is a powerful diagnostic tool which can be used offline (with no need of supervisory or programming software) making easier to find and solve quickly possible problems.

The diagnostics key is placed on the CPU upper part, in an easy access place and, besides giving active diagnostics, allows the access to the navigation menu, described in the [Configuration – CPU's Informative and Configuration Menu](#) section.

The figure below shows the CPU switch placement:

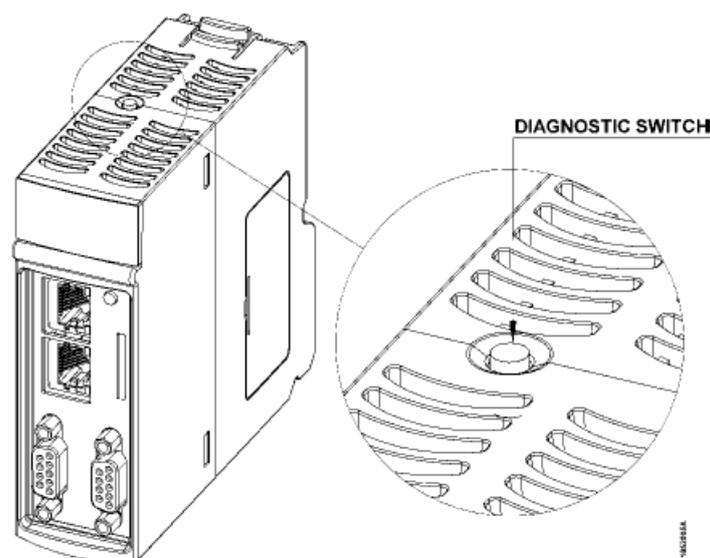


Figure 221: Diagnostic Switch

With only a short touch, the CPU starts to show the bus diagnostics (when active, otherwise shows the “NO DIAG” message). Initially, the Tag is visualized (configured in the module properties in the MasterTool IEC XE software, following

the IEC 61131-3 standard), in other words, the name attributed to the CPU, and after that all diagnostics are shown, through CPU display messages. This process is executed twice on the display. Everything occurs automatically as the user only has to execute the first short touch and the CPU is responsible to show the diagnostics. The diagnostics of other modules present on the bus are also shown on the CPU graphic display by a short press in the diagnostic module button, in the same presentation model of diagnostics.

The figure below shows the process starting with the short touch, with the conditions and the CPU times presented in smaller rectangles. It is important to stress the diagnostics may have more than one screen, in other words, the specified time in the block diagram below is valid for one of them.

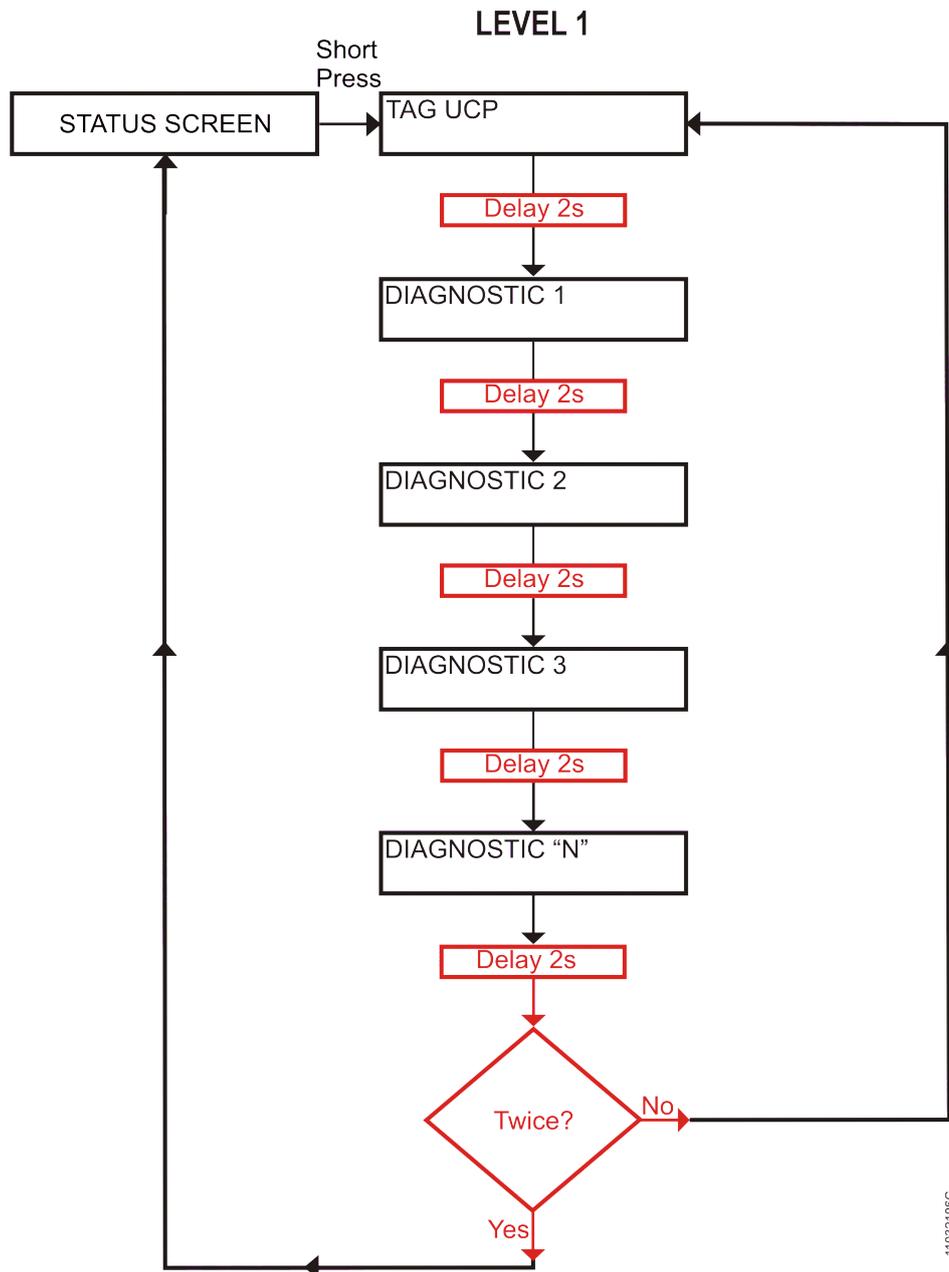


Figure 222: CPU Diagnostics Visualization

Before all visualization process be concluded, it is just to give a short touch on the diagnostic switch, at any moment, or press the diagnostic switch from any I/O module connected to the bus. Also, it is important to observe that the One Touch Diag could be available when the module could be in Operational Mode.

In case a long touch is executed, the CPU goes to navigation menu, which is described in the [Configuration – CPU’s Informative and Configuration Menu](#) section.

The table below shows the difference between the short touch time, the long touch time and stuck button.

Touch type	Minimum time	Maximum time	Indication condition
No touch	-	59.99 ms	-
Short touch	60 ms	0.99 s	Release
Long touch	1 s	20 s	More than 1 s till 20 s
Locked Switch	20.01 s	(∞)	Diagnostics indication, see on Table 205

Table 200: One Touch Time

The messages presented on the Nexto CPU graphic display, correspondent to the diagnostics, are described in the [Diagnostics via Variables](#) section, on Table 205.

If any situation of stuck button occur in one of the I/O modules, the diagnostic button of this module will stop of indicate the diagnostics on CPU graphic display when is pressed. In this case, the CPU will indicate that there is a module with active diagnostics. To remove this diagnostic from the CPU, a hot swap must be done in the module where the diagnostic is active.

For further details on the procedure for viewing the diagnostics of the CPU or other bus modules, see description in the User Manual Nexto Series – MU214600.

6.1.2. Diagnostics via LED

This product have a LED for diagnostic indication (LED DG) and a LED for watchdog event indication (LED WD). The Tables 201 and 202 show the meaning of each state and its respective descriptions.

6.1.2.1. DG (Diagnostic)

Green	Red	Description	Causes	Priority
Off	Off	Not used	No power supply. Hardware problem	-
On	Off	All applications in execution mode (Run)	-	3 (Low)
Off	On	All applications in stopping mode (Stop)	-	3 (Low)
Blinking 2x	Off	Bus modules with diagnostic	At least, a bus module, including the CPU, is with an active diagnostic	1
Blinking 3x	Off	Data forcing	Some memory area is being forced by the user through Master-Tool IEC XE	2
Off	Blinking 4x	Configuration or hardware error in the bus	The bus is damaged or is not properly configured	0 (High)

Table 201: Description of the Diagnostic LEDs States

6.1.2.2. WD (Watchdog)

Red LED	Description	Causes	Priority
Off	No watchdog indication	Normal operation	3 (Low)
Blinking 1x	Software watchdog	User application watchdog	2
On	Hardware watchdog	Damaged module and/or corrupted operational system	1 (High)

Table 202: Description of the Watchdog LED States

Notes:

Software Watchdog: In order to remove the watchdog indication, make an application reset or turn off and turn on the CPU again. This watchdog occurs when the user application execution time is higher than the configured watchdog time.

The diagnostics can be checked in the Exception.wExceptionCode variable, see on Table 209.

Hardware Watchdog: In order to reset any watchdog indication, as in the WD LED or in the Reset.bWatchdogReset operand, the module must be disconnected from the power supply.

In order to verify the application conditions in the module restart, see configurations on Table 39.

6.1.2.3. RJ45 Connector LEDs

Both LEDs placed in the RJ45 connectors, help the user in the installed physical network problem detection, indicating the network Link speed and the existence of interface communication traffic. The LEDs meaning is presented on table below.

Yellow	Green	Description
○	○	Network LINK absent
○	●	1000 Mbytes/s network LINK
●	○	100 Mbytes/s network LINK
●	●	10 Mbytes/s network LINK
X	-	Ethernet network transmission or reception occurrence, for or to this IP address. Blinks on Nexto CPU demand and not every transmission or reception, in other words, it may blink on a lower frequency than the real transmission or reception frequency.

Table 203: Ethernet LEDs Meaning

6.1.3. Diagnostics via System Web Page

Besides the previously presented features, the Nexto Series brings to the user an innovating access tool to the system diagnostics and operation states, through a System Web Page.

The utilization, besides being dynamic, is very intuitive and facilitates the user operations. The use of a supervisory system can be replaced when it is restricted to system status verification.

To access the desired CPU's System Web Page, it is just to use a desktop browser and type, on the address bar, the CPU IP address (Ex.: <http://192.168.1.1>). First, the CPU information is presented, according to Figure 223:



Figure 223: Initial Screen

There is also the *Bus Information* tab, which can be visualized through the Rack or the present module list (option on the screen right side). While there is no application on the CPU, this page will display a configuration with the largest available rack and a standard power supply, connected with the CPU. When the Rack visualization is used, the modules that have diagnostics blink and assume the red color, as shown on Figure 224. Otherwise a list with the system connected modules, Tags and active diagnostics number is presented:

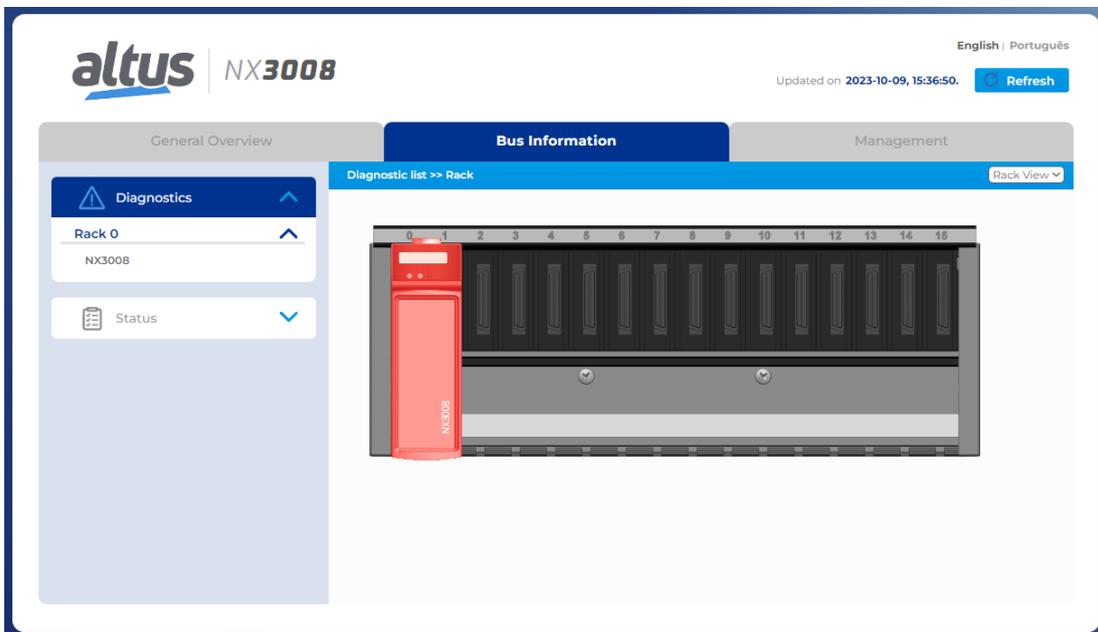


Figure 224: System Information

When the module with diagnostics is pressed, the module active(s) diagnostic(s) are shown, as illustrated on Figure 225:

ATTENTION

When a CPU is restarted and the application goes to exception in the system's startup, the diagnostics will not be valid. It is necessary to fix the problem which generates the application's exception so that the diagnostics are updated.

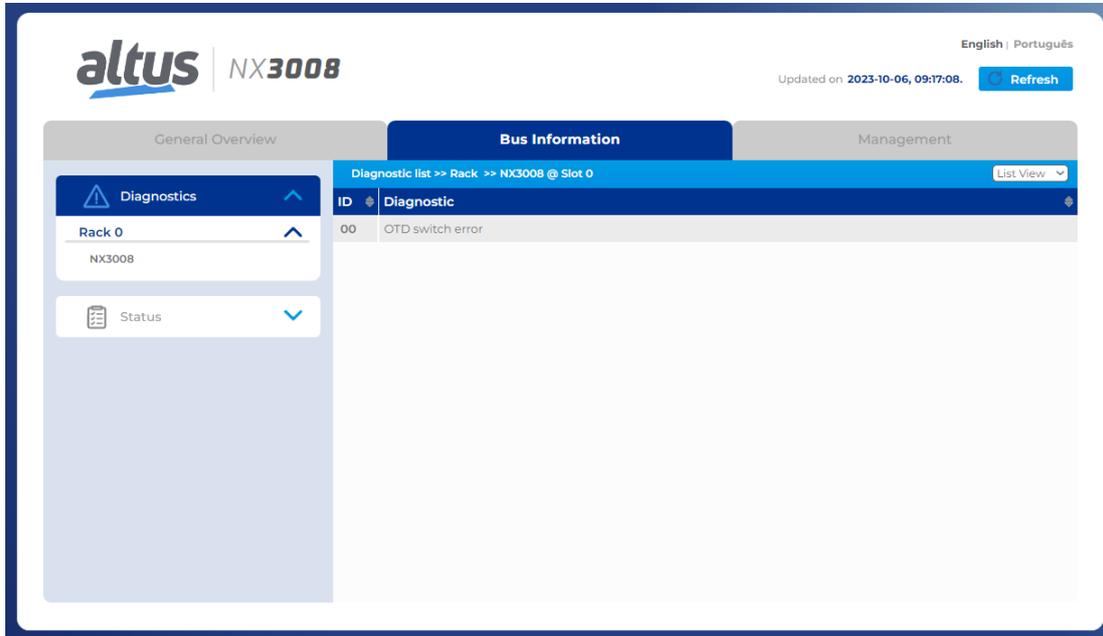


Figure 225: System Diagnostics

In case the Status tab is selected, the state of all detailed diagnostics is shown on the screen, as illustrated on Figure 226:

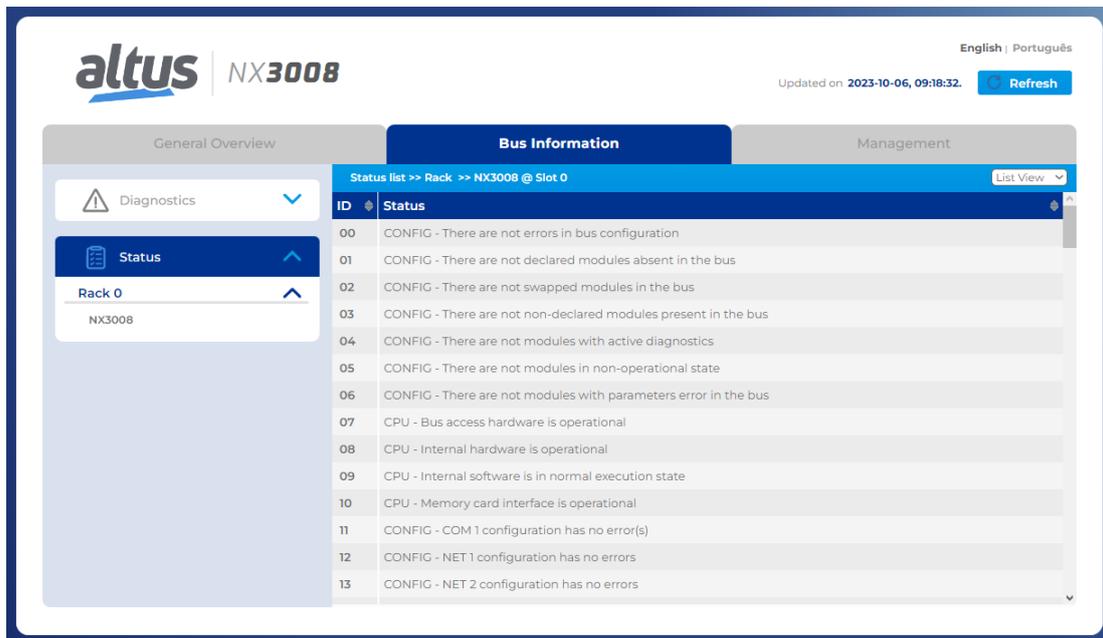


Figure 226: System Status

The user can choose to visualize two language options: Portuguese and English. Simply change in the upper right part of the screen to the desired language.

6.1.4. Diagnostics via Variables

The Nexto Series CPUs have many variables for diagnostic indication. There are data structures with the diagnostics of all modules declared on the bus, mapped on the variables of direct representation %Q, and defined symbolically through the AT directive, in the GVL System_Diagnostics created automatically by the MasterTool IEC XE.

The table below summarizes the diagnostic byte/words division:

Byte	Description
0 to 3	CPU summarized diagnostics.
4 to 1686	CPU detailed diagnostics.

Table 204: CPU Diagnostics Division

6.1.4.1. Summarized Diagnostics

The table below shows the meaning of each CPU summarized diagnostic bit:

Diagnostics Message	DG_Module.tSummarized.*	Description
NO DIAG	-	There is no active diagnostic.
CONFIG. MISMATCH	bConfigMismatch	TRUE – There is a configuration problem in the bus, as the module inserted in the wrong position.
		FALSE – The bus is configured correctly.
ABSENT MODULES	bAbsentModules	TRUE – One or more declared modules are absent.
		FALSE – All declared modules were detected in the bus.
SWAPPED MODULES	bSwappedModules	TRUE – There are changed modules in the bus.
		FALSE – There are no changed modules in the bus.
NON-DECLARED MODULES	bNonDeclaredModules	TRUE – One or more modules in the bus were not declared in the configuration.
		FALSE – All modules were declared.
MODULES W/ DIAGNOSTICS	bModulesWithDiagnostic	TRUE – One or more modules in the bus are with active diagnostic.
		FALSE – There is no active diagnostic in the modules in the bus.
MODULES W/ FATAL ERROR	bModuleFatalError	TRUE – One or more modules in the bus are in fatal error.
		FALSE – All modules are working properly.
MODULES W/ PARAM. ERROR	bModuleParameterError	TRUE – One or more modules in the bus have parameterization error.
		FALSE – All modules are parameterized.
BUS ERROR	bWHSBBusError	TRUE – Master indication there is failure in the WHSB bus.
		FALSE – The WHSB bus is working properly.
HARDWARE FAILURE	bHardwareFailure	TRUE – CPU hardware failure.
		FALSE – The hardware is working properly.
SOFTWARE EXCEPTION	bSoftwareException	TRUE – One or more exceptions generated by the software.
		FALSE – No exceptions generated in the software.
ERROR IN MEMORY CARD	bMemoryCardError	TRUE – The memory card is inserted in the CPU, but is not working properly.
		FALSE – The memory card is working properly.
COM1 CONF. ERROR	bCOM1ConfigError	TRUE – Some error occurred during, or after, the COM 1 serial interface configuration.

Diagnostics Message	DG_Module.tSummarized.*	Description
		FALSE – The COM 1 serial interface configuration is correct.
NET1 CONF. ERROR	bNET1ConfigError	TRUE – Some error occurred during, or after, the NET 1 Ethernet interface configuration.
		FALSE – The NET 1 Ethernet interface configuration is correct.
NET2 CONF. ERROR	bNET2ConfigError	TRUE – Some error occurred during, or after, the NET 2 Ethernet interface configuration.
		FALSE – The NET 2 Ethernet interface configuration is correct.
NET3 CONF. ERROR	bNET3ConfigError	TRUE – Some error occurred during, or after, the NET 3 Ethernet interface configuration.
		FALSE – The NET 3 Ethernet interface configuration is correct.
INVALID DATE/TIME	bInvalidDateTime	TRUE – The date or hour are invalid.
		FALSE – The date and hour are correct.
RUNTIME RESET	bRuntimeReset	TRUE – The RTS (Runtime System) has been restarted at least once. This diagnostics is only cleared in the system restart.
		FALSE – The RTS (Runtime System) is operating normally.
RETENTIVITY LOST	bRetentivityLost	TRUE - An error occurred while saving the retentive data.
		FALSE - Retentive data are being saved successfully.
OTD SWITCH ERROR	bOTDSwitchError	TRUE – True in case the OTD key has been locked for more than 20 s at least once while the CPU was energized. This diagnostic is only cleared in the system restart.
		FALSE – The key is not currently locked or was locked while the CPU was energized.
WRONG CPU SLOT	bWrongCPUSlot	TRUE - The CPU is plugged on a slot different to the declared in user application.
		FALSE - The CPU is properly plugged on slot declared in user application.
USB PORT ERROR	bUSBDiagnostic	TRUE - The USB has some diagnostics.
		FALSE - The USB is without problems.
ABSENT RACK	bAbsentRacks	TRUE – One or more declared racks are absent.
		FALSE – There are no absent racks.
DUPLICATED RACK	bDuplicatedRacks	TRUE – There are racks with a duplicated identification number.
		FALSE – There are no racks with a duplicated identification number.
INVALID RACK	bInvalidRacks	TRUE – There are racks with an invalid identification number.
		FALSE – There are no racks with an invalid identification number.
NON DECLARED RACK	bNonDeclaredRacks	TRUE – There are racks with a non-declared identification number.
		FALSE – There are no racks with a non-declared identification number.
DUPLICATED SLOT	bDuplicatedSlots	TRUE – There are some duplicated slot address.
		FALSE – There are no duplicated slot address.

Table 205: CPU Summarized Diagnostics

Notes:

Configuration Mismatch: The incompatible configuration diagnostic is generated if one or more modules of the rack does not correspond to the declared one, so, in the absence or different modules conditions. The modules inserted in the bus

that were not declared in the project are not considered.

Swapped Modules: If only two modules are changed between themselves in the bus, then changed diagnostic can be identified. Otherwise, the problem is treated as “Configuration Mismatch”.

Modules with Fatal Error: In case the modules with fatal error diagnostic is true, it must be verified which is the problematic module in the bus and send it to Altus Technical Assistance, as it has hardware failure.

Module with Parameterization Error: In case the parameterization error diagnostic is true, it must be verified the module in the bus are correctly configured and if the firmware and MasterTool IEC XE software version are correct. If the problem occurred when inserting a module on the bus, make sure the module supports hot swapping.

Bus Error: Considered a fatal error, interrupting the access to the modules in the bus. In case the bus error diagnostic is true, there might be a hardware problem on the bus communication lines, then, contact Altus Technical Assistance.

Hardware Failure: In case the Hardware Failure diagnostic is true, the CPU must be sent to Altus Technical Assistance, as it has problems in the RTC, auxiliary processor, or other hardware resources.

Software Exception: In case the software exception diagnostic is true, the user must verify his application to guarantee it is not accessing the memory wrongly. If the problem remains, the Altus Technical Support sector must be consulted. The software exception codes are described next in the CPU detailed diagnostics table.

Diagnostic Message: The diagnostics messages can be visualized by the CPU graphic display using the OTD key or using the System Web Page, through the Bus Information tab.

6.1.4.2. Detailed Diagnostics

The tables below contain Nexto Series’ CPUs detailed diagnostics. It is important to have in mind the observations below before consulting them:

- **Visualization of the Diagnostics Structures:** The Diagnostics Structures added to the Project can be seen at the item “*Library Manager*” of MasterTool tree view. There, it is possible to see all data types defined in the structure.
- **Counters:** All CPU diagnostics counters return to zero when their limit value is exceeded.
- *DG_Module*, where the word Module must be replaced by the product being used.

6.1.4.2.1. Target Detailed Diagnostics Group

DG_Module.tDetailed.Target.*	Size	Description
dwCPUModel	DWORD	CPU model.
abyCPUVersion	BYTE ARRAY(4)	Firmware version.
abyBootloaderVersion	BYTE ARRAY(4)	Bootloader version.
abyAuxprocVersion	BYTE ARRAY(4)	Auxiliary processor version.
abyPowprocVersion	BYTE ARRAY(4)	Power processor version.

Table 206: Target Detailed Diagnostics Group Description

6.1.4.2.2. Hardware Detailed Diagnostics Group

DG_Module.tDetailed.Hardware.*	Size	Descrição
bRTCFailure	BIT	The main processor is not enabled to communicate with the RTC (CPU’s clock).
bThermometerFailure	BIT	Failure in the communication between the thermometer and the main processor.
bNoBusSupplyStatus	BIT	The CPU’s integrated power supply is not supplying the bus I/O modules. An additional power supply module, such as the NX8000, must be used for this.

Table 207: Hardware Detailed Diagnostics Group Description

6.1.4.2.3. Exception Detailed Diagnostics Group

DG_Module.tDetailed.Exception.*	Size	Description
wExceptionCode	WORD	Exception code generated by the RTS. See Table 209.
byProcessorLoad	BYTE	Level, in percentage (%), of charge in the processor.

Table 208: Exception Detailed Diagnostics Group Description

Note:

Exception Code: the code of the exception generated by the RTS (Runtime System) can be consulted below:

Code	Description	Code	Description
0x0000	There is no exception code.	0x0051	Access violation.
0x0010	Watchdog time of the IEC task expired (Software Watchdog).	0x0052	Privileged instruction.
0x0012	I/O configuration error.	0x0053	Page failure.
0x0013	Checksum error after the program download.	0x0054	Stack overflow.
0x0014	Fieldbus error.	0x0055	Invalid disposition.
0x0015	I/O updating error.	0x0056	Invalid maneuver.
0x0016	Cycle time (execution) exceeded.	0x0057	Protected page.
0x0017	Program online updating too long.	0x0058	Double failure.
0x0018	External references not resolved.	0x0059	Invalid OpCode.
0x0019	Download rejected.	0x0100	Data type misalignment.
0x001A	Project not loaded, as the retentive variables cannot be reallocated.	0x0101	Arrays limit exceeded.
0x001B	Project not loaded and deleted.	0x0102	Division by zero.
0x001C	Out of memory stack.	0x0103	Overflow.
0x001D	Retentive memory is corrupted and cannot be mapped.	0x0104	Cannot be continued.
0x001E	Project can be loaded but causes a drop later on.	0x0105	Watchdog in the processor load of all IEC task detected.
0x0021	Target of startup application does not match to the current target.	0x0150	FPU: Not specified error.
0x0022	Scheduled tasks error.	0x0151	FPU: Operand is not normal.
		0x0152	FPU: Division by zero.
0x0023	Downloaded file Checksum with error.	0x0153	FPU: Inexact result.
0x0024	Retentive identity is not correspondent to the current identity of the boot project program	0x0154	FPU: Invalid operation.
0x0025	IEC task configuration failure.	0x0155	FPU: Overflow.
0x0026	Application working with wrong target.	0x0156	FPU: Stack verification.
0x0050	Illegal instruction.	0x0157	FPU: Underflow.

Table 209: RTS Exception codes

6.1.4.2.4. WebVisualization Detailed Diagnostics Group

DG_Module.tDetailed.WebVisualization.*	Size	Description
byConnectedClients	BYTE	Clients number connected to the WebVisualization.

Table 210: WebVisualization Detailed Diagnostics Group Description

6.1.4.2.5. RetainInfo Detailed Diagnostics Group

DG_Module.tDetailed.RetainInfo.*	Size	Descrição
byCPUInitStatus	BYTE	CPU Startup Status: 01: Not used 02: Warm Start 03: Cold Start Note: These variables are reset in every powerup.
wCPUColdStartCounter	WORD	Increments when the CPU starts with loss of retentivity. (0 to 65535)
wCPUWarmStartCounter	WORD	Increments when the CPU starts normally with valid retain data. (0 to 65535)
wRTSResetCounter	WORD	Counter of resets performed by RTS (Runtime System). (0 to 65535).

Table 211: RetainInfo Group Detailed Diagnostics

6.1.4.2.6. Reset Detailed Diagnostics Group

DG_Module.tDetailed.Reset.*	Size	Description
bBrownOutReset	BIT	The CPU was restarted due a failure in the power supply in the last startup.
bWatchdogReset	BIT	The CPU was restarted due the active watchdog in the last startup.

Table 212: Reset Detailed Diagnostics Group Description

Note:

Brownout Reset: The brownout reset diagnostic is only true when the power supply exceed the minimum limit required in its technical characteristics, remaining in low-voltage, i.e. without undergoing any interrupt. The CPU will identify the drop in supply and will indicate the power failure diagnostic. When the voltage is reestablished, the CPU will automatically reset and will indicate the brownout reset diagnostic.

6.1.4.2.7. Thermometer Detailed Diagnostics Group

DG_Module.tDetailed.Thermometer.*	Size	Description
bOverTemperatureAlarm	BIT	Alarm generated due internal temperature at 85 °C or above it.
bUnderTemperatureAlarm	BIT	Alarm generated due internal temperature at 0 °C or under it.
diTemperature	DINT	Temperature read in the internal sensor of the CPU.

Table 213: Thermometer Detailed Diagnostics Group Description

Note:

Temperature: In order to see the temperature directly in the memory address, a conversion must be made, since the data size is DINT and monitoring is done in 4 bytes. Therefore, it's recommended to use the associated symbolic variable, because it already provides the final temperature value.

6.1.4.2.8. Serial Detailed Diagnostics Group

DG_Module.tDetailed.Serial.COM1.*	Size	Description
byProtocol	BYTE	Protocol selected in the COM 1: 00: Without protocol 01: MODBUS RTU Master 02: MODBUS RTU Slave 03: Other protocol
dwRXBytes	DWORD	Counter of characters received from COM 1 (0 to 4294967295).
dwTXBytes	DWORD	Counter of characters transmitted from COM 1 (0 to 4294967295).
wRXPendingBytes	WORD	Number of characters left in the reading buffer in COM 1 (0 to 1024).
wTXPendingBytes	WORD	Number of characters left in the transmission buffer in COM 1 (0 to 1024).
wBreakErrorCounter	WORD	The transmitter is holding the data line at zero for too long, according to the databit configured.
wParityErrorCounter	WORD	The received frame has the mismatched parity bit.
wFrameErrorCounter	WORD	The received frame has the wrong start point, usually caused by a noise or baud rate mismatch.
wRXOverrunCounter	WORD	When the receive ring buffer is full and starts to lose the old frames (too many frames not treated by the device).

Table 214: Serial COM 1 Detailed Diagnostics Group Description

Note:

Parity Error Counter: When the serial COM 1 is configured Without Parity, this error counter won't be incremented when it receives a message with a different parity. In this case, a frame error will be indicated.

6.1.4.2.9. CAN Detailed Diagnostics Group

DG_Module.tDetailed.CAN.*	Size	Description
bBusAlarm	BIT	The bus has a critical error and is off.
byBusState	BYTE	Reports the device status.
udiTxCounter	UDINT	Number of packets (Tx) changed on the CAN bus of the CPU.
udiRxCounter	UDINT	Number of packets (Rx) changed on the CAN bus of the CPU.
udiTxErrorCounter	UDINT	Number of packets (Tx) with errors on the CPU CAN bus.
udiRxErrorCounter	UDINT	Number of packets (Rx) with errors on the CPU CAN bus.
udiLostCounter	UDINT	Number of packets lost on the CAN bus of the CPU.

Table 215: CAN Detailed Diagnostics Group Description

6.1.4.2.10. USB Detailed Diagnostics Group

DG_Module.tDetailed.USB.*	Size	Description
byUSBDevice	BYTE	Type of device connected to the USB port.
bOvercurrent	BIT	The device connected to the USB port is drawing more current than supported.
bEnable	BIT	The USB port is enabled.
tMassStorage.byMountState	BYTE	Reports the device status.
tMassStorage.dwFreeSpaceKb	DWORD	Reports the free space on the mass storage device.
tMassStorage.dwTotalSizeKb	DWORD	Reports the total size of the mass storage device.

DG_Module.tDetailed.USB.*	Size	Description
tSerialConverter.dwRXBytes	DWORD	Received character counter on COM 10 (0 to 4294967295).
tSerialConverter.dwTXBytes	DWORD	Counter of characters transmitted by COM 10 (0 to 4294967295).
tSerialConverter.wRXPendingBytes	WORD	Number of characters remaining in the read buffer on COM 10 (0 to 4095).
tSerialConverter.wTXPendingBytes	WORD	Number of characters remaining in the transmit buffer on COM 10 (0 to 1023).
tSerialConverter.wBreakErrorCounter	WORD	The transmitter is holding the data line at zero for too long, according to the databit configured.
tSerialConverter.wParityErrorCounter	WORD	The received frame has the mismatched parity bit.
tSerialConverter.wFrameErrorCounter	WORD	The received frame has the wrong start point, usually caused by a noise or baud rate mismatch.
tSerialConverter.wRXOverrunCounter	WORD	When the receive ring buffer is full and starts to lose the old frames (too many frames not treated by the device).
tModem.bConfigured	BOOL	Indicates that the modem has been configured on the web page.
tModem.byConnectionState	BYTE	Modem connection status.
tModem.szIP	STRING (15)	String with the IP address used by the modem.
tWifiAdapter.bConfigured	BOOL	Indicates that the WiFi adapter has been configured on the web page.
tWifiAdapter.byConnectionState	BYTE	Connection status of the WiFi adapter.
tWifiAdapter.szIP	STRING (15)	String with the IP address used by WiFi.
tWifiAdapter.szMask	STRING (15)	String with the Mask used by WiFi.
tWifiAdapter.szGateway	STRING (15)	String with the Gateway used by WiFi.
tWifiAdapter.szMAC	STRING (17)	String with the MAC address of the WiFi adapter (unique to the device).

Table 216: USB Detailed Diagnostics Group Description

6.1.4.2.11. Ethernet Detailed Diagnostics Group

DG_Modulo.tDetailed.Ethernet.*	Tamanho	Descrição
NET[x].bLinkDown	BIT	Indicates link state on NET[x].
NET[x].byOperatingMode	BYTE	Indicates the operating mode of the interface NET[x].
NET[x].byOperatingState	BYTE	Indicates the operating state of the interface NET[x].
NET[x].szIP	STRING (15)	NET[x] IP Address.
NET[x].szMask	STRING (15)	NET[x] Subnet Mask.
NET[x].szGateway	STRING (15)	NET[x] Gateway Address.
NET[x].szMAC	STRING (17)	NET[x] MAC Address.
NET[x].abyIP	BYTE ARRAY(4)	NET[x] IP Address.
NET[x].abyMask	BYTE ARRAY(4)	NET[x] Subnet Mask.
NET[x].abyGateway	BYTE ARRAY(4)	NET[x] Gateway Address.
NET[x].abyMAC	BYTE ARRAY(6)	NET[x] MAC Address.
NET[x].NICTeaming	WORD	Information about the NICTeaming status of the NET[x] port.
NET[x].dwTransmittedBytes	DWORD	Counter of bytes sent via the NET[x] port (0 to 4294967295).
NET[x].dwTransmittedPackets	DWORD	Counter of packets sent via the NET[x] port (0 to 4294967295).
NET[x].dwTransmittedDropErrors	DWORD	Connection loss counter on transmission over the NET[x] port (0 to 4294967295).
NET[x].dwTransmittedCollisionErrors	DWORD	Transmission collision error counter over NET[x] port (0 to 4294967295).
NET[x].dwReceivedBytes	DWORD	Counter of bytes received via the NET[x] port (0 to 4294967295).
NET[x].dwReceivedPackets	DWORD	Counter of packets received via NET[x] port (0 to 4294967295).
NET[x].dwReceivedDropErrors	DWORD	Connection loss counter on reception via the NET[x] port (0 to 4294967295).

DG_Modulo.tDetailed.Ethernet.*	Tamanho	Descrição
NET[x].dwReceivedFrameErrors	DWORD	Frame error counter on reception over NET[x] port (0 to 4294967295).

Table 217: Diagnósticos Detalhados Grupo Ethernet NET[x]

Note:

[x] is the ethernet interface number of the CPU, where for example, NET 1 represents the value 1.

DG_Modulo.tDetailed.Ethernet.RSTP.*	Size	Description
RSTP[x].bProtocolEnabled	BIT	Indicates if the RSTP protocol is enabled.
RSTP[x].bBridgeIsRoot	BIT	Indicates if the Bridge is root.
RSTP[x].eProtocol	BYTE	Indicates the protocol version.
RSTP[x].sBridgeId	STRING (22)	Local bridge ID (priority and MAC).
RSTP[x].sRootId	STRING (22)	Root bridge ID (priority and MAC).
RSTP[x].eRootPort	BYTE	Indicates which is the root port.
RSTP[x].dwRootPathCost	DWORD	Path Cost to the bridge root.
RSTP[x].byBridgeHelloTime	BYTE	Hello Time configured.
RSTP[x].byRootHelloTime	BYTE	Hello Time learned.
RSTP[x].byBridgeMaxAge	BYTE	Max Age configured.
RSTP[x].byRootMaxAge	BYTE	Max Age learned.
RSTP[x].byBridgeForwDelay	BYTE	Forward Delay configured.
RSTP[x].byRootForwDelay	BYTE	Forward Delay learned.
RSTP[x].dwTxHoldCount	DWORD	Limit of BPDUs transmitted per cycle.
RSTP[x].dwTimeSinceTC	DWORD	Time, in seconds, since the last topology change.
RSTP[x].dwTCCount	DWORD	Number of times the topology has been changed.
RSTP[x].aPort[y].eName	BYTE	Port name.
RSTP[x].aPort[y].eRole	BYTE	Port function.
RSTP[x].aPort[y].eState	BYTE	Porta state.
RSTP[x].aPort[y].wIdentity	WORD	Port ID.
RSTP[x].aPort[y].dwPathCost	DWORD	Port cost.
RSTP[x].aPort[y].bOperEdge	BIT	Indicates if the port is working as Edge.
RSTP[x].aPort[y].bOperP2P	BIT	Indicates if the port is working as Point-to-Point.
RSTP[x].aPort[y].dwNumTxBPDU	DWORD	Number of BPDUs frames transmitted on the port.
RSTP[x].aPort[y].dwNumRxBPDU	DWORD	Number of frames BPDUs received on the port.

Table 218: RSTP Detailed Diagnostics Group Description

Note:

[x]: is the bridge number.

[y]: is the port number within the bridge.

DG_Modulo.tDetailed.Ethernet.MRP.*	Size	Description
MRP[x].eConfiguredRingRole	BYTE	Indicates the device configuration (Manager or Client)
MRP[x].eCurrentRingRole	BYTE	Indicates the current device configuration
MRP[x].eRingState	BYTE	Indicates the ring status
MRP[x].ePrimaryPort	BYTE	Indicates the main MRP NET
MRP[x].eSecondaryPort	BYTE	Indicates secondary MRP NET
MRP[x].eManagerDiagnostics	BYTE	Indicates Manager diagnostic type

Table 219: MRP Detailed Diagnostics Group Description

Note:

[x]: is the MRP number.

6.1.4.2.12. *UserFiles Detailed Diagnostics Group*

DG_Module.tDetailed.UserFiles.*	Size	Description
byMounted	BYTE	Indicates if the memory used for recording user files is able to receive data.
dwFreeSpacekB	DWORD	Free memory space for user files in Kbytes.
dwTotalSizekB	DWORD	Storage capacity of the memory of user files in Kbytes.

Table 220: UserFiles Detailed Diagnostics Group Description

Note:

User Partition: The user partition is a memory area reserved for the storage of data in the CPU. For example: files with PDF extension, files with DOC extension and other data.

6.1.4.2.13. *UserLogs Detailed Diagnostics Group*

DG_Module.tDetailed.UserLogs.*	Size	Description
byMounted	BYTE	Status of the memory where user logs are inserted.
wFreeSpacekB	WORD	User log memory free space in Kbytes.
wTotalSizekB	WORD	User logs memory storage capacity in Kbytes.

Table 221: UserLogs Detailed Diagnostics Group Description

6.1.4.2.14. *MemoryCard Detailed Diagnostics Group*

DG_Module.tDetailed.MemoryCard.*	Size	Description
byMounted	BYTE	Status of the Memory Card: 00: Memory card not mounted 01: Memory card inserted and mounted
bEnable	BIT	Memory Card enabled.
dwFreeSpacekB	DWORD	Free space in the Memory Card in Kbytes.
dwTotalSizekB	DWORD	Storage capacity of the Memory Card in Kbytes.

Table 222: MemoryCard Detailed Diagnostics Group Description

6.1.4.2.15. *WHSB Detailed Diagnostics Group*

DG_Module.tDetailed.WHSB.*	Size	Description
byHotSwapAndStartupStatus	BYTE	Informs the abnormal situation in the bus which caused the application stop for each mode of hot swapping. See Table 224 for more information.
adwRackIOErrorStatus	DWORD ARRAY (32)	Identification of errors in I/O modules, individually. For more information about this diagnostic, see the notes below.
adwModulePresenceStatus	DWORD ARRAY (32)	Status of presence of declared I/O modules in buses, individually. For more information about this diagnostic, see the notes below.
byWHSBBusErrors	BYTE	Counter of failures in the WHSB bus. This counter is restarted in the energization (0 to 255).

Table 223: WHSB Detailed Diagnostics Group Description

Notes:

Bus modules error diagnostic: Each DWORD from this diagnostic array represents a rack, whose positions are represented by the bits of these DWORDS. So, Bit-0 of the DWORD-0 is equivalent to position zero of the rack with address zero.

Each one of these Bits is the result of an OR logic operation between the Incompatible Configuration (bConfigMismatch), absent modules (bAbsentModules), swapped modules (bSwappedModules), module with fatal error (bModuleFatalError) diagnostics and the operational state of the module in a certain position.

Module presence status: Each DWORD from this diagnostic array represents a rack, whose positions are represented by the bits of these DWORDS. So, Bit-0 from DWORD-0 is equivalent to position zero of the rack with address zero. So, if a module is present, this bit will be true. It's important to notice that this diagnostic is valid for all modules, except power supplies, CPUs and non-declared modules, e.g. those that are not in the rack on the respective position (bit remains in false).

Situations in which the Application Stops: The codes for the possible situations in which the application stops can be consulted below:

Code	Enumerable	Description
00	INITIALIZING	This state is presented while other states are not ready.
01	RESET_WATCHDOG	Application in Stop Mode due to hardware watchdog reset or runtime reset, when the option "Start User Application After a Watchdog Reset" is unmarked.
02	ABSENT_MODULES_HOT_SWAP_DISABLED	Application in Stop Mode due to Absent Modules diagnostic being set when the Hot Swap Mode is "Disabled" or "Disabled, for declared modules only".
03	CFG_MISMATCH_HOT_SWAP_DISABLED	Application in Stop Mode due to Configuration Mismatch diagnostic being set when the Hot Swap Mode is "Disabled" or "Disabled, for declared modules only".
04	ABSENT_MODULES_HOT_SWAP_STARTUP_CONSISTENCY	Application in Stop Mode due to Absent Modules diagnostic being set when the Hot Swap Mode is "Enabled, with startup consistency" or "Enabled, with startup consistency for declared modules only".
05	CFG_MISMATCH_HOT_SWAP_STARTUP_CONSISTENCY	Application in Stop Mode due to Incompatible Configuration diagnostic being set when the Hot Swap Mode is "Enabled, with startup consistency" or "Enabled, with startup consistency for declared modules only".
06	APPL_STOP_ALLOWED_TO_RUN	Application in Stop Mode and all consistencies executed successfully. The application can be set to Run Mode.
07	APPL_STOP_MODULES_NOT_READY	Application in Stop Mode and all consistencies executed successfully, but the I/O modules are not able to start the system. It is not possible to set the application to Run Mode.
08	APPL_STOP_MODULES_GETTING_READY_TO_RUN	Application in Stop Mode and all consistencies executed successfully. The I/O modules are being prepared to start the system. It is not possible to set the application to Run Mode.
09	NORMAL_OPERATING_STATE	Application in Run Mode.
10	MODULE_CONSISTENCY_OK	Internal usage.
11	APPL_STOP_DUE_TO_EXCEPTION	Application in Stop Mode due to an exception in the CPU.
12	DUPLICATED_SLOT_HOT_SWAP_DISABLED	Application in Stop Mode due to Duplicated Slots diagnostic being set when the Hot Swap Mode is "Disabled" or "Disabled, for declared modules only".
13	DUPLICATED_SLOT_HOT_SWAP_STARTUP_CONSISTENCY	Application in Stop Mode due to Duplicated Slots diagnostic being set when the Hot Swap Mode is "Enabled, with startup consistency" or "Enabled, with startup consistency for declared modules only".
14	DUPLICATED_SLOT_HOT_SWAP_ENABLED	Application in Stop Mode due to Duplicated Slots diagnostic being set when the Hot Swap Mode is "Enabled, without startup consistency".
15	NON_DECLARED_MODULE_HOT_SWAP_STARTUP_CONSISTENCY	Application in Stop Mode due to Non Declared Modules diagnostic being set when the Hot Swap Mode is "Enabled, with startup consistency".
16	NON_DECLARED_MODULE_HOT_SWAP_DISABLED	Application in Stop Mode due to Non Declared Modules diagnostic being set when the Hot Swap Mode is "Disabled".

Table 224: Codes of the Situations in which the Application Stops

6.1.4.2.16. Application Detailed Diagnostics Group

DG_Module.tDetailed.Application.*	Size	Description
byCPUState	BYTE	Informs the operation state of the CPU: 01: All user applications are in Run Mode 03: All user applications is in Stop Mode
bForcedIOs	BIT	There is one or more forced I/O points.
bNetDefinedByWeb	BIT	The IP address is set by the System Web Page.

Table 225: Application Detailed Diagnostics Group Description

6.1.4.2.17. Rack Detailed Diagnostics Group

DG_Module.tDetailed.Rack.*	Size	Description
dwAbsentRacks	DWORD	Each bit represents an identification number of a rack, if any bit is TRUE, it means that the rack, with that identification number, is absent.
dwDuplicatedRacks	DWORD	Each bit represents an identification number of a rack, if any bit is TRUE, it means that more than one rack is configured with the same identification number.
dwNonDeclaredRacks	DWORD	Each bit represents a rack identification number, if any bit is TRUE, it means that there is a rack configured with an identification number that is not declared in the project.

Table 226: Rack Group Detailed Diagnostics

6.1.4.2.18. ApplicationInfo Detailed Diagnostics Group

DG_Module.tDetailed.ApplicationInfo.*	Size	Description
dwApplicationCRC	DWORD	32-bit CRC of the application. When the application is modified and sent to the CPU, a new CRC is calculated.

Table 227: ApplicationInfo Detailed Diagnostics Group Description

6.1.4.2.19. SNTP Detailed Diagnostics Group

DG_Module.tDetailed.SNTP.*	Size	Description
bServiceEnabled	BIT	SNTP service enabled.
byActiveTimeServer	BYTE	Indicates which server is active: 00: No active server. 01: Primary server active. 02: Secondary server active.
wPrimaryServerDownCount	WORD	Count of times the primary server was unavailable (0 to 65535).
wSecondaryServerDownCount	WORD	Count of times the secondary server was unavailable (0 to 65535).
dwRTCTimeUpdatedCount	DWORD	Count of times the RTC was updated by the SNTP service (0 to 4294967295).
byLastUpdateSuccessful	BYTE	Indicates status of last update: 00: Not updated. 01: Last update failed. 02: Last update was successful.
byLastUpdateTimeServer	BYTE	Indicates which server was used in the last update: 00: No updates. 01: Primary server. 02: Secondary server.

DG_Module.tDetailed.SNTP.*	Size	Description
sLastUpdateTime.byDayOfMonth	BYTE	Day of last RTC update.
sLastUpdateTime.byMonth	BYTE	Month of last RTC update.
sLastUpdateTime.wYear	WORD	Year of last update of RTC.
sLastUpdateTime.byHours	BYTE	Hour of last RTC update.
sLastUpdateTime.byMinutes	BYTE	Minute of last RTC update.
sLastUpdateTime.bySeconds	BYTE	Second of last RTC update.
sLastUpdateTime.wMilliseconds	WORD	Millisecond of last RTC update.

Table 228: SNTP Group Detailed Diagnostics

6.1.5. Diagnostics via Function Blocks

The function blocks allow the visualization of some parameters which cannot be accessed otherwise. The function regarding advanced diagnostics is in the *NextoStandard* library and is described below.

6.1.5.1. GetTaskInfo

This function returns the task information of a specific application.



Figure 227: GetTaskInfo Function

Below, the parameters that must be sent to the function for it to return the application information are described.

Input parameter	Type	Description
psAppName	POINTER TO STRING	Application name.
psTaskName	POINTER TO STRING	Task name.
pstTaskInfo	POINTER TO stTask-Info	Pointer to receive the application information.

Table 229: GetTaskInfo Input Parameters

The data returned by the function, through the pointer informed in the input parameters are described on table below.

Returned Parameters	Size	Description
dwCurScanTime	DWORD	Task cycle time (execution) with 1 μ s resolution.
dwMinScanTime	DWORD	Task cycle minimum time with 1 μ s resolution.
dwMaxScanTime	DWORD	Task cycle maximum time 1 μ s resolution.
dwAvgScanTime	DWORD	Task cycle average time with 1 μ s resolution.
dwLimitMaxScan	DWORD	Task cycle maximum time before watchdog occurrence.

Returned Parameters	Size	Description
dwIECCycleCount	DWORD	IEC cycle counter.

Table 230: GetTaskInfo Output Parameters

Possible ERRORCODE:

- NoError: success execution;
- TaskNotPresent: the desired task does not exist.

Example of utilization in ST language:

```

PROGRAM UserPrg
VAR
sAppName : STRING;
psAppName : POINTER TO STRING;
sTaskName : STRING;
psTaskName : POINTER TO STRING;
pstTaskInfo : POINTER TO NextoStandard.stTaskInfo;
TaskInfo :NextoStandard. stTaskInfo;
Info : NextoStandard.ERRORCODE;
END_VAR
//INPUTS:
sAppName := 'Application'; //Variable receives the application name.
psAppName := ADR(sAppName); //Pointer with application name.
sTaskName := 'MainTask'; //Variable receives task name.
psTaskName := ADR(sTaskName); //Pointer with task name.
pstTaskInfo := ADR(TaskInfo); //Pointer that receives task info.
//FUNCTION:
//Function call.
Info := GetTaskInfo (psAppName, psTaskName, pstTaskInfo);
//Variable Info receives possible function errors.
    
```

6.2. Graphic Display

The graphic display available in this product has an important tool for the process control, as through it is possible to recognize possible error conditions, active components or diagnostics presence. Besides, all diagnostics including the I/O modules are presented to the user through the graphic display. For further information regarding the diagnostic key utilization and its visualization see [One Touch Diag](#) section.

On figure below, it is possible to observe the available characters in this product graphic display and, next, its respective meanings.

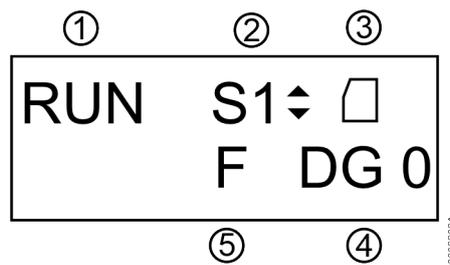


Figure 228: CPU Status Screen

Legend:

- 1. Indication of the CPU status operation. In case the CPU application is running, the state is RUN. In case the CPU application is stopped, the state is STOP and, when is stopped in an application depuration mark, the state is BRKP. For further details, see [CPU Operating States](#) section.
- 2. COM 1 traffic indication. The up arrow (▲) indicates data transmission and the down arrow (▼) indicates data reception. For further information regarding the COM 1 interface see [Serial Interfaces](#) section.
- 3. Memory Card presence indication. Further details regarding its installation see [Memory Card Installation](#) section.
- 4. Indication of the CPU active diagnostics quantity. In case the number shown is different than 0 (zero), there are active diagnostics in the CPU. For further details regarding their visualization on the CPU graphic display, through diagnostic key, see [One Touch Diag](#) section.
- 5. Forced variables in the CPU indication. In case the “F” character is shown in the graphic display, a variable is being forced by the user, whether symbolic, direct representation or AT. For further information regarding variable forcing see [Writing and Forcing Variables](#) section.

Besides the characters described above, Nexto CPUs can present some messages on the graphic display, correspondent to a process which is being executed at the moment.

The table below present the messages and their respective descriptions:

Message	Description
FORMATTING...	Indicates the CPU is formatting the memory card.
FORMATTING ERROR	Indicates that an error occurred while formatting the memory card by the CPU.
NO TAG	There is no configured tag for the CPU in the MasterTool IEC XE.
NO DESC	There is no configured description for the CPU in the MasterTool IEC XE.
MSG. ERROR	Indicates that there are error(s) on diagnostics message(s) of the requested module(s).
SIGNATURE MISSING	Indicates the product presented an unexpected problem. Get in contact with Altus Technical Support sector.
APP. ERROR RESTARTING	Indicates that occurred an error in the application and the Runtime is restarting the application.
APP. NOT LOADED	Indicates that the runtime will not load the application.
LOADING APP.	Indicates that the runtime will load the application.
WRONG SLOT	Indicates that the CPU is in an incorrect position in the rack.
FATAL ERROR	Indicates that there are serious problems in the CPU startup such as CPU partitions that were not properly mounted. Please, contact Altus customer support.
HW-SW MISMATCH	Indicates that the CPU hardware and software are not compatible because the product presented an unexpected problem. Please, contact Altus customer support.
UPDATING FIRMWARE	Indicates the firmware is being updated in the CPU.
RECEIVING FIRMWARE	Indicates the updating file is being transferred to the CPU.
UPDATED	Shows the firmware version updated in the CPU.
UPDATE ERROR	Indicates an error has occurred during the CPU firmware updating, caused by communication failure or configuration problems.
REBOOTING SYSTEM...	Indicates the CPU is being restarted for the updating to have effect.

Table 231: Other Messages of the Graphic Display

6.3. System Log

The *System Log* is an available feature in the MasterTool IEC XE programmer. It is an important tool for process control, as it makes it possible to find events on CPU that may indicate error conditions, presence of active components or active diagnostics. Such events can be viewed in chronological order with a resolution of milliseconds, with a storage capacity of up to one thousand log entries stored in the CPU internal memory, that can't be removed.

In order to access these Logs, just go to the *Device Tree* and double-click on *Device*, then go to the *Log* tab, where hundreds of operations can be seen, such as: task max cycles, user access, online change, application download and upload, application synchronization between CPUs, firmware update between another events and actions.

In order to view the *Logs*, just need to be connected to a CPU (selected Active Path) and click on . When this button is pressed the Logs are displayed and updated instantly. When the button is not being pressed the Logs will be hold in the screen, it means, these button has two stages, one hold the logs state being updated and in the state the updating is disabled. To no longer show the Logs, press .

It is possible to filter the Logs in 4 different types: warning(s), error(s), exception(s) and information.

Another way to filter the messages displayed to the user is to select the component desired to view.

The Log tab's *Time Stamp* is shown by MasterTool after information provided by the device (CPU). MasterTool can display the Time Stamp in local time (computer's time) or UTC, if *UTC time* checkbox is marked.

ATTENTION

If the device's time or time zone parameter are incorrect, the Time Stamp shown in MasterTool also won't be correct.

For further information about the System Logs please check the MasterTool IEC XE User Manual – MU299609 and the RTC Clock and Time Synchronization subsection of this manual.

ATTENTION

The system logs of the CPUs, starting in firmware version 1.4.0.33 (Nexto) and 1.14.36.0 (Xtorm), are reloaded in the cases of a restart of the CPU or a reboot of the Runtime System, that is, it will be possible to check the older logs when one of these situations occurs.

6.4. Not Loading the Application at Startup

If necessary, the user can choose to not load an existing application on the CPU during its startup. Just power the CPU with the diagnostics button pressed and keep it pressed for until the message "APP. NOT LOADED" is shown in the screen. If a login attempt is made, MasterTool IEC XE software will indicate that there is no application on the CPU. For reloading the application, the CPU must be reset or a new application download must be done.

6.5. Common Problems

If, at power on the CPU, it does not work, the following items must be verified:

- Is the room temperature within the device supported range?
- Is the rack power supply being fed with the correct voltage?
- Is the power supply module inserted on the far left in the rack (observing the rack by the front view) followed by the Nexto Series CPU?
- Are there network devices, as hubs, switches or routers, powered, interconnected, configured and working properly?
- Is the Ethernet network cable properly connected to the Nexto CPU NET 1 or NET 2 port and to the network device?
- Is the Nexto Series CPU on, in execution mode (Run) and with no diagnostics related to hardware?

If the Nexto CPU indicates the execution mode (Run) but it does not respond to the requested communications, whether through MasterTool IEC XE or protocols, the following items must be verified:

- Is the CPU Ethernet parameters configuration correct?
- Is the respective communication protocol correctly configured in the CPU?
- Are the variables which enable the MODBUS relations properly enabled?

If no problem has been identified, consult the Altus Technical Support.

6.6. Troubleshooting

The table below shows the symptoms of some problems with their possible causes and solutions. If the problem persists, consult the Altus Technical Support.

Symptom	Possible Cause	Solution
Does not power on	Lack of power supply or incorrectly powered.	Verify if the CPU is connected properly in the rack. Power off and take off all modules from the bus, but the power supply and the CPU. Power on the bus and verify the power supply functioning, the external and the one in the rack. Verify if the supply voltage gets to the Nexto power supply contacts and if is correctly polarized.
Does not communicate	Bad contact or bad configuration.	Verify every communication cable connection. Verify the serial and Ethernet interfaces configuration in the MasterTool IEC XE software.

Table 232: Troubleshooting

6.7. Preventive Maintenance

- It must be verified, each year, if the interconnection cables are connected firmly, without dust accumulation, mainly the protection devices.
- In environments subjected to excessive contamination, the equipment must be periodically cleaned from dust, debris, etc.
- The TVS diodes used for transient protection caused by atmospheric discharges must be periodically inspected, as they might be damaged or destroyed in case the absorbed energy is above limit. In many cases, the failure may not be visual. In critical applications, is recommendable the periodic replacement of the TVS diodes, even if they do not show visual signals of failure.
- Bus tightness and cleanness every six months.
- For further information, see Nexto Series Manual - MU214600.

7. Appendixes

7.1. TLS Key and Certificate Management

This section covers the generation of security files, certificates, and keys using TLS. The certificates commented on below are signed by CA. This type of certificate considers an entity, called Certificate Authority (CA), to generate the certificates. This entity can be an official authority service or a simple computer. It is only necessary to restrict access to the CA to avoid any security breach since this entity can generate certificates for any device. The image below shows how each device interacts with the files.

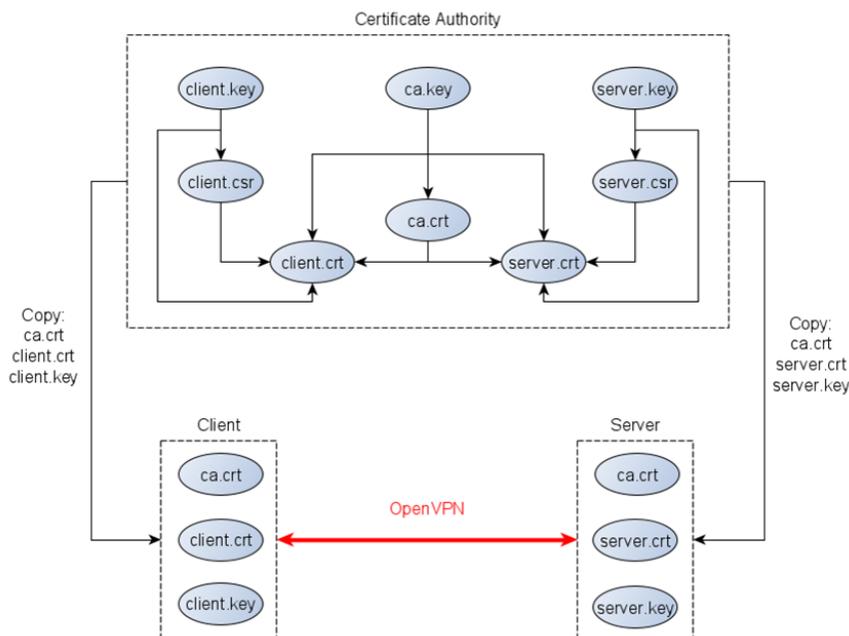


Figure 229: TLS Certificate Generation Flow

First of all, the generated files are private keys. Each device has its key file, created either by the CA entity or the device itself. The most important file is the CA private key `ca.key`, which must not leave the entity. The CA entity generates its certificate based on its private key `ca.crt`. This certificate is a public file used by the devices to validate the VPN connection. Generating certificates from the device first requires a request file (`.csr` or `.req` depending on the tool) based on the device's private key. This document presents two possible tools for generating certificate files: Easy-RSA and OpenSSL.

Make sure you have the date and time set correctly in the CA entity so that the generation of the certificates is based on a current setting.

7.1.1. Easy-RSA Certificate Generation

The OpenVPN project provides this tool to help with the certificate and keys. Easy-RSA is available for Windows and Linux. See below for step-by-step instructions to generate the files in a Windows configuration:

- 1- Open a Windows prompt in the Easy-RSA folder and run `.\EasyRSA-Start.bat` to enter the tool shell.

```
C:\Users\igor.franco\Downloads\EasyRSA-3.0.8-win64\EasyRSA-3.0.8>.\EasyRSA-Start.bat
Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easysrsa' to call the program. Without commands, help is displayed.

EasyRSA Shell
#
```

Figure 230: Certificate Generation using Easy-RSA (step 1)

2 - Copy the file *vars.example* and rename it to *vars* in the tools folder.

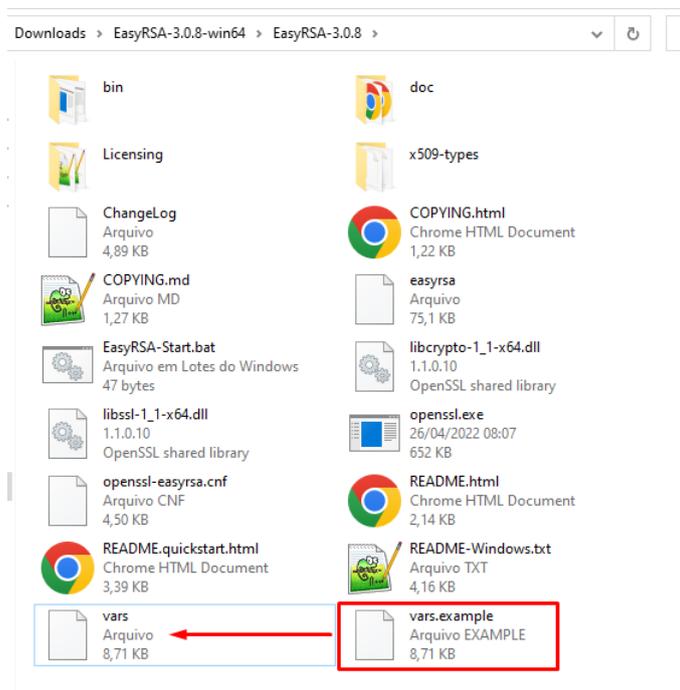


Figure 231: Certificate Generation using Easy-RSA (step 2)

3- Open the file *vars* with a text editor and change the Certification Authority information.

```

75
76 #set_var EASYRSA_TEMP_DIR "$EASYRSA_PKI"
77
78 # Define X509 DN mode.
79 # This is used to adjust what elements are included in the Subject field as the DN
80 # (this is the "Distinguished Name.")
81 # Note that in cn_only mode the Organizational fields further below aren't used.
82 #
83 # Choices are:
84 #   cn_only - use just a CN value
85 #   org     - use the "traditional" Country/Province/City/Org/OU/email/CN format
86
87 #set_var EASYRSA_DN "cn_only"
88
89 # Organizational fields (used with 'org' mode and ignored in 'cn_only' mode.)
90 # These are the default values for fields which will be placed in the
91 # certificate. Don't leave any of these fields blank, although interactively
92 # you may omit any specific field by typing the "." symbol (not valid for
93 # email.)
94
95 #set_var EASYRSA_REQ_COUNTRY  "BR"
96 #set_var EASYRSA_REQ_PROVINCE "Rio Grande do Sul"
97 #set_var EASYRSA_REQ_CITY    "Sao Leopoldo"
98 #set_var EASYRSA_REQ_ORG     "Altus SA"
99 #set_var EASYRSA_REQ_EMAIL   "someemail@altus.com.br"
100 #set_var EASYRSA_REQ_OU      "APED"
101
102 # Choose a size in bits for your keypairs. The recommended value is 2048. Using
103 # 2048-bit keys is considered more than sufficient for many years into the
104 # future. Larger key sizes will slow down TLS negotiation and make key/DH param
105 # generation take much longer. Values up to 4096 should be accepted by most
106 # software. Only used when the crypto alg is rsa (see below.)
107
108 #set_var EASYRSA_KEY_SIZE 2048
109
110 # The default crypto mode is rsa; ec can enable elliptic curve support.
111 # Note that not all software supports ECC, so use care when enabling it.
112 # Choices for crypto alg are: (each in lower-case)
113 # * rsa
114 # * ec
115 # * ed

```

Figure 232: Certificate Generation using Easy-RSA (step 3)

4- Use the command `./easysrsa init-pki` to prepare the configuration.

```
# ./easysrsa init-pki
Note: using Easy-RSA configuration from: ./vars
path = C:/Users/igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-13020.a14492/tmp.XXXXXX
lpPathBuffer = C:\Users\IGOR~1.FRA\AppData\Local\Temp\
szTempName = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmpC051.tmp
path = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmpC051.tmp
fd = 3

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: C:/Users/igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki

EasyRSA Shell
#
```

Figure 233: Certificate Generation using Easy-RSA (step 4)

5- Then type `./easysrsa build-ca nopass` to generate the CA certificate. Remove the `nopass` argument if you want to set a password for the file. Enter the common name of the CA certificate when prompted (press enter to use the default *Easy-RSA CA* as the common name).

```
# ./easysrsa build-ca nopass
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.0j 20 Nov 2018
path = C:/Users/igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-6996.a08916/tmp.XXXXXX
lpPathBuffer = C:\Users\IGOR~1.FRA\AppData\Local\Temp\
szTempName = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmp4FB0.tmp
path = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmp4FB0.tmp
fd = 3
path = C:/Users/igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-6996.a08916/tmp.XXXXXX
lpPathBuffer = C:\Users\IGOR~1.FRA\AppData\Local\Temp\
szTempName = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmp505C.tmp
path = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmp505C.tmp
fd = 3
Generating RSA private key, 2048 bit long modulus
.....+++++
.....+++++
e is 65537 (0x010001)
path = C:/Users/igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-6996.a08916/tmp.XXXXXX
lpPathBuffer = C:\Users\IGOR~1.FRA\AppData\Local\Temp\
szTempName = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmp5194.tmp
path = C:\Users\IGOR~1.FRA\AppData\Local\Temp\tmp5194.tmp
fd = 3
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:CA-Entity

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
C:/Users/igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/ca.crt

EasyRSA Shell
#
```

Figure 234: Certificate Generation using Easy-RSA (step 5)

6 - Generate the device key and request files using the command `./easysrsa gen-req DeviceName nopass`. Change the `DeviceName` with the desired common name. Again, remove the `nopass` argument to use a password for the certificate file. When entering the Common Name as an argument, simply press Enter when prompted (red square).

```

# ./easysrsa gen-req DeviceName nopass
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.0j  20 Nov 2018
path = C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-16216.a13984/tmp.XXXXXX
lpPathBuffer = C:/Users/Igor~1.FRA/AppData/Local/Temp/
szTempName = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp150B.tmp
path = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp150B.tmp
fd = 3
path = C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-16216.a13984/tmp.XXXXXX
lpPathBuffer = C:/Users/Igor~1.FRA/AppData/Local/Temp/
szTempName = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp1696.tmp
path = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp1696.tmp
fd = 3
path = C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-16216.a13984/tmp.XXXXXX
lpPathBuffer = C:/Users/Igor~1.FRA/AppData/Local/Temp/
szTempName = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp1742.tmp
path = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp1742.tmp
fd = 3
Generating a RSA private key
.....++++
.....++++
writing new private key to 'C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-16216.a13984/tmp.a02420'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg. your user, host, or server name) [DeviceName]:
-----
Keypair and certificate request completed. Your files are:
req: C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/reqs/DeviceName.req
key: C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/private/DeviceName.key

EasyRSA Shell

```

Figure 235: Certificate Generation using Easy-RSA (step 6)

7- Finally, type `./easysrsa sign-req server DeviceName` to generate the device certificate. The *DeviceName* is the desired common name, and the *server* is the type (use *client* if you are generating for a VPN client).

```

# ./easysrsa sign-req server DeviceName
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.0j  20 Nov 2018

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=
  commonName = DeviceName

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
path = C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-9368.a06604/tmp.XXXXXX
lpPathBuffer = C:/Users/Igor~1.FRA/AppData/Local/Temp/
szTempName = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmpC79.tmp
path = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmpC79.tmp
fd = 3
path = C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-9368.a06604/tmp.XXXXXX
lpPathBuffer = C:/Users/Igor~1.FRA/AppData/Local/Temp/
szTempName = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmpF29.tmp
path = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmpF29.tmp
fd = 3
path = C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-9368.a06604/tmp.XXXXXX
lpPathBuffer = C:/Users/Igor~1.FRA/AppData/Local/Temp/
szTempName = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp10FE.tmp
path = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp10FE.tmp
fd = 3
path = C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-9368.a06604/tmp.XXXXXX
lpPathBuffer = C:/Users/Igor~1.FRA/AppData/Local/Temp/
szTempName = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp11AA.tmp
path = C:/Users/Igor~1.FRA/AppData/Local/Temp/tmp11AA.tmp
fd = 3
Using configuration from C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/easy-rsa-9368.a06604/tmp.a16398
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12: 'DeviceName'
Certificate is to be certified until Jul 29 12:59:53 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: C:/Users/Igor.franco/Downloads/EasyRSA-3.0.8-win64/EasyRSA-3.0.8/pki/issued/DeviceName.crt

EasyRSA Shell

```

Figure 236: Certificate Generation using Easy-RSA (step 7)

8- Repeat steps 6 and 7 to generate more device certificates.

9- Find the *ca.crt* in the *pki* folder, the device private keys in the *pki/private* path, and the device certificates in the *pki/issued* directory.

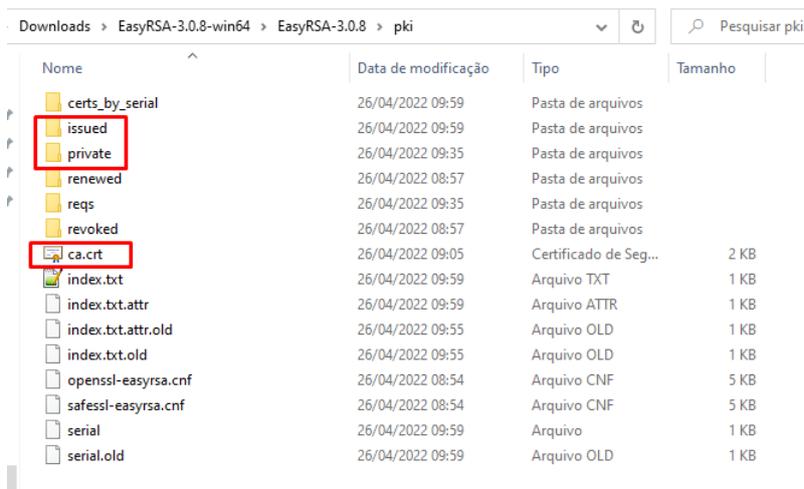


Figure 237: Certificate Generation using Easy-RSA (step 9)

7.1.2. OpenSSL Certificate Generation

OpenSSL is an open-source package with tools that help generate many files and security features. This package is native to most Linux distributions and is available for Windows. Just remember to set the OpenSSL folder in the PATH (environment variable) to allow you to use the command from anywhere via the prompt. Find below the step-by-step using this feature (all files can have any name as desired, the steps consider only an example):

- 1- Open a prompt in the certificate folder (where you will create the files).
- 2- Generate the CA private key with the following command: `openssl genrsa -out ca.key 4096`.

```
C:\Users\igor.franco\Downloads\Certificate>openssl genrsa -out ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....++++
.....++++
e is 65537 (0x010001)
C:\Users\igor.franco\Downloads\Certificate>
```

Figure 238: Certificate Generation using OpenSSL (step 2)

- 3- Then generate the CA certificate based on the private key, using the `openssl req -new -x509 -days 365 -key ca.key -out ca.crt` command.

The parameter `-days` represents the expiration time for the certificate. Set it as desired. In this example, the certificate is valid for one year. Fill in the values requested at the prompt as needed (press enter to use the default, which is enclosed in square brackets []). It is mandatory to define a Common Name for the certificate work.

```
C:\Users\igor.franco\Downloads\Certificate>openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:CA-Entity
Email Address []:
C:\Users\igor.franco\Downloads\Certificate>
```

Figure 239: Certificate Generation using OpenSSL (step 3)

4- Now generate the device's private key, similar to step 2, using the command `openssl genrsa -out DeviceName.key 2048`.

```
C:\Users\igor.franco\Downloads\Certificate>openssl genrsa -out DeviceName.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
C:\Users\igor.franco\Downloads\Certificate>
```

Figure 240: Certificate Generation using OpenSSL (step 4)

5- After that, generate the certificate request file based on the private key using the command `openssl req -new -key DeviceName.key -out DeviceName.csr`.

Enter the desired information, and remember to use a common name other than CA.

```
C:\Users\igor.franco\Downloads\Certificate>openssl req -new -key DeviceName.key -out DeviceName.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:DeviceName
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
C:\Users\igor.franco\Downloads\Certificate>
```

Figure 241: Certificate Generation using OpenSSL (step 5)

6- Finally, generate the device certificate using the CA private key, the CA certificate, and the device certificate request file using the `openssl x509 -req -days 365 -in DeviceName.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out` command.

Set the expiration date as desired with the parameter `-days` and the serial number of the certificate with the argument `-set_serial`.

```
C:\Users\igor.franco\Downloads\Certificate>openssl x509 -req -days 365 -in DeviceName.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out DeviceName.crt
Signature ok
Subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = DeviceName
Getting CA Private Key
C:\Users\igor.franco\Downloads\Certificate>
```

Figure 242: Certificate Generation using OpenSSL (step 6)

7- Repeat steps 4 to 6 for any new device.

8- (Optional) OpenSSL provides a tool to verify that the device certificate works with CA:

Use the command `openssl verify -purpose sslserver -CAfile ca.crt DeviceName.crt`.

```
C:\Users\igor.franco\Downloads\Certificate>openssl verify -purpose sslserver -CAfile ca.crt DeviceName.crt
DeviceName.crt: OK
```

Figure 243: Certificate Generation using OpenSSL (step 8)

7.1.3. TA Key Generation by OpenVPN

The OpenVPN project provides a tool for generating a TLS key, commonly called `ta.key`. This key is an extra layer of protection on OpenVPN's UDP/TCP communication ports, so the use of this key can be interpreted as an HMAC Firewall for VPN communication, requiring the existence of the parameter on both sides of the communication for it to be established.

The key generation can be done with the following command: `openvpn --genkey secret ta.key`. Example of using the command in Windows:

```
C:\Program Files\OpenVPN\bin>openvpn --genkey secret C:\Users\bruno.berwanger\Desktop\Chaves\ta.key
C:\Program Files\OpenVPN\bin>
```

Figure 244: TA Key Generation in Windows

To execute the command, we used the executable installed with the OpenVPN package. The directory used in the image above is an example and is optional. You can use only the desired file name too.

The command can be used to generate the key from Linux, but there is a minor change in the command compared to Windows. To generate the key on Linux, use the following command: `openvpn --genkey --secret ta.key`. To run it, type the command in the terminal, as follows the example:

```
developer@developer:~$ openvpn --genkey --secret ta.key
developer@developer:~$ █
```

Figure 245: TA Key Generation in Linux

This parameter is not mandatory for VPN communication, but if the server uses it, all its clients must also use it, and the key for the server and the clients must be the same.