SENEDA 4.0 SRLS
security - video security - home automation

Via Cariglia 96
71122 Foggia(Italy)
Phone : +39 0881 020289
info@seneda.it
www.seneda.it
VAT Number: 04412580716



CONGRATULATIONS!

Thank you for purchasing our Video Security, Video Alarm, Video Surveillance, Home Automation and Building Automation System

The system, thanks to its powerful Hardware and Software, allows you to satisfy the most varied usage configurations, offering a high level of protection and security.

NEXUS NEW

The system can be managed in a single Network and a single App and was designed, planned and created in Italy by:

SENEDA 4.0 SRLS
Via Cariglia n°96
71122 – Foggia (Italy)

Tel. +39 0881 020289
www.seneda.it
info@seneda.it

TECHNICAL MANUAL

Revision Index: Rev.0.1 of 06/27/2024

ATTENTION!

Before installing and operating the NEXUS NEW system, please read the following instructions carefully!



Index Nexus New Technical Manual (Automatic Index Ctrl key + Click on the page number)

Tips and Warnings---------- 6
Precautions----------6
Disposal of the NEXUS NEW System and its accessories ----------7
General Rules----------7
Introduction ----------7
EC Rules and Directives---------- 7
Safety Rules---------- -7
Environmental Characteristics ----------7
Transport and Storage---------- 7
Operation ----------7
Protection against the penetration of liquids ---------- 7
Block Diagram ----------8
Bosch Video Analytics Technologies----------9
Installation ----------10
UPR BUS ----------10
LAN TCP IP ----------10
220 Vac mains power supply---------- 10
Nexus New Technical Features and Functions----------11
Hardware Features ----------11
Software Features ----------11
Security Features ----------12
Video Features ----------12
Home Automation and Technology Features ----------12
Hardware CPU Central ----------13
Hardware Power Supply - 1020/C2 ----------14
Hardware RS485 Router - 1020/C3 ----------15
Hardware Alarm Acquisition Sensor Interface 1021/S1 ----------16
Hardware Interfaced DT Sensor - 0012/3 ----------17
Hardware Interfaced PIR Sensor - 0012/4 ----------18
Hardware Interfaced Temperature Sensor - 0012/4----------19
Hardware Interfaced Twilight Sensor - 0012/4 ----------20
Hardware Digital Actuator Interface - 1022/A1 ----------21
Hardware Access Control Interface - 1022/A01-AC ----------22
Hardware Interfaced Self-Powered Siren 0013/2 ----------23
Hardware Interfaced Domo Socket - 1022/A3 ----------24
Hardware RFID Transponder Key Reader - 1023/M1 ----------25
Hardware Remote Keypad - 1023/M2 ----------26
Hardware Keyboard / Touch- 1023/M ----------27
Hardware Domo Climate Interface and Remote Controls - 1024/D1 ----------28
Hardware Domo Automation Interface – 1024/D4 ----------29
Hardware Domo Interface Electricity Consumption Control – 1024/D5---------- 30
RS485 BUS with SENEDA 4.0 protocol ----------31
BUS connection between Control Unit and UPR Devices ----------31
TCP IP Network ----------32
System programming ----------33
Programming Tools----------36
Add New System----------37
Enter Installation Data----------38
Enter Service Intervention Data----------38
PC Connection /Local/Remote Central----------39
Network Configuration----------40
System Code Programming Menu ----------41
System Initialization (Automatic search for devices installed on the Networks)----------42
Device List----------43
Manual Insertion NON Bosch Cameras----------44
Device Programming---------- 45
Remote Power Supply – 1020/C2 ----------45
Digital Sensor Interface - 1021/S1 ----------46

Addressed DT Sensor - 1021/S2 ----48
Addressed PIR Sensor - 1021/S4 ----50
Temperature Sensor - 1021/S5 ----52
Addressed Twilight Sensor - 1021/S6 ----53
Actuator Interface - 1022/A1 ----54
Access Control Actuator Interface - 1022/A01-AC ----55
Self-Powered Siren - 1022/A2 ----56
Addressed Domo Socket - 1022/A3 ----57
RFI Key Reader - 1023/M1---- 58
LCD Keypad - 1023/M2 ----59
Domo Clima Interface - 1024/D1 ----60
Domo Automation Interface - 1024/D4 ----61
Domo Electricity Consumption Control Interface - 1024/D5 ----62
Touch Display – 1023/M3 ----63
Programming Telephone Terminals ----64
Security Menu ----65
List of UPR Devices ----65
Programming Security Blocks ----66
Programming Code ----67
Key Programming----68
Weekly Security Time Programmer ----69
Home Automation / Technological Menu ----70
Add new block button ----71
Video Surveillance Menu ----72
Scenarios ----73
Event History ----74
Services Menu ----75
220Vac Network Filter ----75
Central Upgrade ----75
System Reboot- Local ----75
System Reboot- Public ----75
Record to Cloud ----75
Terminate Connection ----75
Active Status ----76
Device Failure ----76
Tampering ----76
Alarms ----77
220 Vac Mains/ Return Failure on the Control Panel Power Supply and Remote Power Devices---- 77
Control Panel Battery with Low Voltage---- 77
Maintenance Entry from LCD or Touch Keypad ----77
Maintenance End from LCD or Touch Keypad ----77
Firmware Update----77
Reset Procedure in the Event of Control Panel Default---- 77
Remote Assistance----77
Total Reset of the Control Panel---- 77
Print Configurations performed----77

Tips and Warnings

Precautions

The Nexus New System (hereinafter referred to as the System), must be installed in accordance with the EMC information referred to in this manual.

Radio equipment and mobile phones, if used near the System, may affect its operation.

The use of accessories and cables other than those specified by the manufacturer, as spare parts, may cause an increase in Emissions or a decrease in Immunity of the System.

System Disposal **Nexus New** and its accessories

The “RAEE Decree” is the implementation by Italy of the European directives 2002/95/EC, 2002/96/EC and 2003/108/EC on the restriction of the use of certain hazardous substances in Electrical and Electronic Equipment and on the management of the end of life of the same type of equipment.

Its objective is to ensure that products are recycled using the best available techniques in terms of treatment, reuse and recycling to guarantee people's health and intense environmental protection.

The RAEE decree is applied to the System, therefore, once decommissioned, the system must not be disposed of as urban waste, but a separate collection must be carried out for it, through the delivery of the products to the separate collection facilities set up by the municipalities, in the case of private users, or through delivery to the manufacturer, in the case of companies or distributors.

The penalties envisaged in the event of illegal disposal of said waste are reported in the Legislative Decree. 175/05 (Directive 2002/96/EC).

The following symbol indicates the separate collection of electrical and electronic equipment.



General Rules

SENEDA 4.0 products are built using the most advanced technologies and certified, top-quality electronic and mechanical components.
Every single device is tested before being placed on the market.
Components sensitive to electrostatic discharges are mounted on the circuits of the electronic boards, which can be irreparably damaged if handled incorrectly.
The continuity test must be performed after disconnecting the System from the power supply and after disconnecting the connection cables.
SENEDA 4.0 products are built using the most advanced technologies and certified, top-quality electronic and mechanical components.
Every single device is tested before being placed on the market.
Components sensitive to electrostatic discharges are mounted on the circuits of the electronic boards, which can be irreparably damaged if handled incorrectly.
The continuity test must be performed after having disconnected the System from the power supply and after having disconnected the connection cables.

CE Standards and Directives

• EN50130-4: 2011-11 Immunity
• EN61000-6-3: 2023-06 Emissions
• EN62368-1: 2022-10 Security
• CEI79-2;V2: 2017-02 Burglar Alarm Equipment
And therefore compliant with the ESSENTIAL REQUIREMENTS of the DIRECTIVES 2014/35/EU, 2014/30/EU and 2011/65/EU.
A copy of the product's “Declaration of Conformity” is available from the Manufacturer.

Safety Precautions

Please observe the following safety precautions to avoid injury and prevent damage to the product or any device connected to it. In particular:
• Use a power cord that is appropriate and specific for this device
• Do not connect the device to a power source that exceeds the ratings on the plate
• Do not allow children to play with the device
• Do not use chemicals such as petrol or alcohol for cleaning
• Make sure all connections are tight
• Installation must be carried out by specialist personnel
• Do not operate with wet hands during installation
• It is recommended to handle the packaging containing the device and its accessories with care
• Store the device and its accessories in a dry and ventilated place
The manufacturer declines all responsibility for any damage that may directly or indirectly arise to people, animals or things as a result of failure to comply with all the installation and/or use instructions indicated in this manual.

Environmental Characteristics

Transport and Storage

- Minimum temperature: -10°C
- Maximum temperature: +75°C
- Minimum relative humidity: 30% non-condensing
- Maximum relative humidity: 95% non-condensing
- Minimum atmospheric pressure: 700hPa
- Maximum atmospheric pressure: 1060hPa

Operation

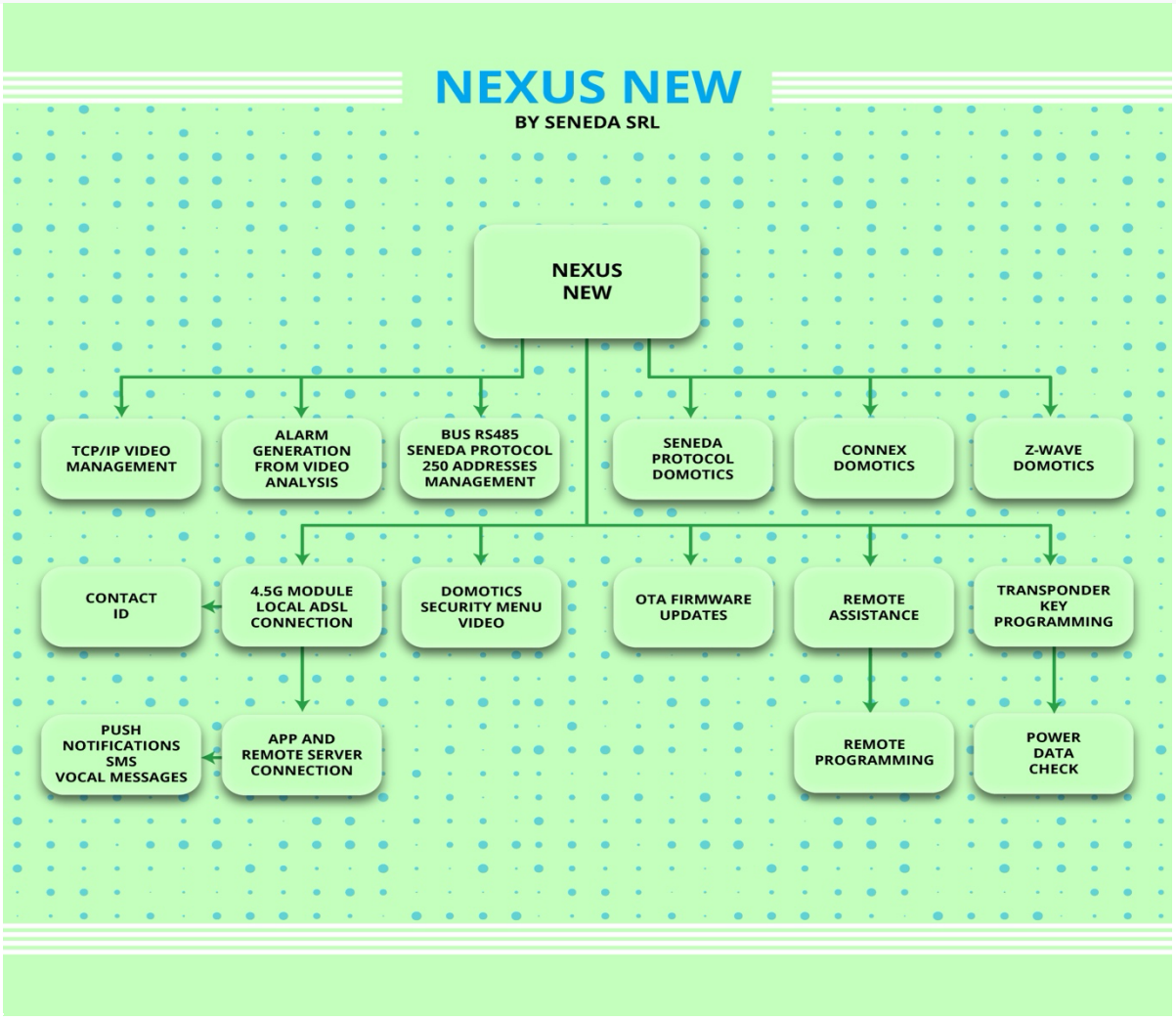
- Minimum temperature: +10°C
- Maximum temperature: +40°C
- Minimum relative humidity: 30% non-condensing
- Maximum relative humidity: 75% non-condensing
- Minimum atmospheric pressure: 700hPa
- Maximum atmospheric pressure: 1060hPa

Protection against penetration of liquids

- Grade: IP 44

System Description

BLOCK DIAGRAM



NEXUS NEW

SECURITY - VIDEO ALARM - IP VIDEO SURVEILLANCE - HOME AUTOMATION

ANTI-INTRUSION

By manipulating the data from the Video Images, it is able to carry out an in-depth analysis by verifying effective intrusion alarm conditions, helping to almost cancel the danger of false activations, replacing the old Burglar Detection sensor devices (radar, barriers, etc.). In case of detection, it sends a Video / Audio clip of the event in real time.

VIDEO SURVEILLANCE

We have implemented an innovative Lay-Out for the construction of video surveillance systems
NEXUS contains all the **performances of the classic IP video surveillance systems** but makes the NVR systems - Hard Disk, Network Switch, etc. obsolete.

DOMOTICS AND CONTROLS

Specialized management interfaces: Lighting technology; Climate; Remote controls; Automation
- CONNEX and Z-WAVE interface

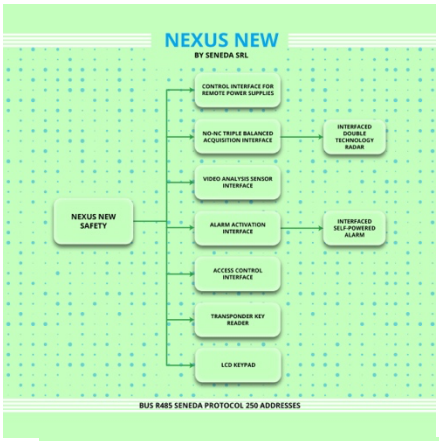
CONNECTIVITY

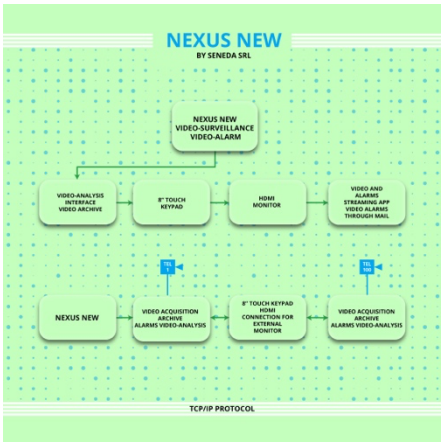
with the 4.5 G module and the ADSL connection
- A single APP to manage security, video surveillance, home automation and tech management. PUSH notifications, SMS and Voice Mail
- Interfacing with the most common protocols used by the Telealarm operating centers (SIA-IP DC9 PROTOCOL; CONTACT ID)
- Simple and intuitive programming software on Windows platform, remote service, remote programming

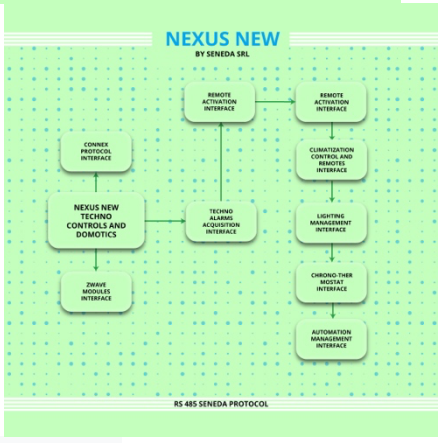
SENEDA s.r.l.
sicurezza - video sicurezza - domotica

www.seneda.it
info@seneda.it
+393920732279

SAFETY VIDEO HOME AUTOMATION







Technology

Nexus New Uses a RS485 BUS with a proprietary protocol that allows the management of 250 remote interface devices for the management of all the Anti-intrusion functions.

In combination with the TCPIP network, it manages up to 150 IP cameras with Video-Analysis function with extrapolation of alarm events detected by the algorithmic analysis of video images.

Intrusion

Detection and reporting of intrusion within virtual areas or when crossing virtual lines in a certain direction by subjects of interest.

Gate Flow

Counting and aggregating the number of people crossing virtual lines in one direction.

ATM

Detection and reporting of one or more people loitering within a certain area.

Stolen Object

Detection and reporting of removed objects within virtual areas.

Panic Disorder

Detection and reporting of sudden and anomalous changes in speed and/or acceleration in the movements of subjects within virtual areas.

Smoke Fire

Detection and reporting of smoke or fire within virtual areas.

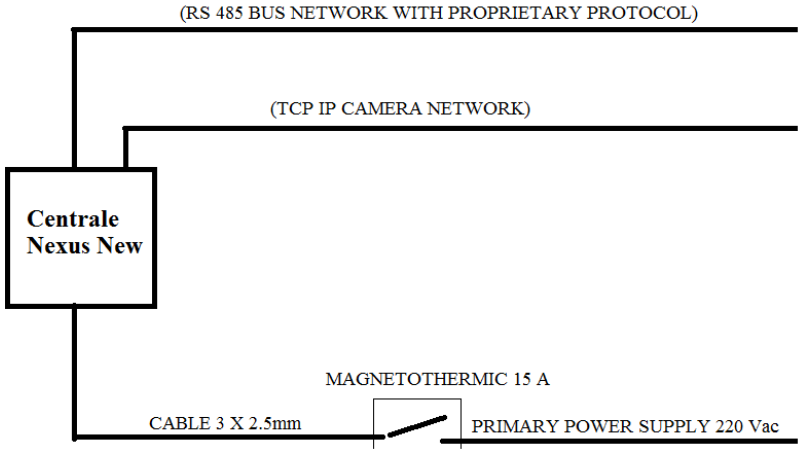
Installation

Precautions

For the final quality of the installation, careful initial planning is crucial; in particular, it is necessary to determine and plan how the System will be used. In particular, in order to obtain the best protection of the site to be protected and the best installation, it is necessary to:

• Check the possibilities of intrusion
• Choose suitable sensors for effective protection of the focused points; the same must be as selective as possible to avoid false activations
• For the detection of alarms from Video Analysis, the Cameras are those specified below
• Size the power supplies according to the electrical absorption
• Establish the position of the actuation devices
• It is advisable to mount two external Self-Powered Sirens placed far apart from each other
• Check the availability of the 4G network of the operator you have chosen to use
• Position the control unit in a room that is not accessible to outsiders and in any case in a protected place not exposed to bad weather
• The Central unit must be mounted in a position that guarantees easy access for maintenance work
• Avoid exposing it to excessive temperatures and humidity
• Establish the path and lengths of the cables
• Size the section of the power cables according to the electrical absorption so as not to have an excessive voltage drop, or provide additional power supplies along the line by connecting all the negatives (GND) of the power supply in parallel with each other
• The maximum length of the BUS of network is 800m. Beyond this distance it is necessary to use RS 485 amplifiers
• The control unit can manage, via BUS, a maximum of 250 devices for the Intrusion and Home Automation functions and, via LAN network, a maximum of 150 Cameras
• The maximum distance between one Switch and another in the LAN network is 100m (Use only Gbit Switches)

SYSTEM WIRING



UPR BUS Network

Connects the control unit to all the Interface devices for the management of Security and Home Automation functions.
The control unit can manage a total of 250 Addresses.

TCP IP LAN Network

Connects Cameras, Touch Keypads to the network.
The control unit can manage a total of 250 Addresses.
NB: Conductors 4 and 5 can be used on the LAN cable for the BUS485.

220Vac mains power supply

For the section of the conductors of the power cable, comply with current regulations.
It is mandatory to connect the control unit to an efficient earthing and protect the line with a 10A Thermal Magnetic switch with U intervention curve.
Use a direct line with the general meter or from the general user panel.
Do not connect the control unit to the socket or the lighting device.

Technical Features and Functions

Hardware Features

• Integrated Single-card CPU managed by the VAR-SOM IMX Processor
• 11-15Vdc 2.5A Switching Power Supply (optional 5A)
• Hardware Control of Power Data
• 4.46 Gbit Non-volatile Memory
• Integrated 4G LTE Module
• RJ Connector for Connection to the Local ADSL Network
• RJ Connector for Connection to the Local Network of the Cameras
• RJ Connector for Connection to the Local Network (Lan Cameras + BUS485)
• Additional BUS485 Terminal Block
• 12Vdc Service Power Output
• Control Unit Tamper Input
• 220Vac Primary Network Presence Signaling LED
• 4G LTE Network Presence Signaling LED
• General Anti-Intrusion ON/OFF Signaling LED
• Partial Anti-Intrusion Blocks ON/OFF Signaling LED
• Fault and Anomaly Signaling LED
• SD Card (used by the manufacturer to download the control unit firmware – DO NOT use)
• Absorption 125÷180mA
• 7Ah Battery compartment container in ABS
• 17Ah Battery compartment container optional

Software Features

- Programming from a Tool connected locally or remotely
- Automatic search for devices connected to the BUS network
- Management, via BUS, of the following items addressed up to a maximum of 250 devices:
  - 1020/C2 - Remote Power Supply Interface
  - 1020/C3 - RS 485 Router
  - 1021/S1 - Alarm Acquisition Interface
  - 1021/S3 - DT Sensor
  - 1021/S4 - PIR Sensor
  - 1021/S5 - Temperature Sensor
  - 1021/S6 - Twilight Sensor
  - 1022/A1 - Command Actuator
  - 1022/A0/AC - Access Control Actuator
  - 1022/A2 - Self-Powered Interfaced Siren
  - 1022/A3 - Controlled Socket
  - 1024/D1 - Remote Control Climate Interface
  - 1024/D4 - Domo Automation Interface
  - 1025/D5 – Domo Electrical Consumption Control Interface
  - 1023/M1 - RFI Reader
  - 1023/M2 - LCD Keyboard
  - 1023/M3 - Touch Monitor
  - 1023/M4 - Transponder Key

• Querying of devices connected to the BUS via Intelligent Polling (Proprietary Protocol)
• Testing of the status of the Inputs of the Acquisition devices
• Self-diagnostics
• Differentiated reports by type of Alarm, Tampering and Fault
• Management on LAN network of Cameras with ONVIF Protocol for a maximum of 150
• Bosch Configuration Manager integrated on Tool for programming the Video Analysis functions
• Management on LAN network of Touch Displays + additional Monitors
• Programming of 60 Autonomous Security Blocks (areas)
• Programming of 60 Home Automation Blocks (functions) and Management of the Functions:
◦ Chronothermostat, Automation, Lighting, Air Conditioning, Remote Management of Remote Controls
◦ Control of Electricity Consumption, Controlled Sockets, Management of Technological Alarms
• Control of Power Supply data of the Central Unit and of the Remote Power Supply groups with time filter programming
• No. 3 Operating States; Installation, Maintenance, Active Status
• Password programming for Installer and User access

- Weekly Timer, 72 ON/OFF functions for automatic Security commands
- N° 1 Weekly Timer for each Home Automation function
- Management menu; SECURITY, HOME AUTOMATION, VIDEO/AUDIO separated
- Programming of 14 Telephone Numbers for SMS messaging
- Android and IOS APP
- Link for downloading live Video images and from history managed by remote Server
- Centralization and Visualization Tool for Data and Video events for Operations Centers of Security Institutes

Security Features

- Differentiated management of the different signals: Theft Alarm, Fire, Robbery, Tampering, Fault
- Management of forced Arming with Automatic Reset
- Management of forced Disarming with sending of the Robbery signal
- Management of the END function, between Sensors and between Sensors and Cameras
- Management of the Patrol function
- Management of the Alarm Pulse count
- Management of the Timings for each Device
- Management of Primary Network Failure/Return with Time filter
- Management of Primary Network Remote Power Supplies and Buffer Batteries
- Programming of 30 security subsystems (Areas)
- Programming of 64 ON/OFF functions (Automatic and Semi-Automatic) for the insertion of security blocks
- Programming of 250 customized Proximity Codes and Keys with 20-character text
- Historical Memory with 1000 cyclic events
- Firmware updates from Cloud
- Event Display on TOOL
- Online event printing
- Calendar clock with Daylight Saving Time - Solar and Leap Year management
- Data Remote Control in SMS technique
- Poush Notifications on IOS and ANDROID platform
- Anti Jammer

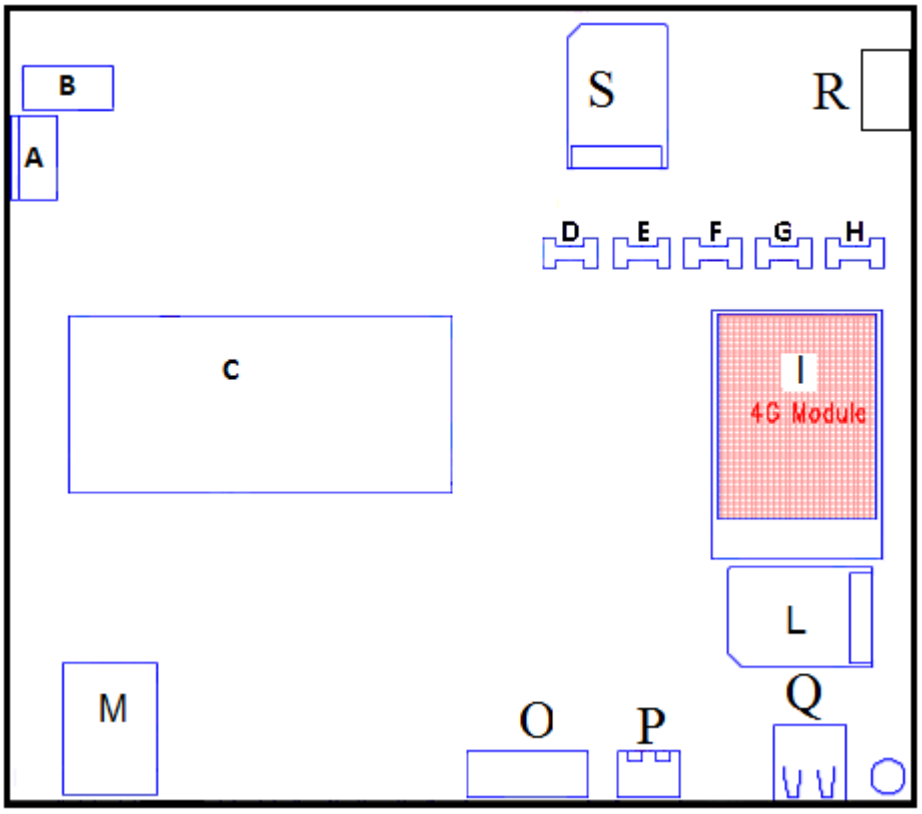
Video Features

- LAN network management of BOSCH DINION series cameras with extrapolation of alarm events from algorithmic analysis of video and cameras with ONVIF protocol for a total max. 150 Cameras
- Sending Video/Audio clips in case of alarm of the affected area
- END function between the alarm from video analysis and the alarm of a traditional sensor
- END function between the alarm of a traditional sensor and the Video/Audio images of ONVIF Cameras
- Configuration and Management of the THEFT – FIRE – ROBBERY alarm signals from VIDEO ANALYSIS
- Event history on the Camera SD Card and automatic download to Remote Server
- Download historical Video events directly from Link
- Simple and intuitive configuration tool
- Video functions menu (Video analysis parameter settings, History, etc.)
- Management of Touch Display on LAN network
- Viewing of the Cameras on the Touch and HDMI output to connect external Monitors
- Menu on the Touch for managing the Video functions
- Remote control of video data on ANDROID and IOS APP (Single APP for Security, CCTV, Home Automation)

Home Automation and Technological Functions

- Management on BUS of 250 devices
- Creation of 60 blocks for the Management of functions
  - Controlled electrical sockets, Lighting systems, Chronothermostat, Climate management, Remote controls
  - Management of automations, Management of technological devices, Management and Control of electricity consumption
- For each block, association of a 64-function automatic weekly programmer
- Programming of 30 Scenarios

CPU



Main Features:

A = DC power input connector + 220 Vac primary network presence signal
B = Self-resettable general fuse
C = Microprocessor
D = 220Vac network presence signal LED
E = Anomaly signal LED
F = General inserted signal LED
G = Partially inserted signal LED
H = 4G network signal LED
I = 4G module
L = SIM port
M = RJ connector for connection to the ADSL network and the local network Cameras
O = Interface network BUS terminal block
P = 12Vdc auxiliary power supply
Q = USB connector
R = Central Protection Switch input
S = SD Card (Not Usable)

Power supply - 1020/C2

Interface Module for Remote Power Supplies, the device is used to Power Devices when the voltage / Current supplied by the Central Power Supply is insufficient. Completely supervised by the Control Unit, it provides the following data and Parameters:

Technical Characteristics

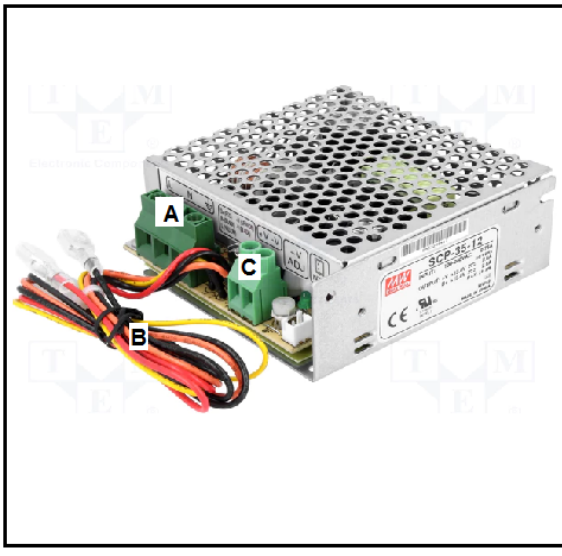
- Input voltage: 220Vac - 50Hz
- Output voltage: 12-14 Vdc
- Max. current delivered 2.6 A (Optional 5th)
- Max power 35.9W 2.6 A
- Switching technology

"Attention: Connection to an efficient earthing is mandatory"

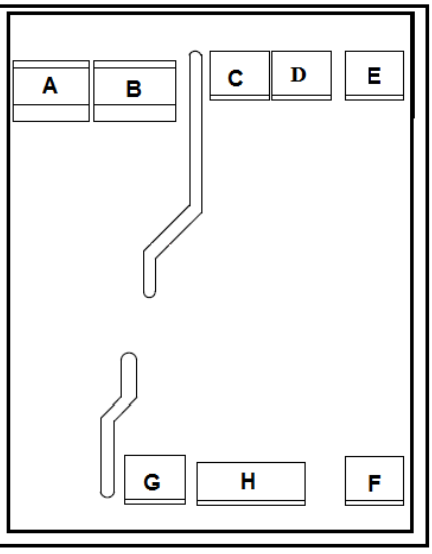
Chassis

- ABS container
- Dimensions [mm]: H=310 W=310 D=91
- Anti-opening protection
- Battery compartment 12Vcc-7A
- Optional container with 17Ah battery compartment

POWER SUPPLY



INTERFACE



INTERFACE

A. Primary power input 220 Vac
B. Primary power output 220 Vac: to be connected to terminal A of the power supply
C. Battery cable output: to be connected to the buffer battery
D. Power supply battery cable input: connect the battery cables of the power supply
E. Power input 12Vdc: to be connected to terminal C of the power supply
F. Output 12Vdc
G. Tamper input
H. Network bus (isolate the +12 Vdc terminal)

POWER SUPPLY:

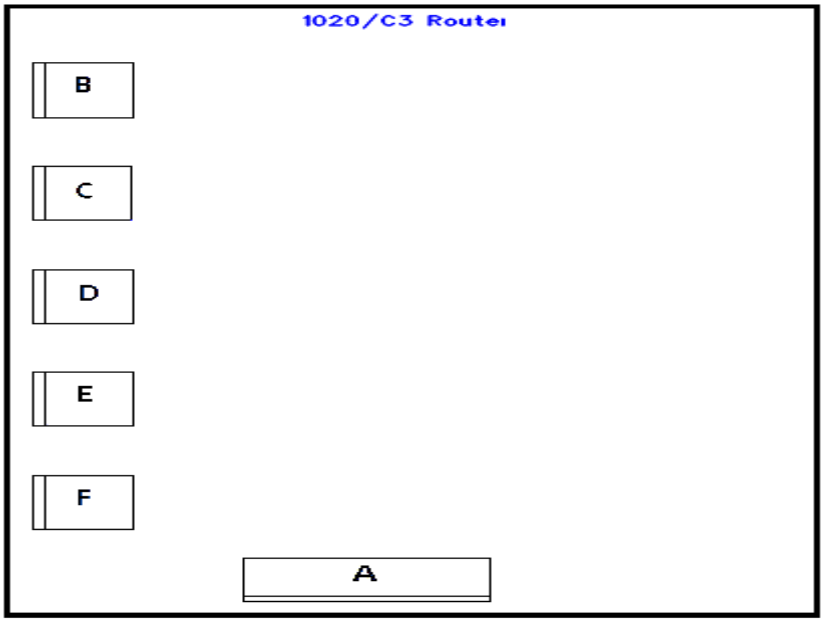
A. Primary Power Input 220Vac: (from terminal B of the interface)
B. Power Output 12Vdc: to be connected to terminal E of the Interface
C. Battery Cables: to be connected to terminal D of the Interface

Router RS485 - 1020/C3

Main Features

The RS485 BUS is a balanced network with a typical impedance of 120Ω.
In the case of complex installations, with long cable lengths and multiple branches, it is advisable to use this device equipped with 4 separate networks which allow for easy balancing.
NB: insert a 120Ω resistor as a termination between A and B on the last device of each network.

ROUTER



Main Features

• Power supply voltage: 12Vdc±5%
• Current consumption: 18mA
• Transceiver protection from extra voltages: up to 15SKV
• Protection against polarity inversions: yes
• Operating temperature: 0°C +40°C
• Made in Risc technology
• Dimensions [mm]: L=85; B=135; H=30

A. Central BUS terminal block. Connect in parallel to the Q terminal of the central CPU
B. Peripheral BUS networks
C. Peripheral BUS networks
D. Peripheral BUS networks
E. Peripheral BUS networks
F. Service power supply

Sensor Interface Alarm Acquisition - 1021/S1

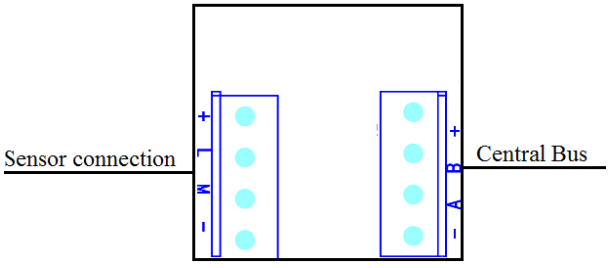
Main Features

The Inputs can be freely configured from the Control Panel as:
• NO/NC Input referred to GND
• Alarm/Tamper/Mask Input with Double and/or Triple Resistive Balancing
The device communicates in polling with the Control Panel on RS485 serial BUS with Proprietary protocol.
The following types can be programmed from the Control Panel:
• Theft
• Robbery
• Fire
• Technological
The following functions can be programmed for each type:
• Timing: delay of the alarm signal from 00" to 180"
• Pulse Counting: programming of the number of pulses (from 01 to 15) and amplitude to obtain the alarm condition
• Patrol Function: by associating the device with two others, a path is defined by establishing the priority parameters and the times of the path itself.
• Consent Function: association of 2 sensor devices to obtain the END function. The alarm condition occurs if both devices generate one within the programmed time.
• Self-exclusion: by establishing a number of alarms in a defined time, the sensor is automatically excluded (the tampering alarm has a fixed default self-exclusion of 5 alarms in 30')
• Customization: entering a 20-character text to define the function or location of the device.

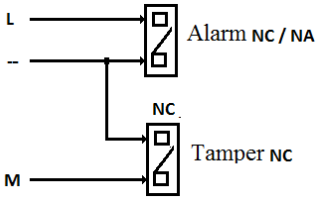
Technical Specifications

• Supply voltage: 12Vdc±5%
• Current consumption: 7mA
• Overvoltage protection: up to 35SKV
• Operating temperature: 0°C +40°C
• Dimensions [mm]: L=35; B=42; H=22
• Made in SMD technology with RISC processor
• Preconfigured address

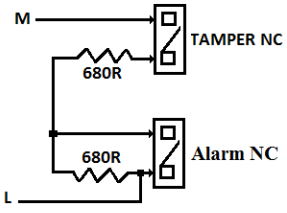
Electrical Connection



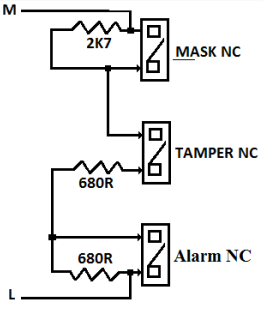
NA/NC CONNECTION



DOUBLE BALANCE



TRIPLE BALANCE



Interfaced DT Sensor - SN0012/3



Main Features

DT Sensor owned by UTC Fire&Security Article Interlogix DT105.
The technical characteristics of the sensor are shown on the manufacturer's information sheet.
Inside the sensor there is an interface circuit with our System.
The device communicates in polling with the central unit through the RS485 serial BUS.
From the Central Unit it is possible to program the following parameters:
• Type: Theft, Fire, Robbery, Technological
• Timing: alarm delay from 000" to 180"
• Consent: association of the device with another sensor to obtain the END function
• Follow me function: by associating the device with two others, a stable path is defined by making the priority and time parameters of the path itself.
• Pulse counting: programming the number of pulses (from 01 to 15) and the amplitude of the pulses themselves to obtain the alarm condition
• Self-exclusion: with a number of alarms in a defined time, the self-exclusion of that sensor is obtained
• Customization: entering a text of 20 characters to define the function or location of the device itself.

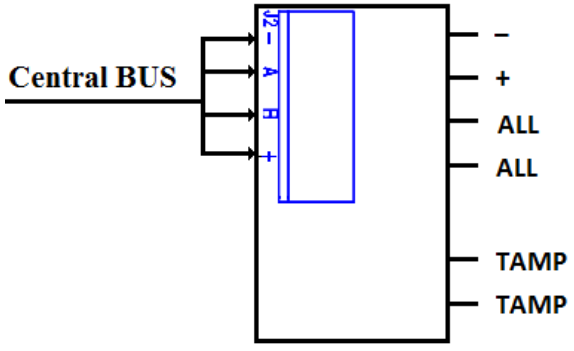
Technical Specifications

• Supply voltage: 12Vdc±5%
• Current consumption: 7mA
• Overvoltage protection: up to 35SKV
• Operating temperature: 0°C +40°C
• Dimensions [mm]: L=35; B=42; H=22
• Made in SMD technology with RISC processor
• Pre-configured address

Sensor Specifications

• Dual technology detector MW + PIR
• Range 6-12m
• Current consumption in alarm 15mA

Electrical Connection



Interfaced PIR Sensor - SN0012/4



Main Features

Composed of two Keystone modules
a) Interface module for connection to the BUS
b) Keystone Sensor Module
The device communicates in polling with the central unit via the RS485 BUS.
From the control unit it is possible to program the following parameters:
• Type: Theft, Fire, Robbery, Technological
• Timing: Alarm delay from “000” to 180”
• Consent: Association of the device with another sensor to obtain the END function
• Follow me function: By associating the device with two others, a path is defined by establishing the priority and time parameters of the path itself.
• Pulse counting: Programming the number of pulses (from 01 to 15) and the amplitude of the pulses themselves to obtain the alarm condition
• Self-exclusion: With a number of alarms in a defined time, the self-exclusion of that sensor is obtained
• Customization: Entering a text of 20 characters to define the function or location of the device itself.

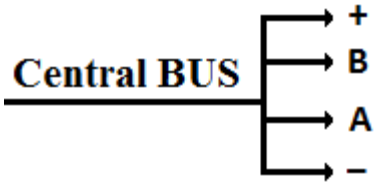
Technical Specifications

• Supply voltage: 12Vdc±5%
• Current consumption: 7mA
• Overvoltage protection: up to 35SKV
• Operating temperature: 0°C +40°C
• Coverage angle: 45°
• Container: Keystone
• Color: Black
• Made in SMD technology with RISC processor
• Pre-configured address

Sensor Specifications

• PIR detector
• Range 6m

Electrical Connection



Interfaced Temperature Sensor - SN0012/4



Main Features

The device communicates in polling with the central unit through a RS485 serial BUS.
From the control unit it is possible to program the following parameters:

- Type: Technological
- Self-exclusion: With a number of alarms in a defined time, the self-exclusion of that sensor is obtained
- Customization: Enter a text of 20 characters to define the function or location of the device itself.

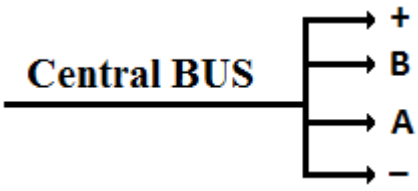
Technical Specifications

- Supply voltage: 12Vdc±5%
- Current consumption: 7mA
- Overvoltage protection: up to 35SKV
- Operating temperature: 0°C +40°C
- Coverage angle: 45°
- Container: Keystone
- Color: Black
- Made in SMD technology with RISC processor
- Preconfigured address

Sensor Specifications

- Temperature Detector
- Detection range: -15° +90°

Electrical Connection



Interfaced Twilight Sensor - SN0012/4



Main Features

The device communicates in polling with the central unit through a RS485 serial BUS.
From the control unit it is possible to program the following parameters:
• Type: Technological
• Self-exclusion: With a number of alarms in a defined time, the self-exclusion of that sensor is obtained
• Customization: Enter a text of 20 characters to define the function or location of the device itself.

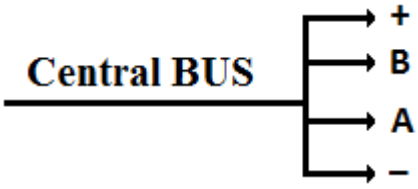
Technical Specifications

• Supply voltage: 12Vdc±5%
• Current consumption: 7mA
• Overvoltage protection: up to 35SKV
• Operating temperature: 0°C +40°C
• Coverage angle: 45°
• Container: Keystone
• Color: Black
• Made in SMD technology with RISC processor
• Pre-configured address

Sensor Specifications

• Twilight Detector
• Detection range: -15° +90°

Electrical Connection



Digital Actuator Interface - 1022/A1



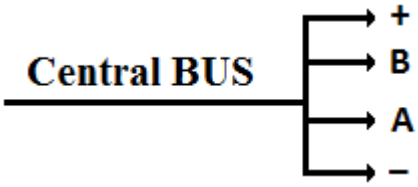
Main Features

Remote peripheral unit for digital alarm actuations: the device communicates in polling with the central unit on RS485 serial BUS with proprietary protocol.
The following parameters can be programmed from the control unit:
• Type: Security, Home Automation, Remote Activation
• Configuration: Alarm
• Relay operation: Bistable or Timed
• Alarm actuation times: from “00” ÷ “60 + 01’ ÷ 720’
• Customization: Enter a text of 20 characters to define the function or location of the device itself.

Technical Specifications

• Power supply voltage: 12Vdc±5%
• Current consumption: 7 ÷ 45mA
• Operating temperature: 0°C +40°C
• Container: ABS in DIN module
• Made in SMD technology with RISC processor
• Preconfigured address
• Maximum load of relay output: 10A – 220Vac

Electrical Connection



Access Control Interface - 1022/A01-AC



Main Features

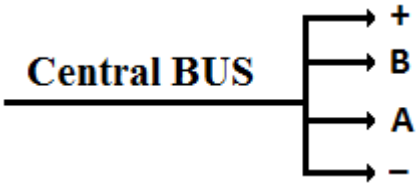
Remote peripheral unit for digital ON/OFF commands.
The device relay switches whenever the Safety block to which it belongs changes status (Inserted / Disarmed).
The device communicates in polling with the central unit on RS485 serial BUS with proprietary protocol.
The following parameters can be programmed from the control unit:

- The Relay switches only when the block to which it belongs is Inserted
- The Relay switches only when the block to which it belongs is Disarmed
- The Relay switches both when the block to which it belongs is Inserted and when it is Disarmed
- Relay operation: Bistable or Timed
- Alarm activation times: from “00” ÷ “60 + 01’ ÷ 720’
- Customization: Enter a text of 20 characters to define the function or location of the device itself.
- Maximum Relay Output Load: 10A – 220Vac

Technical Specifications

- Supply voltage: 12Vdc±5%
- Current consumption: 7 ÷ 45mA
- Operating temperature: 0°C +40°C
- Container: ABS in DIN Module
- Made in SMD technology with RISC processor
- Preconfigured address
- Maximum Relay Output Load: 10A – 220Vac

Electrical Connection



Interfaced Self-powered Siren – sn 0013/2



Main Features

NB: Siren owned by AMC ELETTRONICA
The technical characteristics of the Siren are shown on the manufacturer's information sheet
Inside it is housed a SENEDA device that interfaces with our NEXUS NEW system.
The Interface is a remote peripheral unit for digital alarm actuations and the device communicates in polling with the central unit via an RS485 serial BUS with proprietary protocol.

- Alarm Activation Command
- System Status Command
- Siren Tampering Line

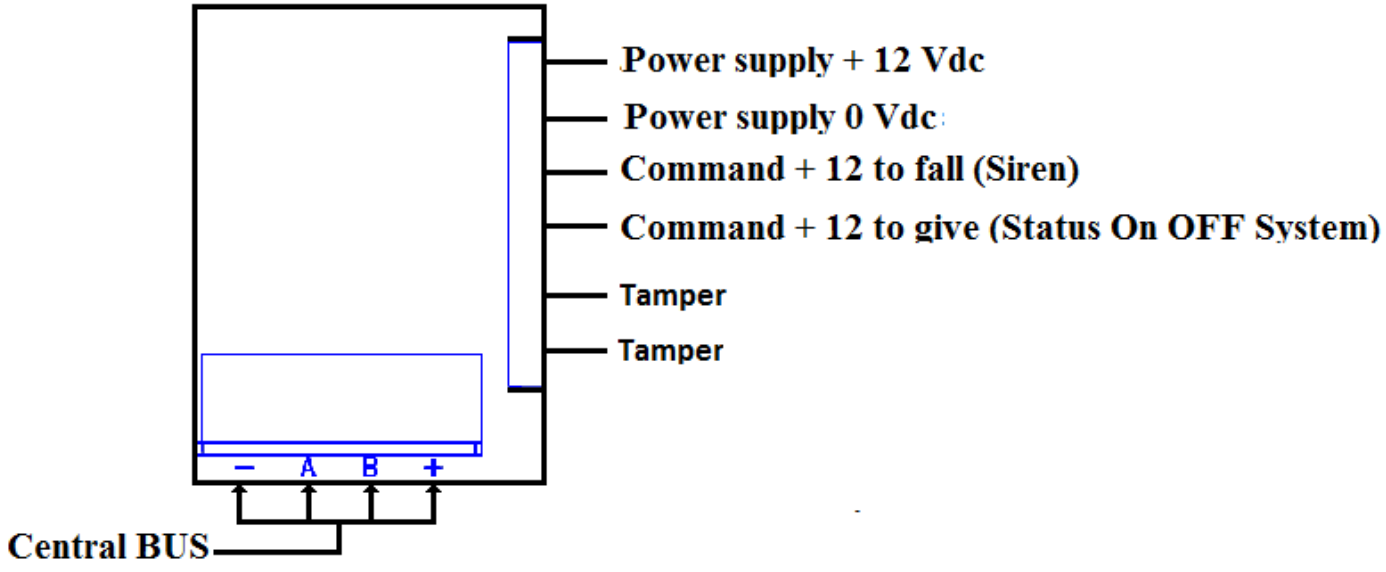
The following parameters can be programmed from the control unit:

- Type: Security, Home Automation
- Activation times: Alarm from "00' ÷ 15'
- Customization: Enter a text of 20 characters to define the function or location of the device itself.

Technical Specifications

- Supply voltage: 12Vdc±5%
- Current consumption: 7mA
- Operating temperature: 0°C +40°C
- Made in SMD technology with RISC processor
- Preconfigured address

Electrical Connection



Interfaced Domo Socket - 1022/A3



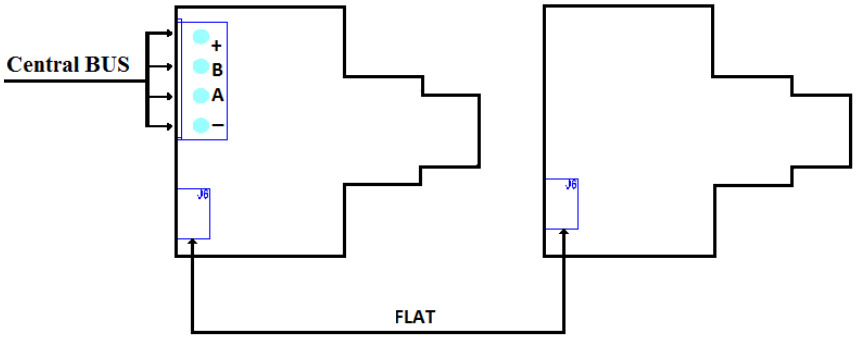
Main Features

Remote peripheral unit for home automation actuations in Keystone container.
The device has a 15A - 220Vac relay output with Anti-spark circuit to control household appliances.
The device communicates in polling with the central unit on RS485 serial BUS with proprietary protocol.
From the control unit it is possible to program the following parameters:
• Type: Home automation, Remote activation
• Relay operation: Bistable or Timed
• Activation times: Alarm from “00” ÷ “60 + 01’ ÷ 720’
• Customization: Enter a text of 20 characters to define the function or location of the device itself.

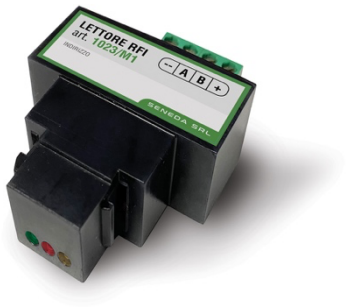
Technical Specifications

• Power supply voltage: 12Vdc±5%
• Current consumption: 7 - 45mA
• Operating temperature: 0°C +40°C
• Made in SMD technology with RISC processor
• Relay output with Max Load = 15 A – 220 V ac
• Relay operation: Bistable and Timed
• Container: N°2 Keystone modules
• Preconfigured address.

Electrical Connection



RFID Transponder Key Reader - 1023/M1



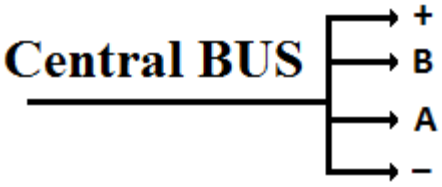
Main Features

This intelligent remote peripheral unit communicates with the control unit via a serial BUS with a proprietary protocol.
Provides the control unit with the data read on the digital Transponder keys for activating/deactivating the system.
• Data transfer: Reading of keys with data exchange using transponder technology (no physical contact)
• The transponder reading distance is 1.2cm
Signal LEDs:
• Red: ON/OFF GENERAL BLOCK
• Yellow: ON/OFF PARTIAL BLOCK
• Green: SERVICE OR ANOMALY SIGNALS
The following parameters can be programmed from the control unit:
• Customization: Entering a 20-character text to define the function or location of the device itself
• Timing: Insertion delay from 000” to 180”

Technical Specifications

• Power supply voltage: 12Vdc±5%
• Current consumption: 18mA
• Operating temperature: 0°C +40°C
• Container: Keystone Module
• Preconfigured address
• Made in SMD technology with RISC processor

Electrical Connection



Remote Keyboard - 1023/M2



Main Features

User interface for local management of Security and Home Automation functions. It communicates with the control unit via a serial BUS with a proprietary protocol.

- No. 3 LED signals:
  - Red: ON/OFF GENERAL BLOCK
  - Yellow: ON/OFF PARTIAL BLOCK
  - Green: SERVICE OR ANOMALY SIGNALS
- 16-key silicone keyboard with click function
- 20x2 character backlit display

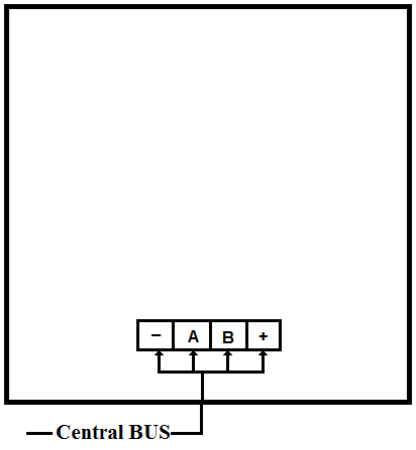
The following parameters can be programmed from the control unit:

- Customization: Enter a 20-character text to define the function or location of the device itself
- Timing: Insertion delay from 000” to 180”

Technical Specifications

- Power supply voltage: 12Vdc±5%
- Current absorption: 50mA
- BUS485 transceiver with protection against electrical discharges up to 15SKV
- Made in SMD technology with RISC processor
- Preconfigured address

Electrical Connection



Keyboard / Touch Monitor - 1023/M



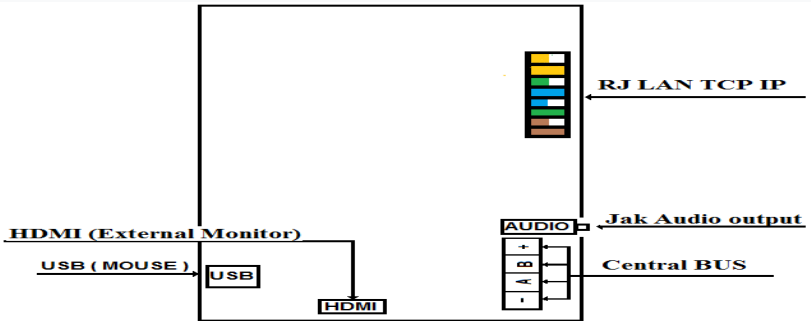
Main Features

• User Interface, 7.5" Touch Display
• The device communicates with the control unit via BUS and TCP IP Network.
• It manages two fundamental functions:
• Security and Home Automation
• Video Alarm and Video Surveillance
• The following optional cards can be housed on board:
• HDMI card to manage Video functions with a larger screen
• Audio Output
• USB output to connect a Mouse and navigate within the Video Surveillance menu
• The device is equipped with:
• Calendar Clock
• Room temperature reader
• From the control unit it is possible to program:
• Timings for Security functions
• Personalization by entering a 20-character text

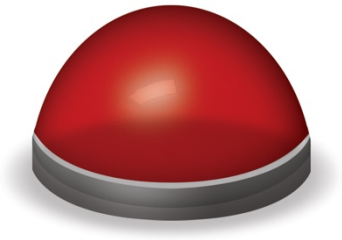
Technical Specifications

• Power Supply Voltage: 12Vdc±5%
• Current Consumption: 125mA
• Overvoltage Protection: Up to 15SKV
• Operating Temperature: 0°C +40°C
• Container: ABS Plastic
• Preconfigured Address
• Made in SMD technology with RISC processor
• Preconfigured BUS network address
• LAN network address Freely programmable
• Dimensions [mm]: B125 mm – L 20 mm – H 60 mm

Electrical Connection



Domo Clima Interface and Remote Controls - 1024/D1

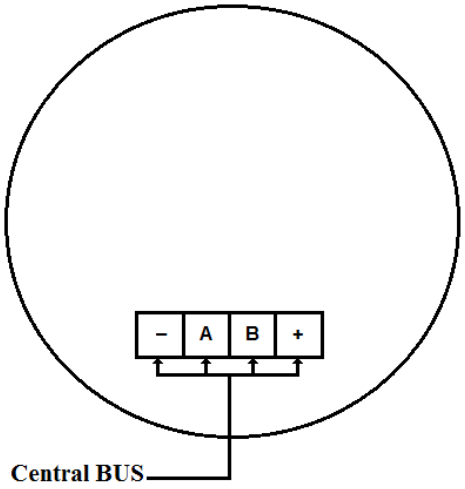


Main Features

Remote home automation unit that communicates with the control unit via a serial BUS with a proprietary protocol.
The card allows the storage of 5 remote controls and for each of them it allows the storage of 5 functions.
All functions can be freely managed remotely or via a Touch keyboard.
The control unit also allows you to create a block with specific functions for managing air conditioning systems.

Technical Features

- Power Supply Voltage: 12Vdc±5%
- Current Consumption: 80mA
- Overvoltage Protection: Up to 15 SKV
- Operating Temperature: 0°C +40°C
- Infrared Radiation: 360°
- Beep function for both acquisition and commands
- Made in SMD technology with RISC processor
- Preconfigured Address
- Base Container in ABS, Cover in Polycarbonate



Domo Automatismi Interface – 1024/D4

Main Features

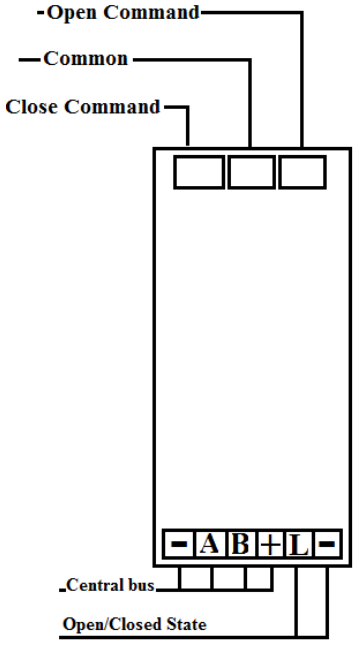
Remote Home Automation Unit, communicates with the control unit via a serial BUS with proprietary protocol.

- The board allows management of Automation Systems (Awnings, Shutters, Gates, etc.).
- All functions can be freely managed remotely or via Touch Keyboard.

Technical Specifications

• Power Supply Voltage: 12Vdc±5%
• Current Consumption: 80mA
• Overvoltage Protection: Up to 15 SKV
• Operating Temperature: 0°C +40°C
• Control Relay with loads up to 10A 220Vac
• Bistable and Timed Relay Operation
• Made in SMD technology with RISC processor
• Preconfigured Address
• Base Container in ABS one DIN module

Electrical Connection



Domo Interface for Electricity Consumption Control – 1024/D5

Main Features

Remote home automation unit communicates with the control panel via a serial bus with a proprietary protocol.

- Upon request via notification from the app, the device will send instantaneous consumption data.
- It also allows you to set 5 alarm threshold levels (values expressed in Watts) in 1000 Watt increments.

Caratteristiche Tecniche

- Tensione di Alimentazione: 12Vdc±5%
- Assorbimento di Corrente: 80mA
- Protezione alle Extratensioni: Fino a 15 SKV
- Temperatura d'esercizio: 0°C +40°C
- Sensore carichi elettrici fino a 5,5 KW
- Realizzato in tecnologia SMD con processore RISC
- Indirizzo Preconfigurato
- Contenitore Base in ABS un modulo DIN

Collegamento Elettrico



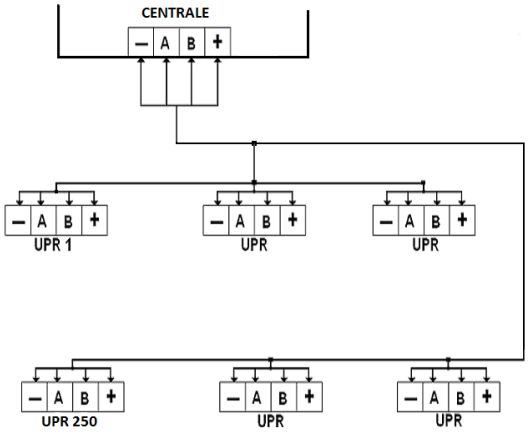
Connections and Tests

BUS RS485 with SENEDA 4.0 protocol

Connection network between the Control Unit and all the Security, Domo / Technological and Keyboard and Touch Keyboard devices.
On the control unit there is the RS485 terminal block on which to connect the data pair and the power supply of the devices.
The maximum length of the BUS network is 800m, the control unit can manage up to 250 addresses.
The Bus is a balanced network with a typical impedance of 120Ω.
Use a twisted and shielded pair with a section of 0.75mm.

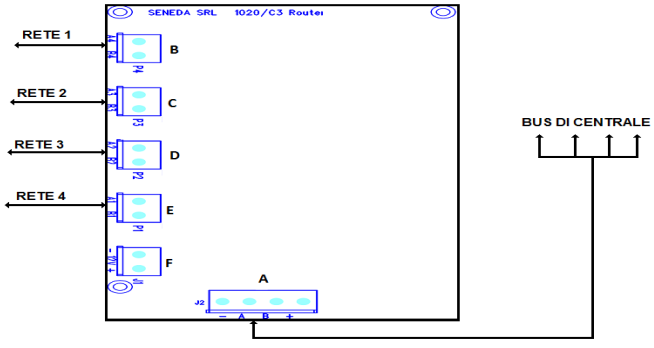
BUS connection between the Control Unit and UPR Devices

Our Interface devices are marked with the physical address,
Please note: In the same system, check that there are no devices with the same address.



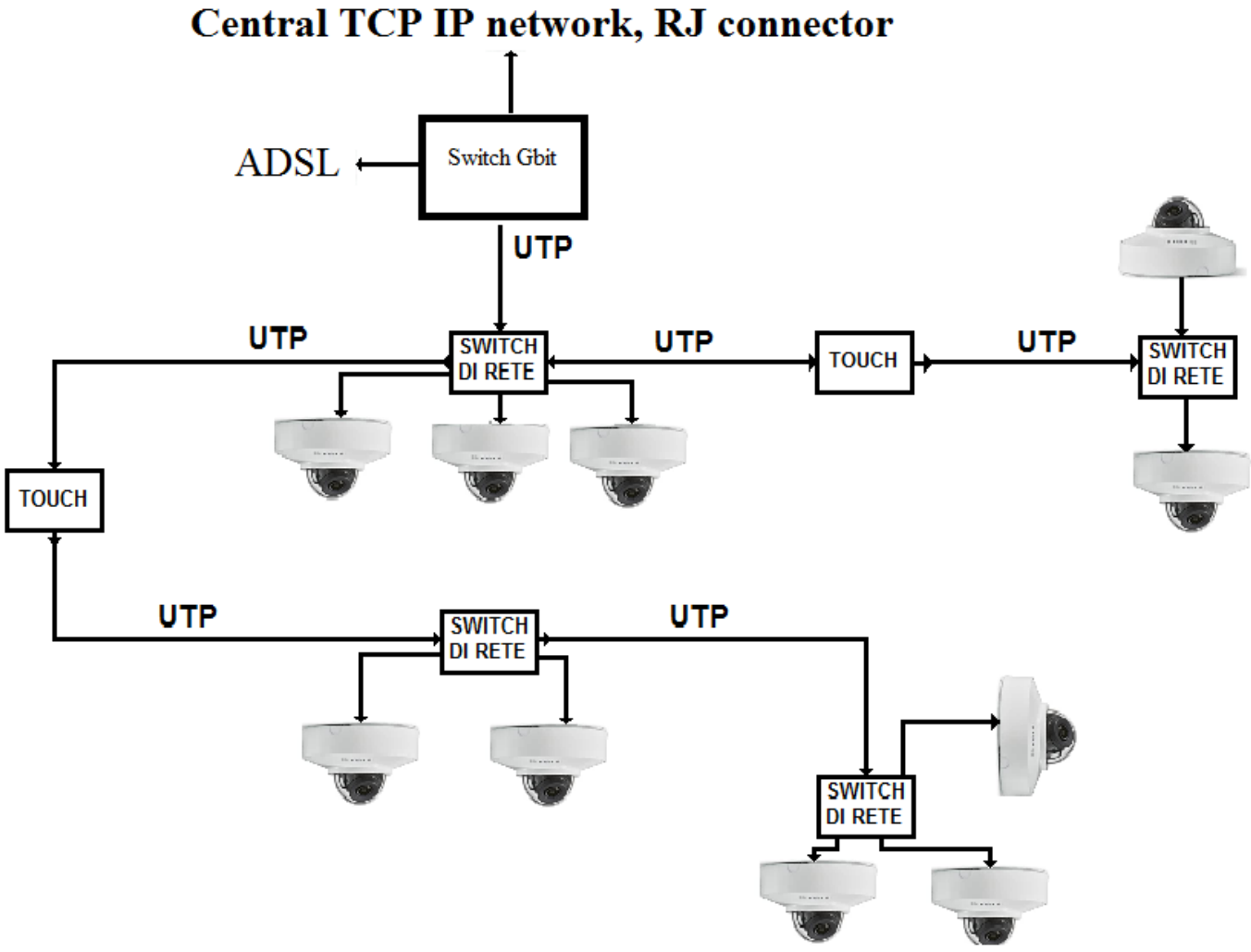
Power the control unit and perform the following checks
1. Measure the supply voltage between the terminals (+ and -) of the BUS, the value must be between 11.8 and 13.9Vdc
2. If the voltage value is lower than that mentioned, there may be a short circuit on the power cables on the network, therefore it must be identified and removed
3. Perform the same test on all Remote Power Supplies possibly installed on the network
4. Disconnect the positive cable of the network power supply and connect an Ammeter in series.
The measured value must be less than 2A.

If the value is higher, additional power supplies must be installed along the network (article code 1020/C2).
NB: Connect all the GNDs (Negative of the Central Power Supply and Remote Power Supplies) together.
If the value is equal to zero, the network may be interrupted.
To calculate the capacity of the buffer battery, multiply the current value read at point (4) by the autonomy time you want to give to the system in the absence of a primary power supply network.
The compartment of the Control Unit supports a 7Ah battery (optional additional container with compartment for a 17Ah battery).
In complex installations, with multiple lines and different cable impedances, use our RS485 ROUTER device, item code 1020/C3 as shown in the following diagram:



TCP IP Network

Connection network between Control Panel, Cameras and Touch Keypads.



The Central CPU has an RJ connector:
To connect the cameras to the network and the ADSL network, you must use a Network Switch (Gbit)
The Central can manage up to 150 cameras including Touch Keyboards
the maximum distance between the various network switches is 100m.
Use only Gbit Switches and UTP cat. 6 cable.
The cameras must be powered at 12Vdc and have a current consumption of approximately 150 mA (800 mA with active IR)
NB: (When the Video Analysis function is activated, the IR LEDs must be deactivated and the area must be illuminated with alternative supports, taking care to position the light source 1.5 m from the camera lens)
The power supply must be taken from a buffered source, as the Central could detect an alarm condition due to a lack of power supply or loss of video signal.
Use our Remote Power Supplies (Art. 1020/C2).
The Control Panel manages video streams from cameras with ONVIP protocol (BOSCH, DAHUA, HIKVISION, etc.)
The Control Panel manages Video Analysis exclusively from BOSCH DINION series cameras.
For programming of Video Analysis functions, consult the BOSCH manual.
It is possible to use other cameras with Video Analysis by taking the alarm from it and interfacing it with our Sensor devices and then enabling the association between camera and Sensor in programming.

First Operation = ADSL NETWORK CHECK

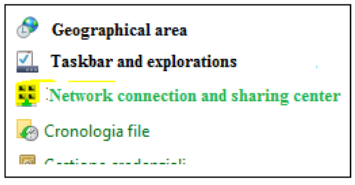
• Test the Internal LAN NETWORK and the Internet Router and check the free addresses and which family they are supported on
Proceed as follows:
- Set the PC network to Obtain an IP Address Automatically
- Open the Command Prompt and Type ipconfig
The monitor will display:
a) IPv4 = Free network address for example 192.168.X.XX
b) Subnet Mask (Standard data) 255.255.255.0
c) Gateway = 192.168.X.X
Store this data for subsequent programming (see Chapter NETWORK CONFIGURATION page 42)

PC configuration for first connection

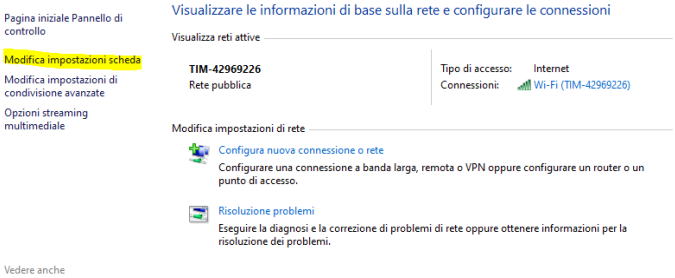
The control unit is configured in the factory with the default address 192.168.1.225, therefore, in this case, you can conveniently use the IP address 192.168.1.200 for the connection, which must be typed in the text field corresponding to the item “IP address:”, while in the text field corresponding to “Subnet mask” write the value 255.255.255.0

The programming TOOL is made on the WINDOWS platform.
The minimum PC specifications must be:
• Windows 10 and later
• Intel 10 and/or Ryzen 5 processor
• RAM 8Gb -/- 256Mb
• Minimum free space on Hard Disk 250Gb
• RJ LAN serial port

Download the program from the website www.seneda.it (to download the program you must fill out the form) load it onto the PC and follow the instructions on the screen that the program displays.
Before using the Tool, you must ensure that the PC is correctly configured for the LAN connection.
Follow the procedure described for Windows
• From the Control Panel, Select
1. Internet Network
2. Network and Sharing Center



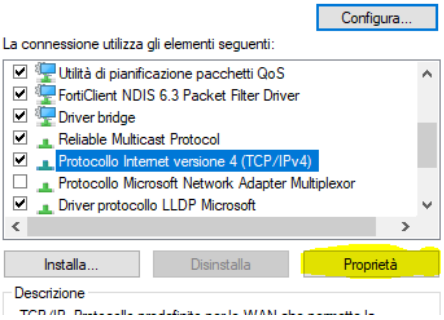
The following screen will open:



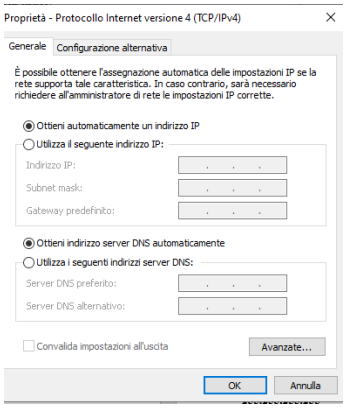
With the Right Mouse Button, disable all network devices that are NOT used to connect to the control panel (for example BlueTooth Network Connection) and leave them disabled until the end of the control panel initialization procedure. Then:

• Right-click on the icon to be used, from the drop-down menu click on the item "Properties".
• Select:
◦ Change card settings

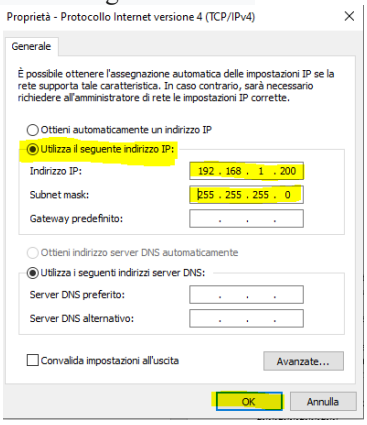
The following screen will open:



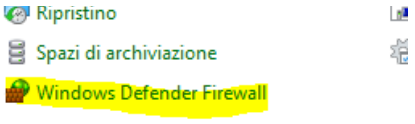
In the window that appears, click on “Internet Protocol Version 4 (TCP/IPv4)”, highlight it and then “Properties”. The following screen will open:



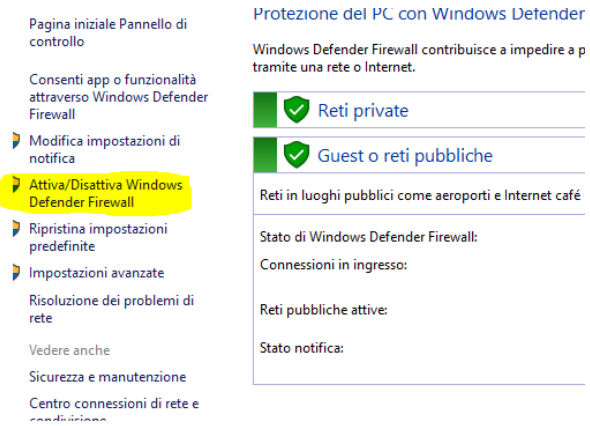
In the window that appears, click on the item “Use the following IP address:”



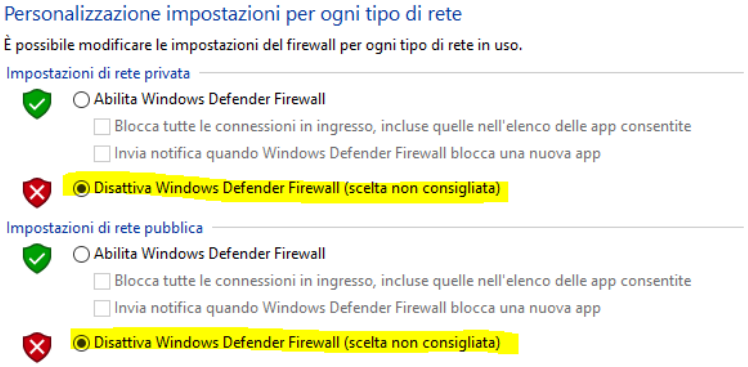
• The control unit is configured in the factory with the default address 192.168.1.225, therefore in this case you can conveniently use the IP address 192.168.1.200 for the connection, which must be typed in the text field corresponding to the item “IP address:”
• In the text field corresponding to “Subnet mask”, write the value 255.255.255.0
• In the text field corresponding to “default gateway”, write the value 192.168.1.1
• Click on the “OK” button in the “Internet Protocol (TCP/IP) Properties” window and then on the “OK” button in the “Local Area Connection (LAN) Properties” window to confirm the changes.
• Connect the PC to the control unit using the cable supplied and start the program. “NEXUS PRO”
• Open the “Control Panel” and select the “Windows Defender Firewall” item



• Open “Windows Defender Firewall” and click on the item in the left menu “Turn Windows Defender Firewall on/off”

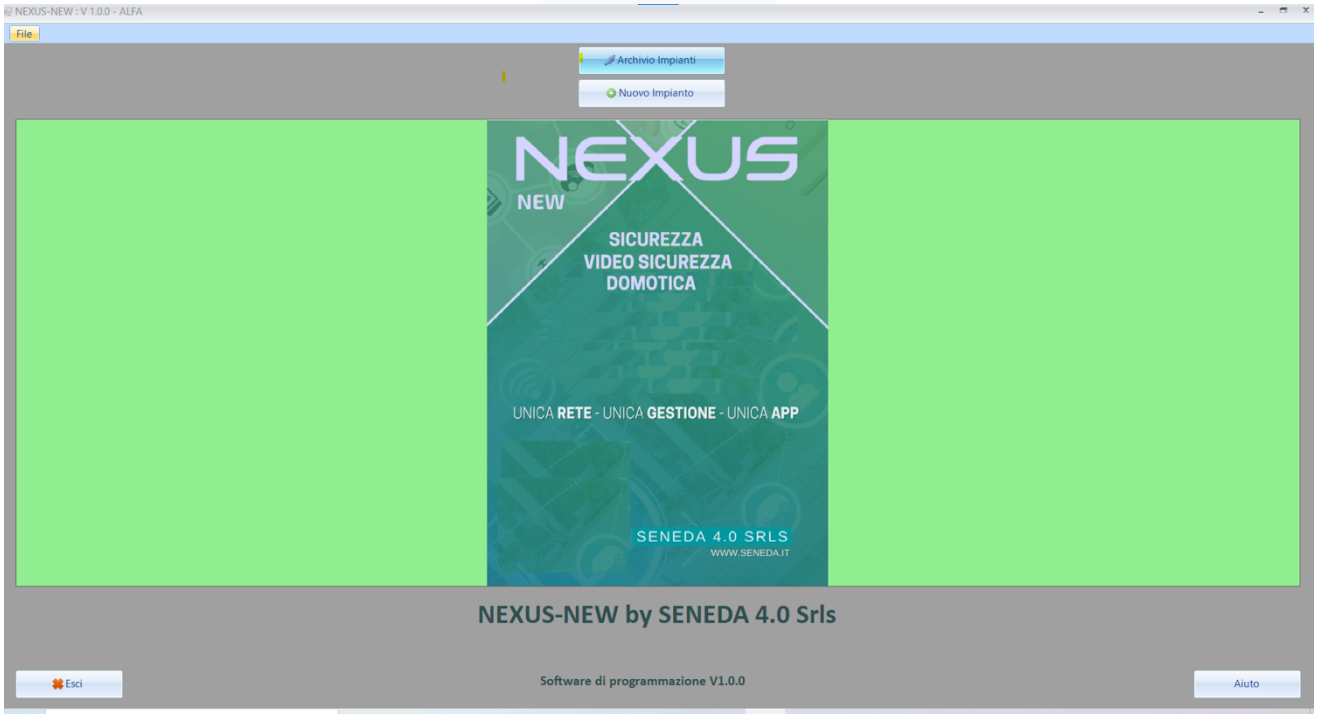


Disable the firewall until the end of the initialization and configuration operations of the control panel



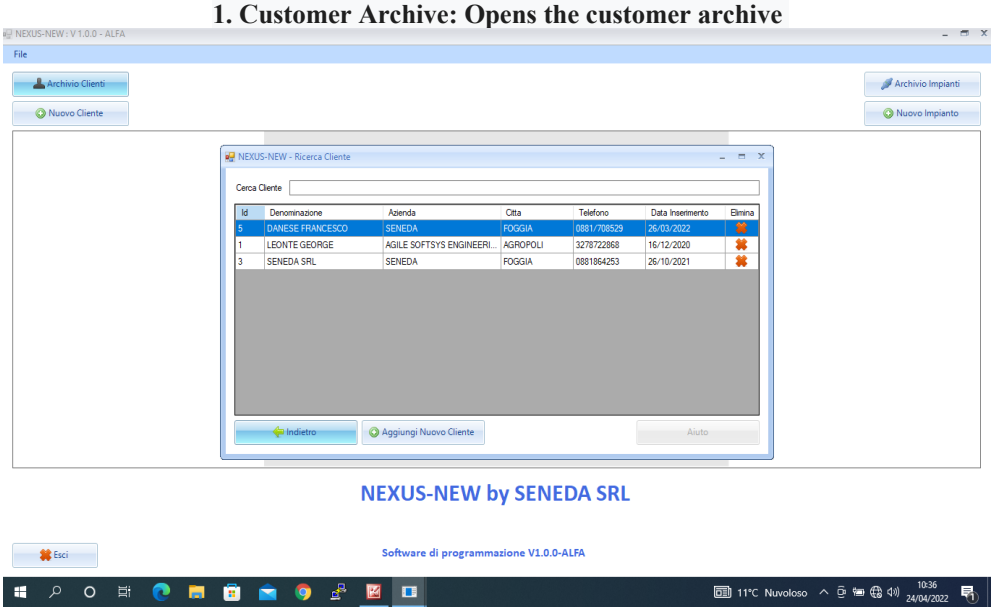
Warning:
Always remember to restore the PC configuration after configuring the control panel by performing the following operations:
• Restore the configuration of previously deactivated network devices
• Restore the configuration of the network device used to connect to the control panel
• Restore the status of Windows Firewall Defender

HOME Screen



1. **Archivio Clienti**: Opens the customer archive screen
2. **Nuovo Cliente**: Allows the programming of a new Client
3. **Aiuto** : Help Page Programming Guide
4. **Esci** : Exits the program.

1. Customer Archive: Opens the customer archive



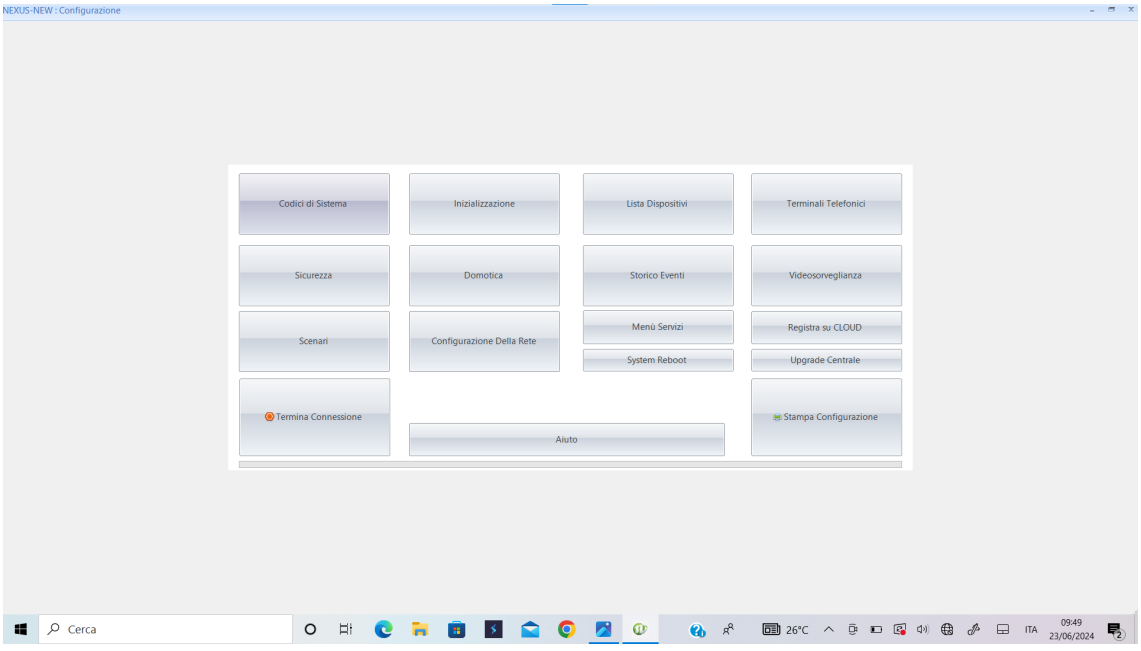
List of customers already in the archive. For each customer the screen shows the Plant data
To enter the plant select and double click
FUNCTION KEYS
DELETE: Delete the customer from the archive
BACK: Return to the Home page
ADD NEW CUSTOMER: Allows you to insert a new customer

2. Add New System: Allows the programming of a new System

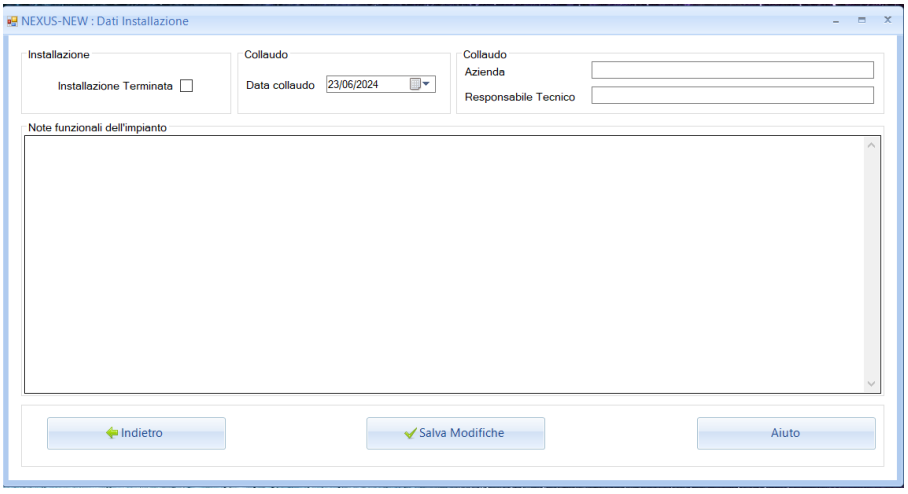


CENTRAL: Enter the data as shown in the diagram
• **Master Code:** Unique 4-digit identification code for the Central. The same applies as the Password to access the APP
• **Central Sim:** Telephone Number of the SIM to be entered into the Central
• **Server Address:** Address of the Server to which the Central is connected (DO NOT CHANGE)
• **Central Address:** The default address of the Central is 192.168.1.225
• **SW and HW:** Software and Hardware versions of the Central
• **Installation Date:** By clicking on the drop-down menu you can select the date
• **Testing Date:** By clicking on the drop-down menu you can select the date
CUSTOMER: Enter the customer's personal data: Company, Address, City, Postcode, Telephone, Email.
• **Connect:** Allows Local/Remote Connection (See specific next chapter)
• **Restore:** After the first Installation the PC stores all the configuration data programmed in the Control Panel, in case of replacement of the Control Panel this button allows you to download the last stored configuration to the new Control Panel.
• **Reset:** Deletes all the previously programmed data bringing the Control Panel to the default data

• **View Configuration:**
This screen allows you to view the data programmed on the control panel previously.
For a new system the screen is not accessible.

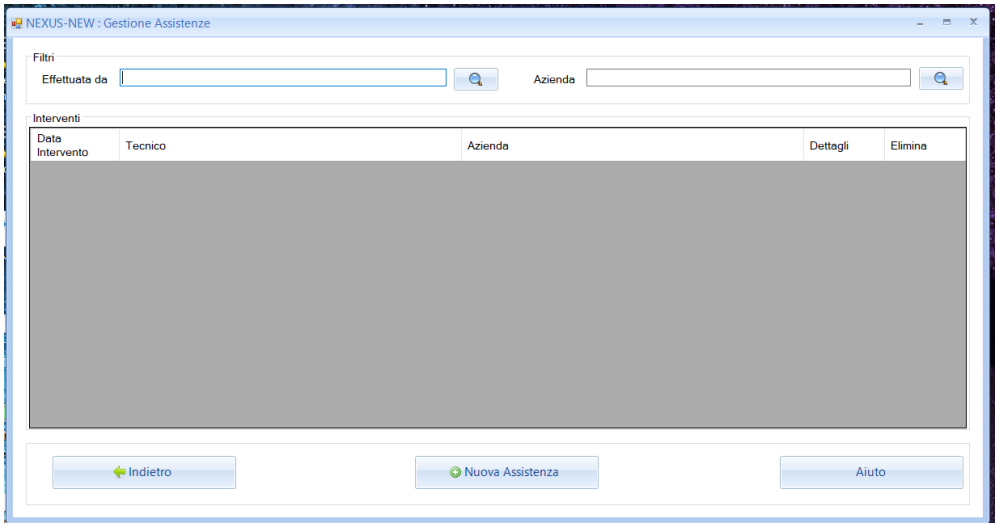


• Installation Data:



This screen allows you to enter data relating to the physical installation of the system. Enter the data as shown in the diagram and save it.
For a new system, the screen is not accessible.

• **Assistance Management:** Allows you to create a maintenance intervention history

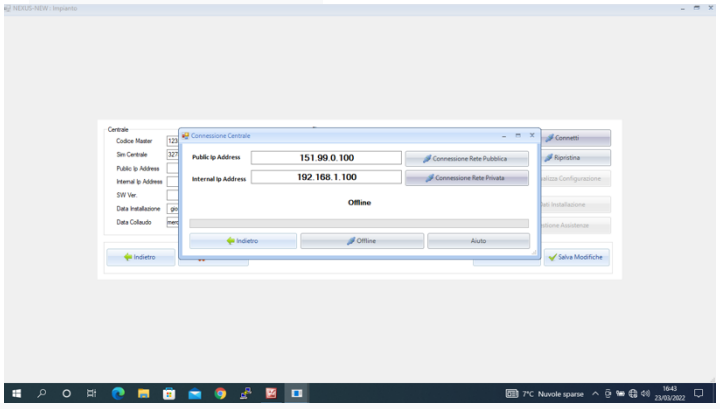


This screen allows you to enter notes of the assistance interventions carried out on the system.
Enter the data as shown in the diagram and save them
For a new system the screen is not accessible .

• **Back:** Return to the previous screen
• **Delete:** Delete all the data entered
• **Help:** Help page for programming assistance
• **Save System:** Save the data entered
• **Connect:** Position the switch on the control unit as shown in the figure in the SERVICE position

Local / Remote Connection





1) Move the Diverter to the Maintenance position
2) From the Screen, pressing the “Connect” button will access the following screen:

Description:
• Public Network Connection Button: Allows the control unit to be connected remotely
• Private Network Connection: Allows direct local connection between PC and Control Unit
• Help: Programming help page
• Back: Returns to the previous menu
• Once the Local/Remote connection has been made, the following General Menu Screen appears:

Main menu

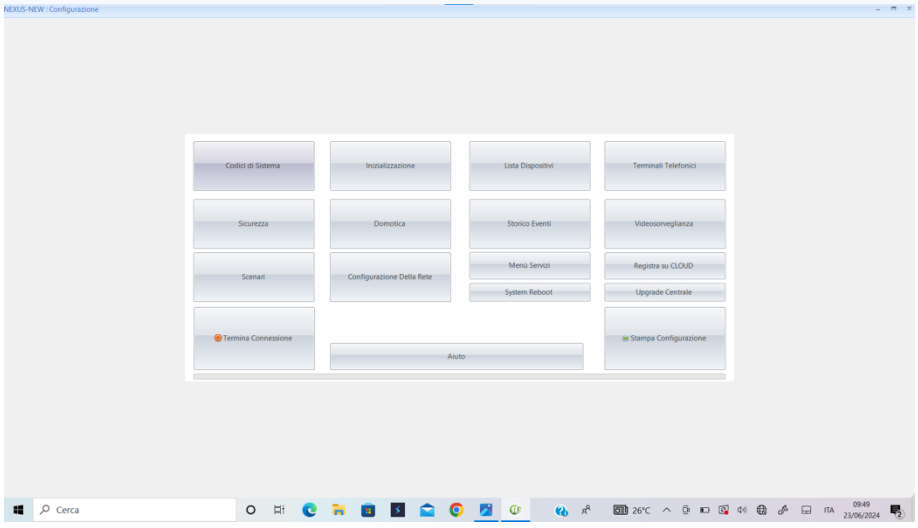
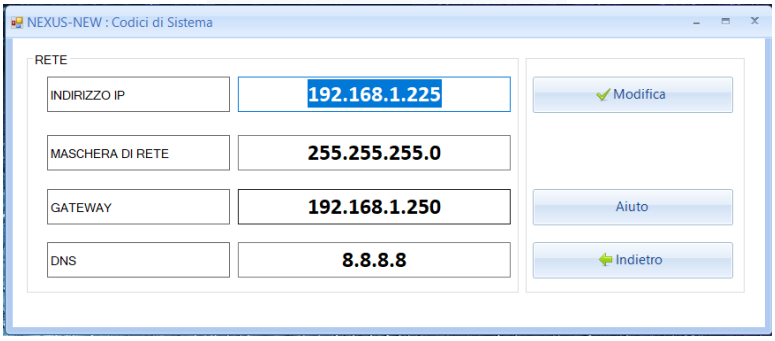


Figure 1

The list and order of operations to be performed for programming
• NETWORK CONFIGURATION
• SYSTEM CODES
• INITIALIZATION
• LIST AND PROGRAMMING OF DEVICES
• TELEPHONE TERMINALS
• SECURITY (SEE BELOW MENU)
• HOME AUTOMATION (SEE BELOW MENU)
• VIDEO SURVEILLANCE (SEE BELOW MENU)
• SCENARIOS
• EVENT HISTORY
• SERVICES MENU = Network Filter + System Reboot + Central Upgrade
• RECORD ON CLOUD
• TERMINATE CONNECTION
• PRINT CONFIGURATION: Allows you to print a paper archive of the programming performed
• HELP: Help page for programming assistance

NETWORK CONFIGURATION



Depending on the data read from the Network check (Page 34)
If the Network is on the same family 192.168.1.XX you can proceed with the programming

If instead the Network is on a different family and has a different Gateway 192.168.X.XX **change the connection parameters both** on the Control Panel and on the PC
1) Change the IP Address by choosing a free IP Address
2) Leave the Network Mask unchanged
3) Enter the new Gateway
4) Change the DNS parameter to **8888**
• Save the data entered with the Modify button
• Click on the Back button
• The Main Menu Screen appears
• Click on the Terminate Connection button
• The Screen appears

Make the same changes on the PC following the procedures described on page 34/35/36

Have the Internet Network Operator open the ports
• 1883, 554, 8554 , 8888 , 9999 , 11000 , 11001
On the address that is assigned to the Central

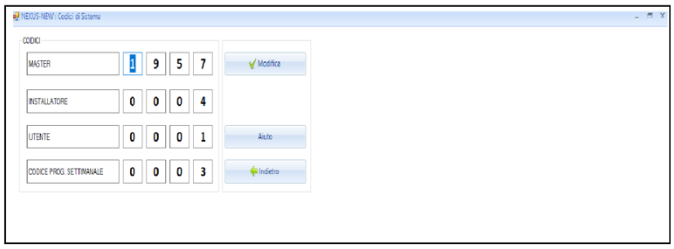
Reconnect the PC Central using the new network data entered

Make the same changes on the PC following the procedures described on page 34/35/36

Have the Internet Network Operator open the ports
• 1883, 554, 8554, 8888, 9999, 11000, 11001
On the address that is assigned to the Central

Reconnect to the Central PC using the new network data entered

System Code Programming Menu



• Master Code
The Master Code is a unique code that allows the Control Panel to be recognized Remotely. The Code is NOT modifiable!

MASTER	X	X	X	X

• Installer Code
The Installer code is a code that allows the same to put the control unit in Service mode from LCD or Touch KEYPAD
The Code can be changed by entering the new data and saving.
In the active state (normal operation) it is accepted only if all the Safety Locks are off (Disarmed).
The code allows access to the connection between the Control Unit and the Programming TOOL both locally and remotely.

INSTALLATORE	0	0	0	4

◦ Click on the first digit
◦ Edit the Digits
◦ The cursor automatically advances digit by digit
◦ Save with the EDIT button

• User Code
• The USER code is a code that allows the user to put the control panel in SERVICE mode
The code in the active state (normal operation) is accepted only if all the
Security blocks are off (Disarmed).
The Code allows the user to access the User menu.

UTENTE	0	0	0	1

◦ Click on the first digit
◦ Change the Digit
◦ The cursor automatically advances to the second, etc.
◦ Save with the MODIFY button

• Weekly Security Programmer Code
Programming and Changing the Automatic Activation/Deactivation code of the Security Locks by the Weekly Time Programmer.

CODICE PROG. SETTIMANALE	0	0	0	3

◦ Click on the first digit
◦ Change the Digit
◦ The cursor automatically advances to the second, etc.
◦ Save with the EDIT button

• EDIT: Save the data entered
• HELP: Programming help page
• BACK: Return to the previous menu

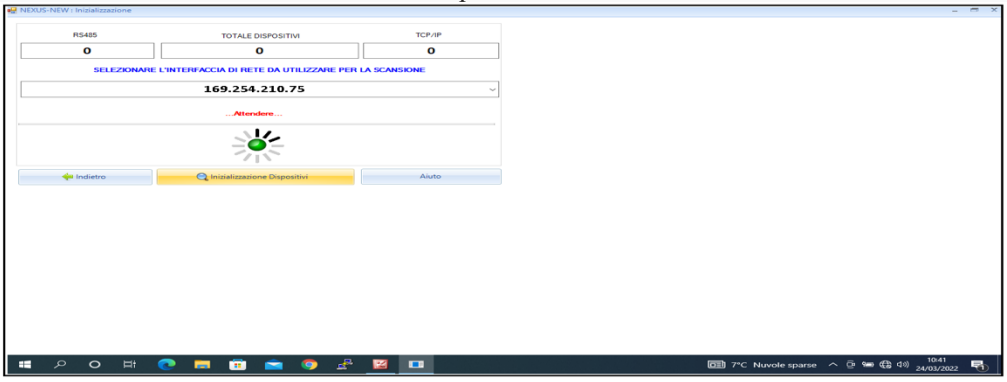
System Initialization

Start button for automatic search of devices connected to the BUS Network (Addressed Security and Domo/Technological Interface Devices) and to the LAN TCP IP network (Cameras).
NB: TOUCH devices have a double Address for both the BUS and IP networks.



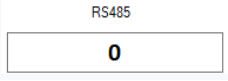
The Screen allows you to select the address of the LAN network on which the Cameras and Touch are Installed.

Select the Network Interface to use for the Scan: From the drop-down menu select the network address then Device Initialization:

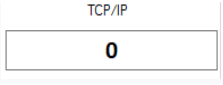


The Control Unit automatically searches for devices connected to both the BUS and LAN networks.
The Cursor with the word Wait indicates the search phase.
The search (depending on how many devices have been connected) can last several minutes!

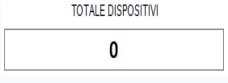
At the end of the search:



Indication of the number of devices found on the Bus network



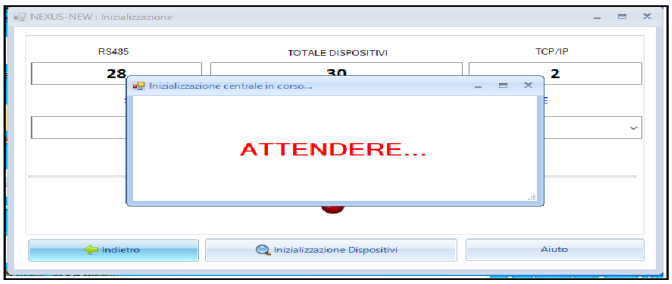
Indication of the number of devices found on the LAN network



Indication of the total number of devices found on the two networks

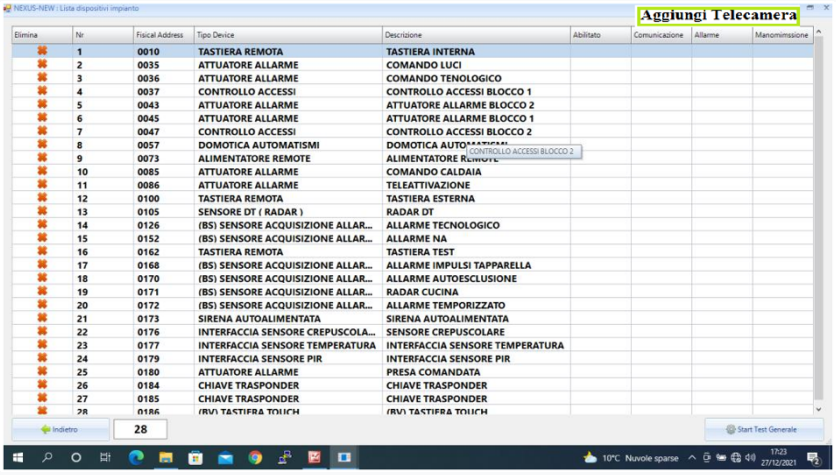
- **HELP**: Programming help page
- **BACK:** The following screen appears

NB: the control unit automatically searches the LAN network exclusively for Bosch Dinion series cameras.
If cameras from other brands with Onvif protocol have also been installed, they must be entered manually.

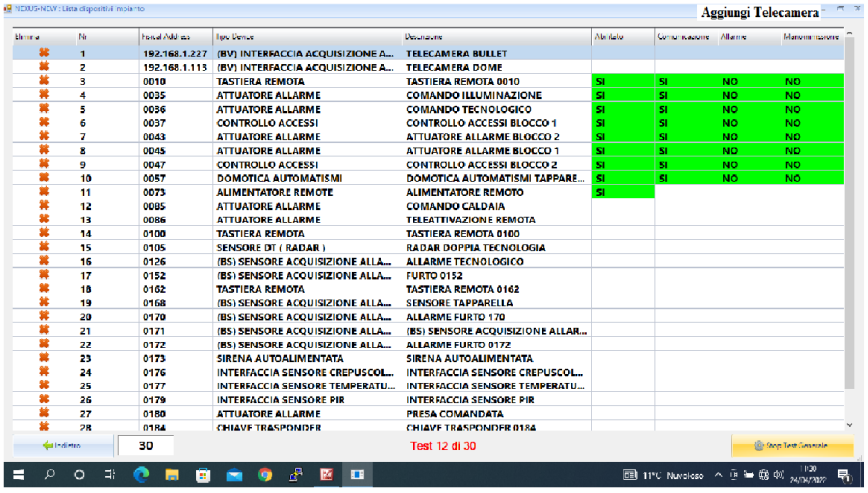


If the number of devices found is correct, press the BACK button
The control unit stores the devices found during the search phase and at the end of the wait the Main Screen appears.
From the Main Screen (Figure 1), by selecting “Device Programming”, you can access the general list of all devices.

Device List

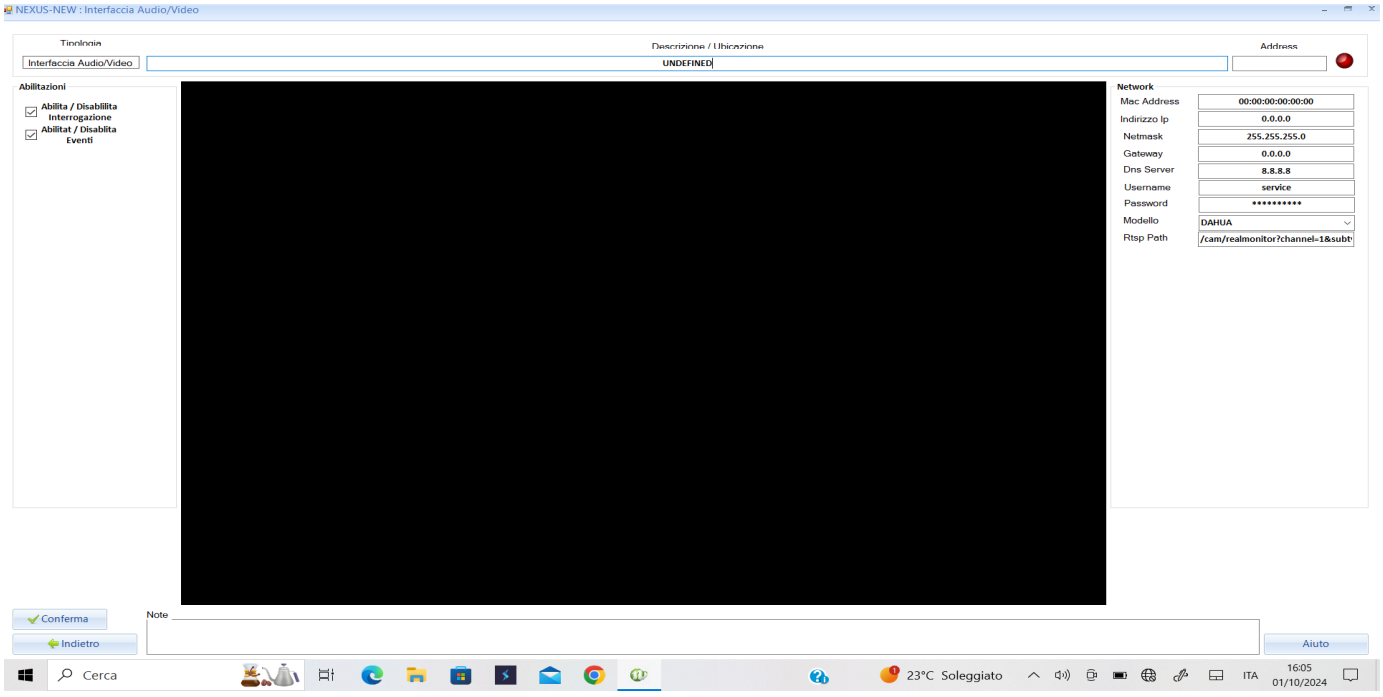


Description:
• Delete: Clicking on the asterisk deletes the device from the Query
• Nr: Chronological Order of the devices
• Physical Address: Physical address of the device, for the Cameras the IP address is indicated
• Device Type: Indicates the type of device
• Description: Description that is associated with the device if already Programmed, otherwise the box is empty
• Start General Test: Performs a general test of all the devices in the BUS network, in particular:
◦ Enabled for Operation: Green Enabled - Red Disabled
◦ Communication Status: Green Correct Communication - Red Incorrect or Absent Communication
◦ Alarm Status: Green Rest Status - Red Alarm Status
◦ Tamper Status: Green Rest Status - Red Alarm Status



Please note: the Control Unit automatically searches the LAN network exclusively for Bosch Dinion series cameras.

If other Brand Cameras with Onvif protocol have also been installed, they must be inserted manually.
To insert manually proceed as follows:
1) From the device list, click on the button: Add Camera
The following screen appears:



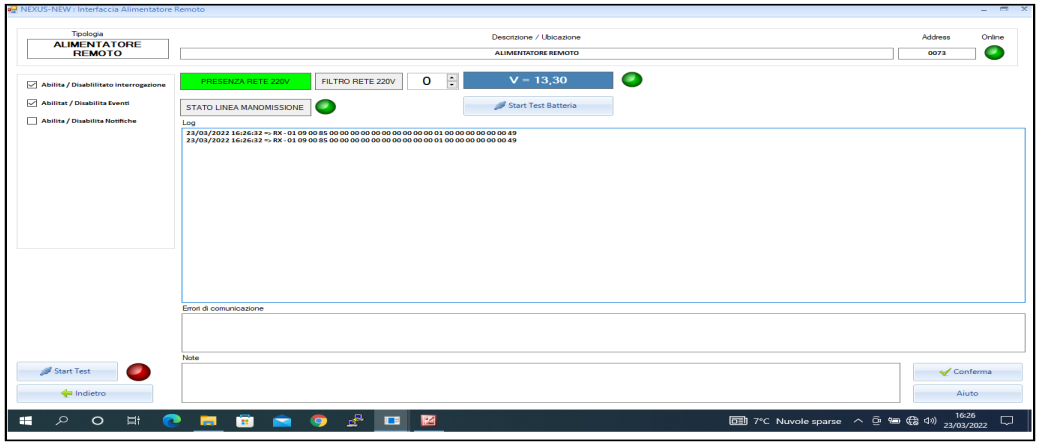
Enter the following data:
Address: Enter the IP address of the Camera 195.168.X .XX
Mac Address: Enter the Mac Address of the Camera
Address: Enter the IP address of the Camera 195.168.X .XX
Netmask: 255.255.255.0
Gateway: Gateway of the Camera 192.168.X.X
DNS Server: 8.8.8.8
Username: Username of the Camera
Password: Password of the camera
Model: from the drop-down menu select the Brand of the Camera
Rtsp Path: Default
Undefined: Enter a 20-character text to define the function or location of the camera
Confirm: Confirm the data entered and after a few seconds the image of the camera should appear.

Device Programming

• Selecting one of the devices allows programming the operating parameters.

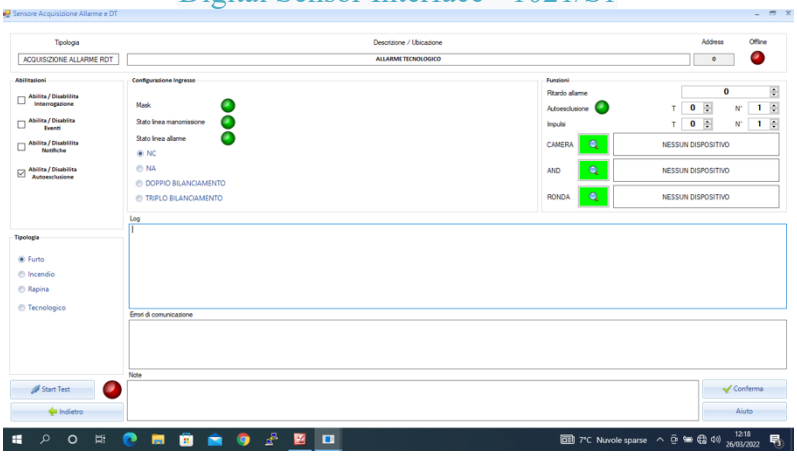
Remote Power Supply – 1020/C2

Device for controlling and managing the data of the Remote Power Supplies located along the network of both the BUS and the IP network.



- Description:
- **Type:** Indication of the device type.
- **Enable / Disable device query:** Disables Device query
- **Enable / Disable Events:** Disabled the device does not generate events, they are stored in the History.
- **Enable / Disable Notifications:** Disables the sending of Events (APP, SMS, etc.)
- **Description / Location:** Allows the entry of a 20-character text to define the Function and/or Location.
- **Address:** Indicates the physical address of the device.
- **220 Vac Network Presence:** Indicates the presence of the primary network.
  "In case of absence the box turns red with the writing "NETWORK ABSENCE".
- **220 Vac Network Filter:** Allows you to insert a time filter (from 01'÷15') before sending the Network Absence report to the Control Unit.
- **Start Battery Test:** Allows you to release the primary network input relay so as to subject the buffer battery to stress under load, displaying its voltage drop
- **Start Test:** Allows you to perform the communication test between the Control Unit/Device. The report is then shown in "Communication errors".
- **Tamper line status:** Check the status of the Tamper line, the status is highlighted by the dot:
  - **Green** Tamper line Closed
  - **Red** Tamper line Open
- **Stop Test:** End of Test
- **Notes:** Notes can be entered
- **Edit:** Save the entered data
- **Help:** Programming help page
- **Back:** Return to the previous menu

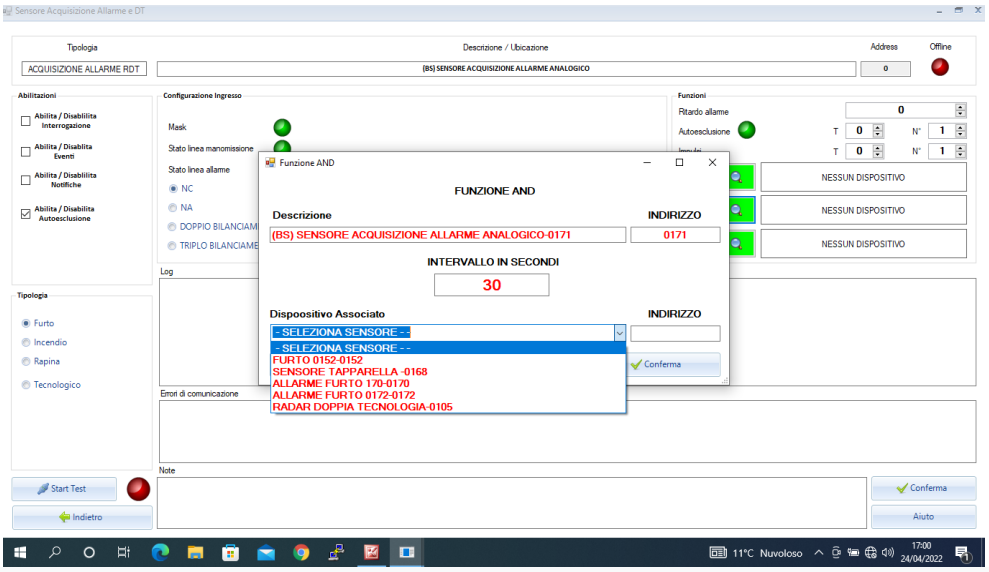
Digital Sensor Interface - 1021/S1



- Alarm signal acquisition device, can be connected to any detection device that has a clean alarm contact, both NC and NA

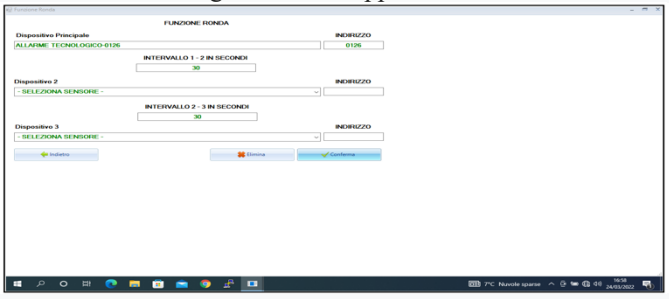
- Description:
- Type: Indication of the device type.
- Enable / Disable device interrogation: Disables the interrogation of the Device
- Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
- Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
- Description / Location: Allows the entry of a 20-character text to define the Function and/or Location
- Address: Indicates the physical address of the device.
- Type: The Device can acquire alarm signals such as: Theft, Fire, Robbery, Technological.
  - Theft and Fire: They will be inserted in the Security devices
  - Robbery: They will not be inserted in any Block as the robbery is inserted in a virtual block that is always active
  - Technological: They will be inserted in the Domo/Technological devices
- Input Configuration: The alarm input can be configured in different modes:
  - NC: Normally Closed input referred to the negative power supply
  - NA: Normally Open input referred to the negative power supply
  - Double Balance: Double Resistive Balance for Alarm and Tampering
  - Triple Balance: Triple Resistive Balance for Alarm, Tampering, Mask
- Functions: The following functions can be associated with the device:
  - Alarm Delay: Sets the delay with which the sensor signals the alarm condition to the control unit. The parameters are 01" ÷ 180" selectable from the drop-down menu.
  - Self-exclusion: Sets the automatic Self-exclusion function of the sensor after x alarms in x time. The parameters can be selected from the drop-down menu:
    - T: Time interval in which the alarms must occur, the time is expressed in minutes from 00'÷ 60'
    - N: Number of alarms after which the self-exclusion must occur, the parameters are from N° 1 ÷ 10
- Pulses: It is possible to set the parameters to manage Fast Inertial sensors or Switch contacts for roller shutters. The parameters can be selected from the drop-down menu:
  - T: Pulse duration width. It is possible to select n°7 steps, from the highest value (less sensitive) to the lowest. Step:1=100ms, 2=2ms, 3=1ms, 4=500us, 5=250us, 6=100us, 7=50us
  - N: Number of Pulses. Allows you to select how many pulses the sensor must generate to detect the Alarm condition. You can select a value from 01 to 5 from the drop-down menu
- Camera Function: This function allows you to associate Sensor-Camera. In the event of a Sensor Alarm, the associated Camera will send a Video Clip to the Control Unit.

- END Function: With this function you can set the alarm consent function between two devices. The alarm will occur only if both associated sensors generate an alarm condition in a defined time.
  - By clicking on the symbol , the Screen with the list of Security devices and Cameras will appear
  - Select the sensor or camera to associate
  - Set the interval time between the two alarms



• Patrol function: With this function it is possible to set a defined path by establishing the times and the position that three sensors must have in the sequence without alarms occurring.
By inverting or modifying the path or the set times, the alarm condition occurs.

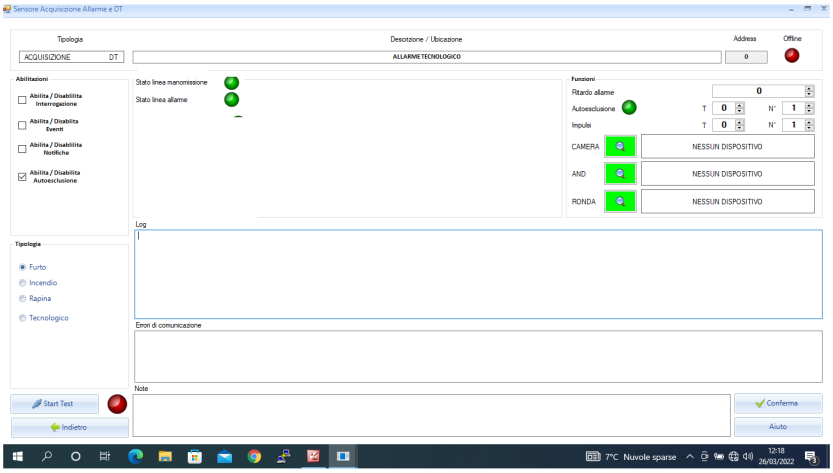
- By clicking on the symbol the following screen will appear:



◦ Main Device: From the drop-down menu you can select the time, between 01" ÷ 300", that elapses between the alarm of the main sensor and the second sensor.
◦ 2nd Device of the path: From the drop-down menu select the device you want to associate and the time, between 01" ÷ 300", that elapses between the alarm of the second sensor and the third.
◦ 3rd Device of the path: From the drop-down menu select the device you want to associate.

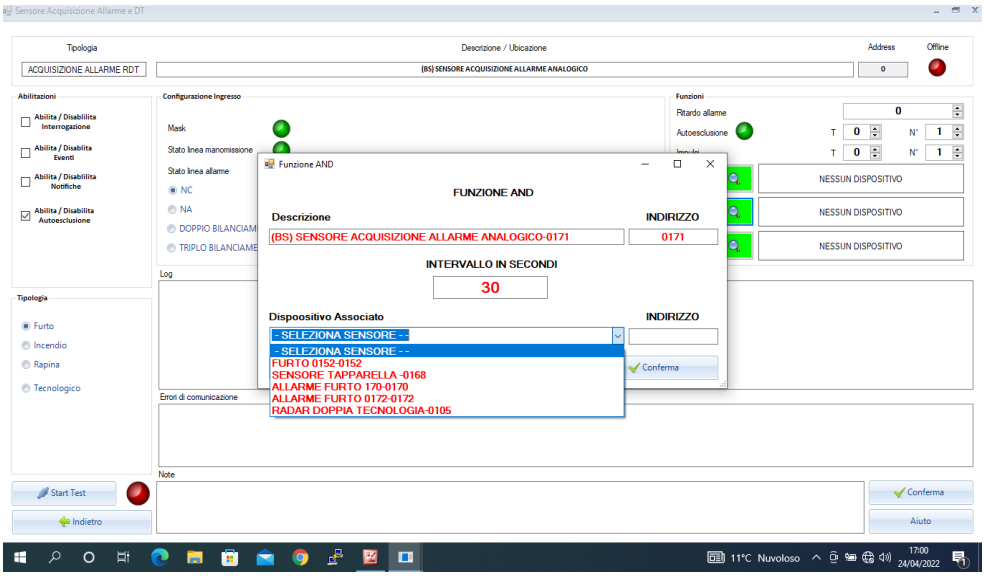
• Start Test: Allows you to query the Device and the alarm lines; the report is then shown in "Communication errors". Tests the alarm input lines of the device in the various configurations. The status of the lines is displayed by:
◦ Green Alarm/Tamper line in Rest state
◦ Red Alarm/Tamper line in Alarm state
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

Addressable DT Sensor - 1021/S2

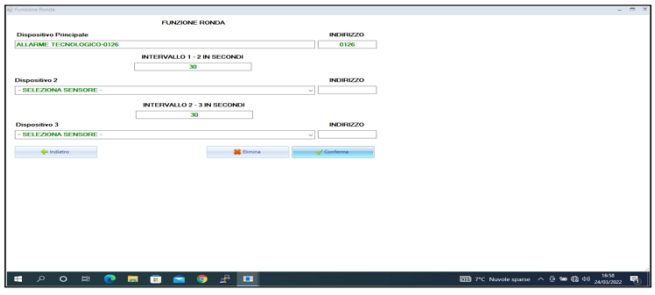


Dual Technology Sensor with Integrated Addressable Network Interface.

- Description:
- Type: Indication of the type of device.
- Enable / Disable the interrogation of the device: Disables the interrogation of the Device
- Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
- Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
- Description / Location: Allows the entry of a 20-character text to define the Function and/or Location
- Address: Indicates the physical address of the device.
- Type: The Device can acquire alarm signals such as: Theft, Fire, Robbery, Technological.
  - Theft and Fire: They will be inserted in the Security devices
  - Technological: They will be inserted in the Domo/Technological devices
- Functions: The following functions can be associated with the device:
  - Alarm Delay: Sets the timing for the delay with which the sensor must signal an alarm condition. The parameters are 01" ÷ 180" selectable from the drop-down menu.
  - Self-exclusion: Sets the automatic self-exclusion function of the sensor after x alarms in x time. The parameters are selectable from the drop-down menu:
    - T: Time interval in which the alarms must occur, the time is expressed in minutes from 00'÷ 60'
    - N: Number of alarms after which self-exclusion must occur, the parameters are from N° 1 ÷ 10
  - Pulses: It is possible to set the parameters to manage Fast Inertial sensors or Switch contacts for roller shutters. The parameters can be selected from the drop-down menu:
    - T: Pulse duration width. It is possible to select 7 steps, from the highest value (less sensitive) to the lowest. Step: 1=100ms, 2=2ms, 3=1ms, 4=500us, 5=250us, 6=100us, 7=50us
    - N: Number of Pulses. It allows you to select how many pulses the sensor must generate to detect the Alarm condition. It is possible to select a value from 01 ÷ 5 from the drop-down menu
  - Camera Function: This function allows you to associate Sensor-Camera. In the event of a Sensor Alarm, the associated Camera will send a Video Clip to the Control Unit.
  - END Function: With this function it is possible to set the alarm consent function between two devices. The alarm will occur only if both associated sensors generate an alarm condition in a well-defined time.
    - By clicking on the symbol  the following screen will appear with the list of devices, Security sensors and Cameras for which the Video-Analysis function has been enabled.

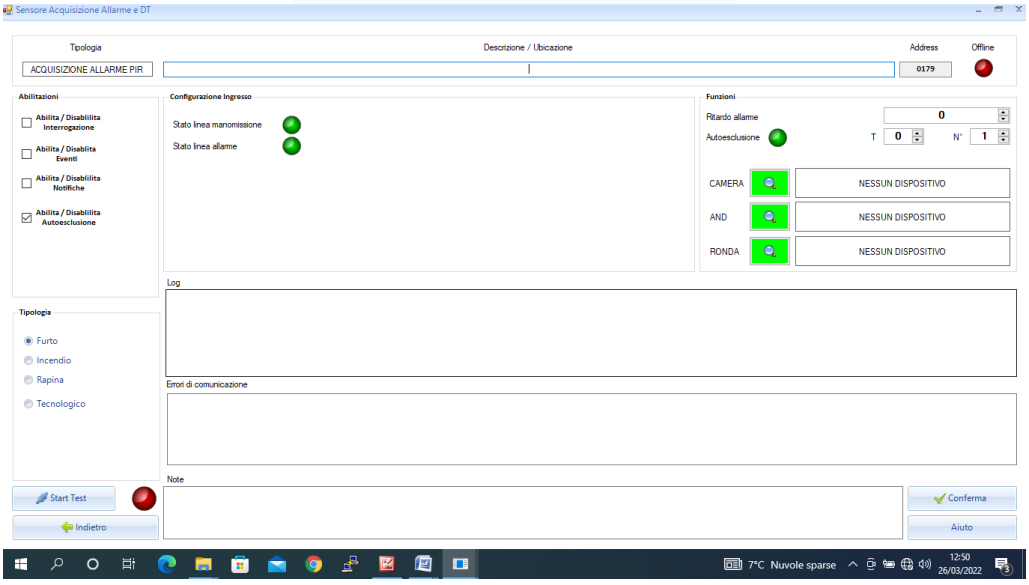


▪ Set the interval time between the two alarms
▪ Select the sensor or camera to associate
◦ Patrol Function: With this function it is possible to set a defined path by establishing the times and the position that the three sensors must have in the sequence, without alarms occurring. Inverting or modifying the set path will verify the alarm condition.
▪ Clicking on the symbol will display the following Figure:



◦ Main Device: From the drop-down menu you can select the time, between 01" ÷ 300", that elapses between the alarm of the main sensor and the second sensor.
◦ 2nd Device of the path: From the drop-down menu select the device you want to associate and the time, between 01" ÷ 300", that elapses between the alarm of the second sensor and the third.
◦ 3rd Device of the path: From the drop-down menu select the device you want to associate.
• Start Test: Allows you to query the Device and the alarm lines; the report is then shown in "Communication errors". Tests the alarm input lines of the device in the various configurations. The status of the lines is displayed by:
◦ Green Alarm/Tamper line in Rest state
◦ Red Alarm/Tamper line in Alarm state
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

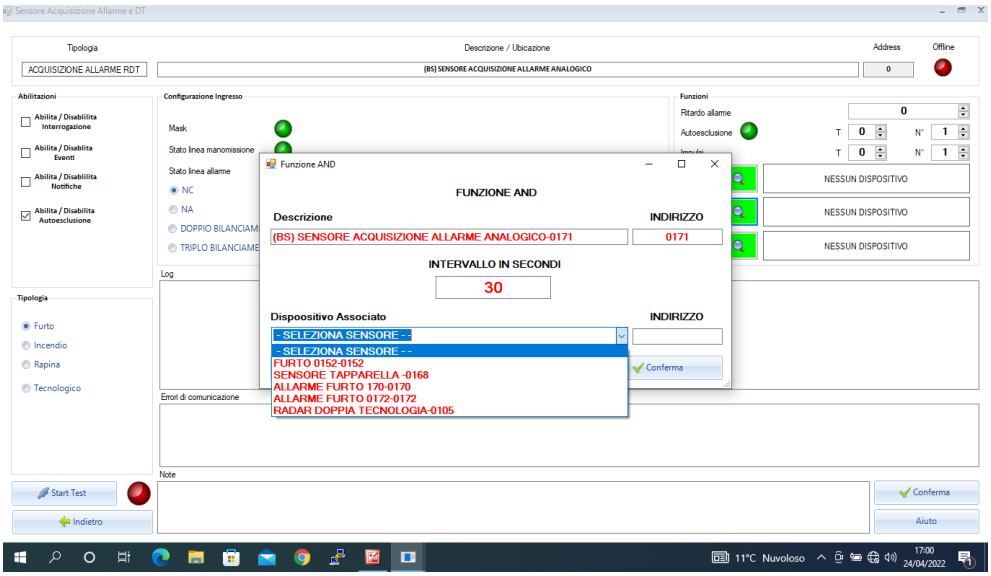
Addressable PIR Sensor - 1021/S4



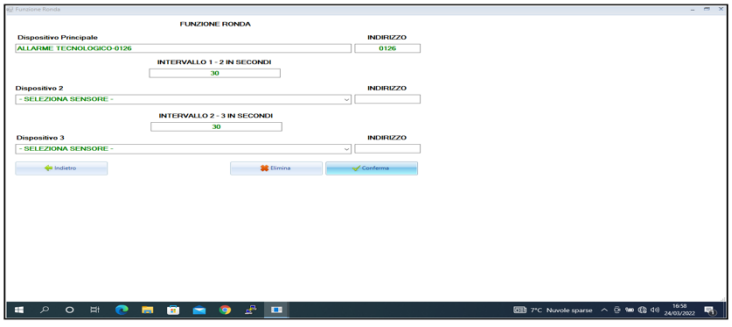
PIR Sensor with Addressed Network Interface integrated in Keystone module

Description:

- Type: Indication of the type of device.
- Enable / Disable the interrogation of the device: Disables the interrogation of the Device
- Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
- Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
- Description / Location: Allows the entry of a 20-character text to define the Function and/or Location
- Address: Indicates the physical address of the device.
- Type: The Device can acquire alarm signals such as: Theft, Fire, Robbery, Technological.
  - Theft and Fire: They will be inserted in the Security devices
  - Technological: They will be inserted in the Domo/Technological devices
- Functions: It is possible to associate the following functions to the device:
  - Alarm Delay: Sets the timing for the delay with which the sensor must signal an alarm condition. The parameters are 01" ÷ 180" selectable from the drop-down menu.
  - Self-exclusion: Sets the automatic self-exclusion function of the sensor after x alarms in x time. The parameters are selectable from the drop-down menu:
    - T: Time interval in which the alarms must occur, The time is expressed in minutes from 00'÷ 60'
    - N: Number of alarms after which the self-exclusion must occur, the parameters are from N° 1 ÷ 10
  - Pulses: It is possible to set the parameters to manage Fast Inertial sensors or Switch contacts for roller shutters. The parameters are selectable from the drop-down menu:
    - T: Pulse duration amplitude. It is possible to select n°7 steps, from the highest value (less sensitive) to the lowest. Step:1=100ms, 2=2ms, 3=1ms, 4=500us, 5=250us, 6=100us, 7=50us
    - N: Number of Pulses. Allows you to select how many pulses the sensor must generate to detect the Alarm condition. You can select a value from 01 ÷ 5 from the drop-down menu
  - Camera Function: This function allows you to associate Sensor-Camera. In the event of a Sensor Alarm, the associated Camera will send a Video Clip to the Control Unit.
  - END Function: With this function it is possible to set the alarm consent function between two devices. The alarm will occur only if both associated sensors generate an alarm condition in a well-defined time.
    - By clicking on the symbol , the following screen will appear with the list of devices, Security sensors and Cameras for which the Video-Analysis function has been enabled.

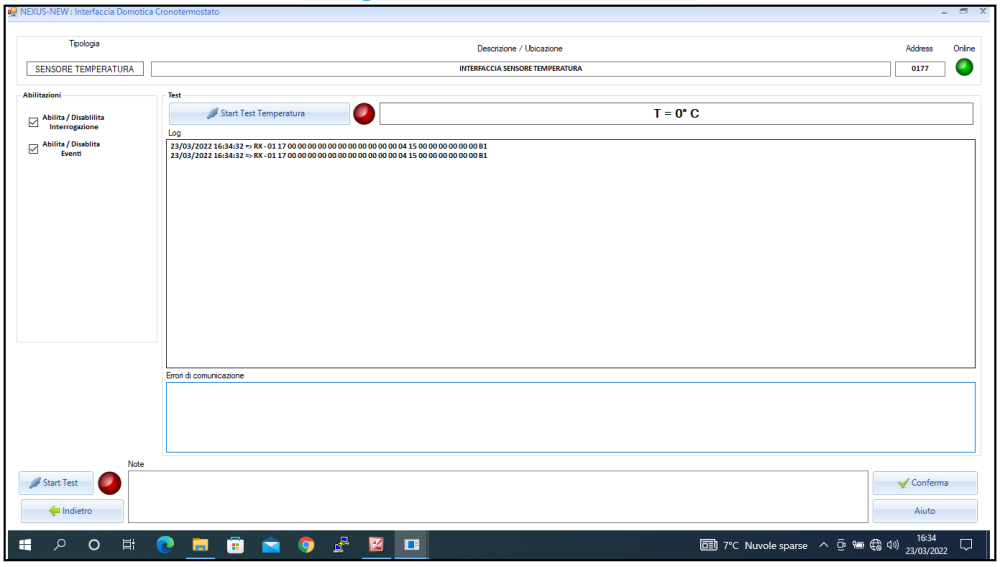


- Set the interval time between the two alarms
- Select the sensor or camera to associate
  - Patrol Function: With this function it is possible to set a defined path by establishing the times and the position that the three sensors must have in the sequence, without alarms occurring. Inverting or modifying the set path will verify the alarm condition.
- Clicking on the symbol will display the following Figure:



◦ Main Device: From the drop-down menu you can select the time, between 01" ÷ 300", that elapses between the alarm of the main sensor and the second sensor.
◦ 2nd Device of the path: From the drop-down menu select the device you want to associate and the time, between 01" ÷ 300", that elapses between the alarm of the second sensor and the third.
◦ 3rd Device of the path: From the drop-down menu select the device you want to associate.
• Start Test: Allows you to query the Device and the alarm lines; the report is then shown in "Communication errors". Tests the alarm input lines of the device in the various configurations. The status of the lines is displayed by:
◦ Green Alarm/Tamper line in Rest state
◦ Red Alarm/Tamper line in Alarm state
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

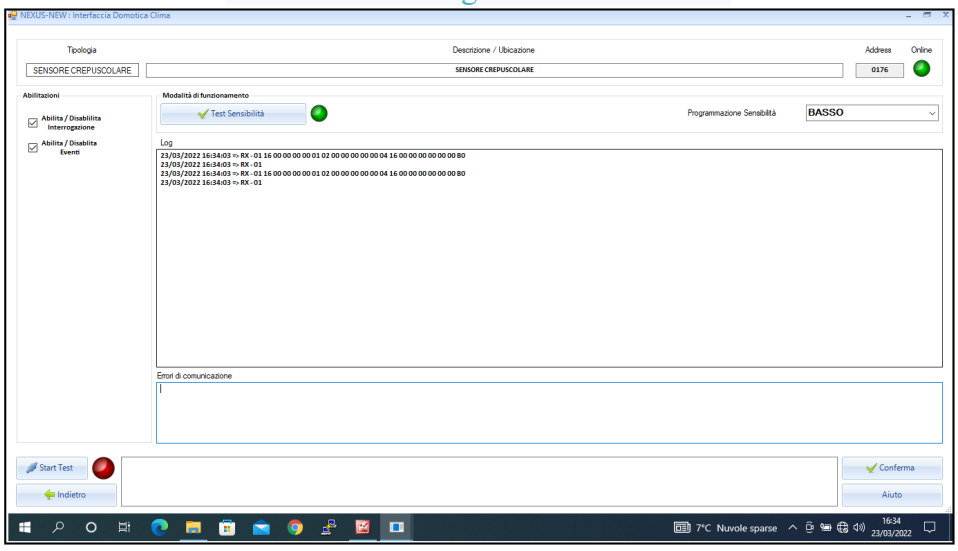
Temperature Sensor - 1021/S5



Home Automation Temperature Detector built-in in keystone module

Description:
• Type: Indication of the type of device.
• Enable / Disable device querying: Disables Device querying
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device.
• Start Test: Device interrogation test and Temperature Reading test
◦ Device interrogation test,
◦ Room Temperature Reading the Temperature reading will be reported in the box
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

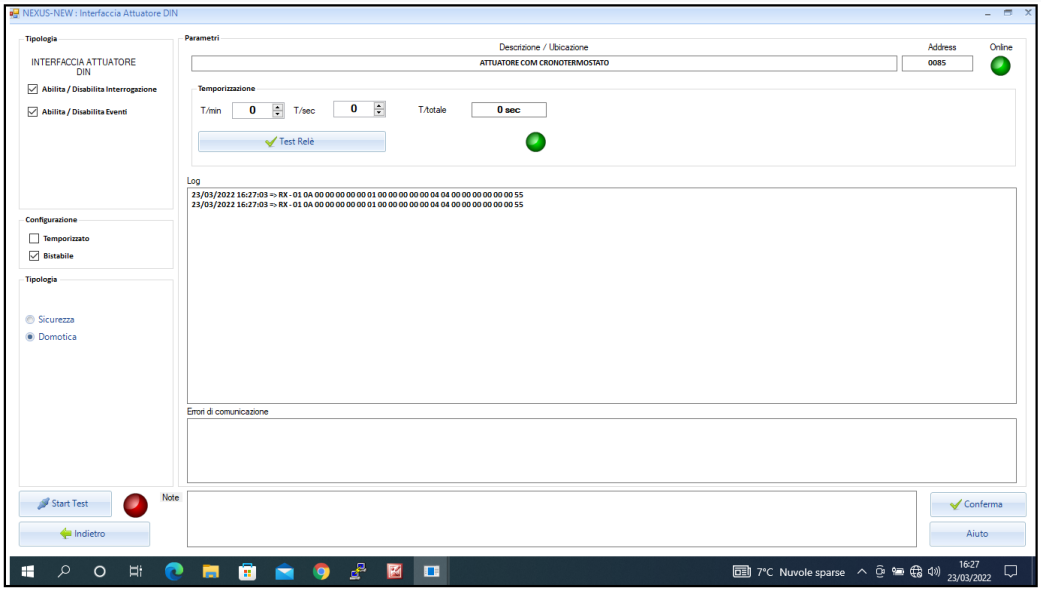
Addressable Twilight Sensor - 1021/S6



Home Automation Twilight Detector built-in in keystone module

Description:
• Type: Indication of the type of device.
• Enable / Disable device interrogation: Disables the interrogation of the Device
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device.
• Start Test: Device interrogation test and brightness level reading test
◦ Device interrogation test
◦ Programming of the brightness level to be detected, it is possible, from the drop-down menu, to select 5 brightness levels: Low, Medium low, Medium, Medium High, High.
• Detection test: Press the SENSITIVITY TEST button, once the level is reached the green dot becomes red
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

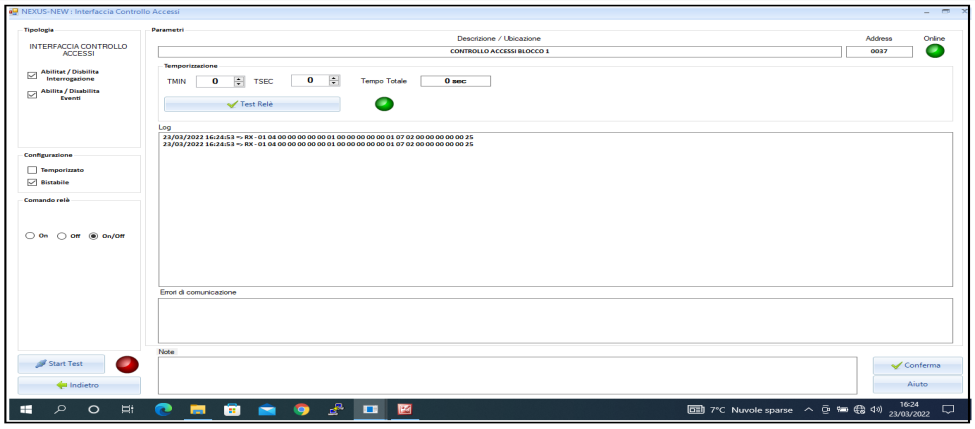
Actuator Interface - 1022/A1



DIN module interface for implementing Alarms or Domo/Technological Commands

Description:
• Type: Indication of the type of device.
• Enable / Disable the device query.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device
• Type: The Device can be programmed to perform the following functions:
◦ Security: The device will be part of the Security blocks
◦ Home Automation: The device will be part of the Domo/Technological blocks
◦ Configurations: Selection of the operating mode of the Bistable or Timed Relay. In Timed mode, times are expressed in minutes, in the 0'÷ 10' scale and in seconds, in the 01" ÷ 59" scale
• Start test: Device and Relay interrogation test:
◦ Device interrogation test
◦ Relay Operation Test: By activating the Test, the relay switches and the light changes from Green to Red
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

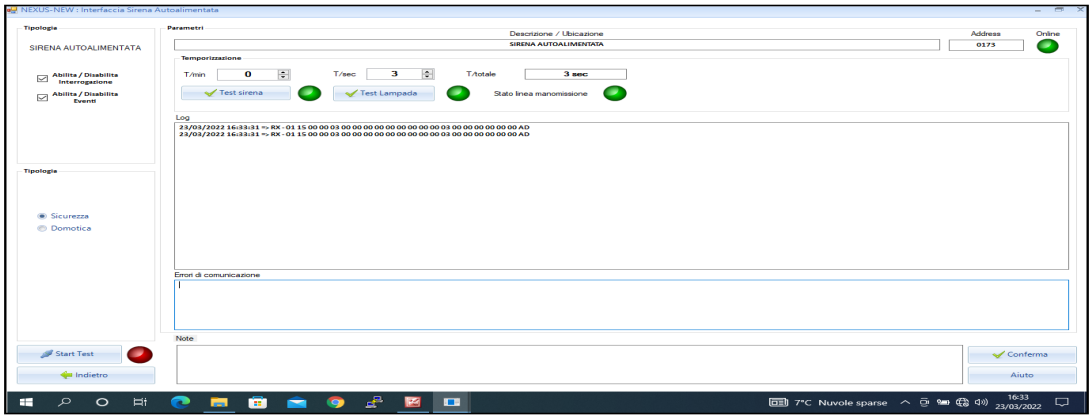
Access Control Actuator Interface - 1022/A01-AC



DIN module interface, equipped with a relay output, which switches according to the on/off status of the safety block to which it is associated.

Description:
• Type: Indication of the device type.
• Enable / Disable the device query.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device
• Configurations: Selection of the operating mode of the Bistable or Timed Relay. In the Timed mode the times are expressed in minutes, in the scale from 0'÷ 10', and in seconds, in the scale from 01" ÷ 59"
• Relay Command: Provides a status of the ARM/DISARM condition of the Safety Block to which the device is associated. The device Relay has three activation modes:
◦ Activation only when the Lock is inserted
◦ Activation only when the Lock is released
◦ Activation both when the Lock is inserted and released
• Start Test: Device interrogation test and Relay test
◦ Device interrogation test
◦ Relay Operation Test: When the Test is activated, the relay switches and the light changes from Green to Red
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the data entered
• Help: Programming help page
• Back: Return to the previous menu

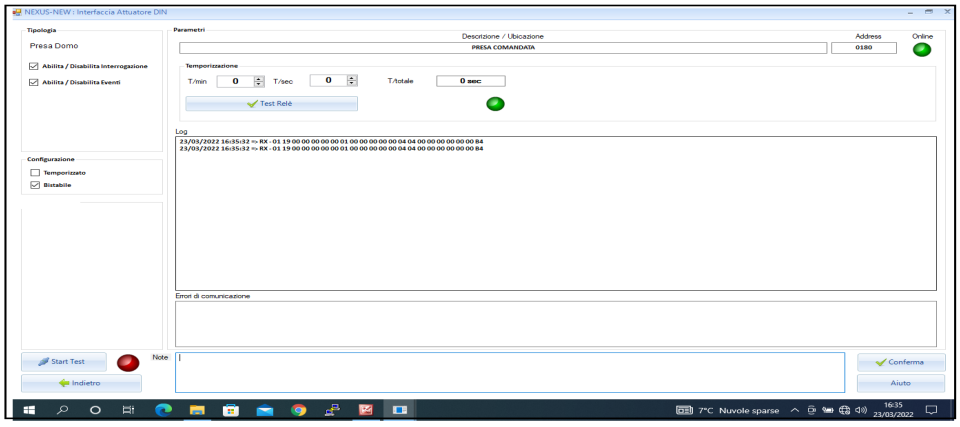
Self-powered siren - 1022/A2



Self-powered siren with integrated Addressable interface.

Description:
• Type: Indication of the type of device.
• Enable / Disable the interrogation of the device.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device
• Type: The Device can be programmed to perform the following functions:
◦ Security: The device will be part of the Security blocks
◦ Domo / Technological: The device will be part of the Domo / Technological blocks
• Configurations: Alarm Time. The times are expressed in minutes, in the scale from 0’÷ 10’, and in seconds, in the scale from 01” ÷ 59”
• Start Test: Device interrogation and Operation Test
◦ Device interrogation test
◦ Siren Test: The light from Green becomes Red, the device must sound
◦ Lamp Test: The light from Green becomes Red, the lamp must turn on
◦ Tamper line status:
▪ Green light tampering Closed
▪ Red light tampering open
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

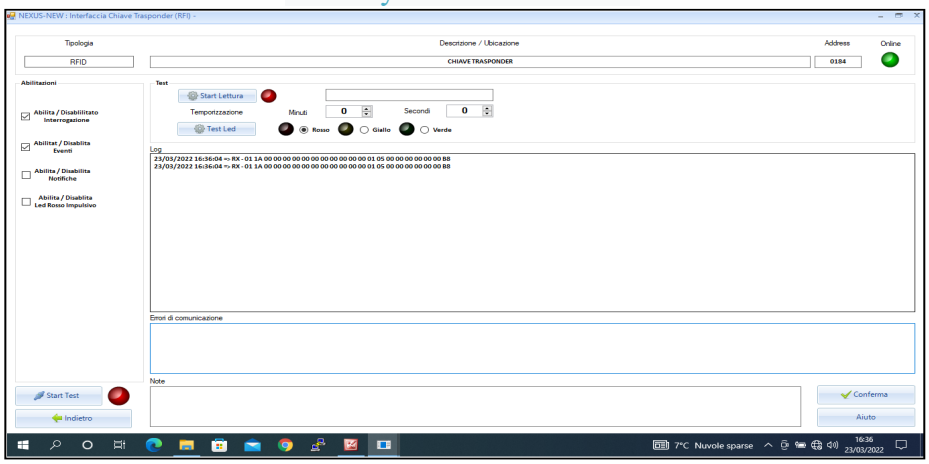
Addressable Domo Socket - 1022/A3



Home automation device for 220Vac controls. The device is composed of two Keystone built-in modules.

Description:
• Type: Indication of the device type.
• Enable / Disable device interrogation.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device
• Type: The Device can be programmed to perform the following functions:
◦ Security: The device will be part of the Security blocks
◦ Home automation: The device will be part of the Home/Technological blocks
◦ Configurations: Selection of the operating mode of the Bistable or Timed Relay. In Timed mode, times are expressed in minutes, in the 0'÷ 10' scale and in seconds, in the 01" ÷ 59" scale
• Start test: Device and Relay interrogation test:
◦ Device interrogation test
◦ Relay Operation Test: By activating the Test, the relay switches and the Red light turns on
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

RFI Key Reader - 1023/M1

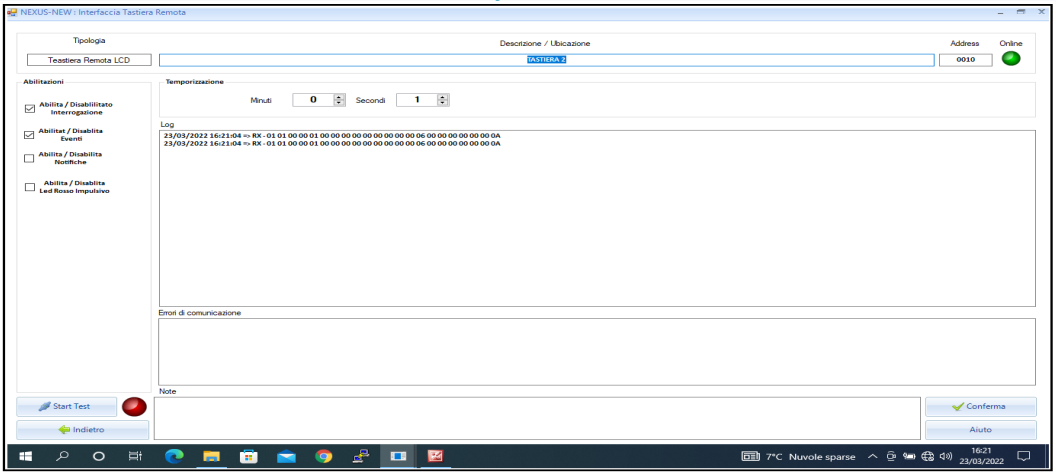


- Addressed transponder reader of proximity keys in Keystone module,

Description:

- Type: Indication of the type of device.
- Enable / Disable the interrogation of the device.
- Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
- Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
- Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
- Address: Indicates the physical address of the device
- Timing: Delay in the activation of the Security block to which it is associated. The times are expressed in minutes, on the scale from 0'÷ 3', and in seconds, on the scale 01" ÷ 59"
- Transponder Key Reading Test: It is possible to perform a Transponder Key Reading test:
  - Bring a Key close to the reader
  - Click the "start Reading" button
  - The code printed on the Key will be shown on the box
- LED test: The RFI Reader is equipped with three signal LEDs:
  - Red LED: ON/OFF signal inserted General Block or Block to which the Reader belongs
  - Yellow LED: ON/OFF signal of a Partial Block Inserted * Not the one it belongs to *
  - Green LED: Service signal, Maintenance, Fault, Anomaly, Tampering, Disabled Zone, No primary network on the Control Panel, SIM without Credit, No ADSL network.
  - To perform the Test: Select the LED and click on test
- Stop Test: End of Test
- Notes: Notes can be entered
- Edit: Save the entered data
- Help: Programming help page
- Back: Return to the previous menu

LCD Keyboard - 1023/M2

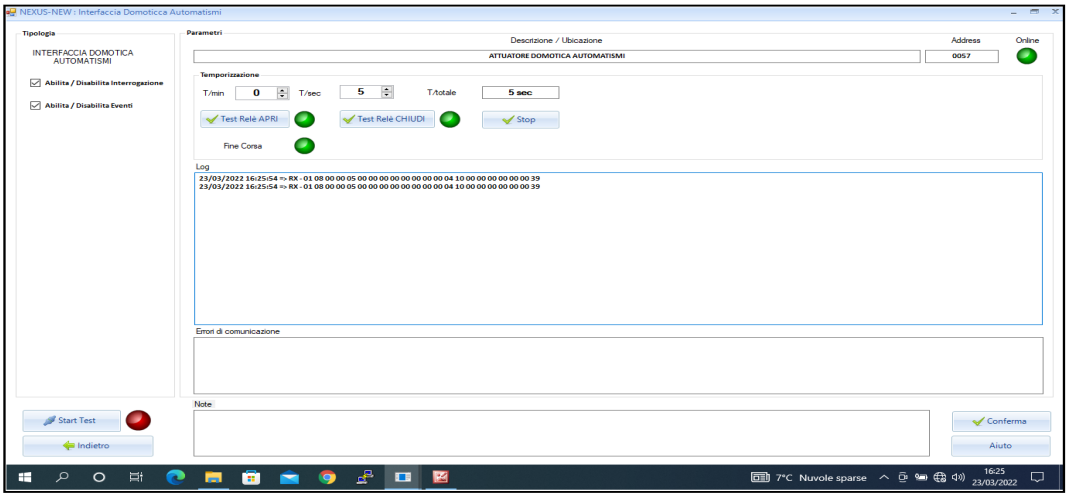


Control keypad with LCD display for managing Security and Home Automation functions.

Description:
• Type: Indication of the device type.
• Enable / Disable device querying.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device
• Timing: Delay in activating the Security block to which it is associated. The times are expressed in minutes, in the scale from 0'÷ 3', and in seconds, in the scale 01" ÷ 59"
• LED test: The keyboard is equipped with three signal LEDs:
◦ Red LED: ON/OFF signal inserted General Block or Block to which the Reader belongs
◦ Yellow LED: ON/OFF signal of a Partial Block Inserted * Not the one it belongs to *
◦ Green LED: Service signal, Maintenance, Fault, Anomaly, Tampering, Disabled Zone, No primary network on the Control Panel, SIM without Credit, No ADSL network.
◦ To perform the Test: Select the LED and click on test
• Start Test: Query the Device
• Stop Test: End of Test
• Notes: Notes can be inserted
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

Interfaccia Domo Clima - 1024/D1

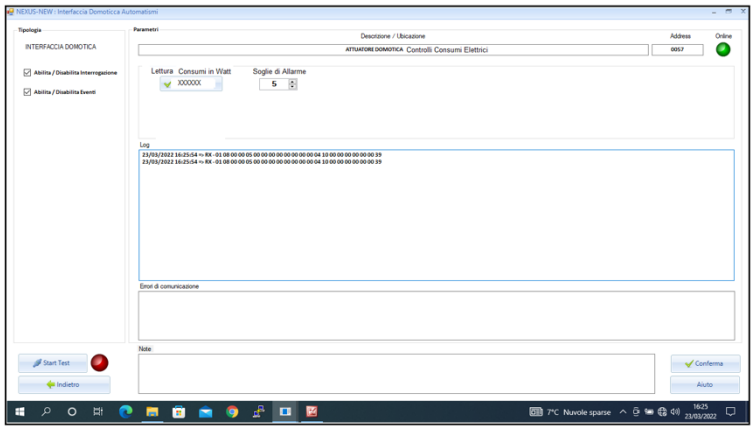
Domo Automatismi Interface - 1024/D4



Addressed Home Automation Interface in DIN module for the management of Automations

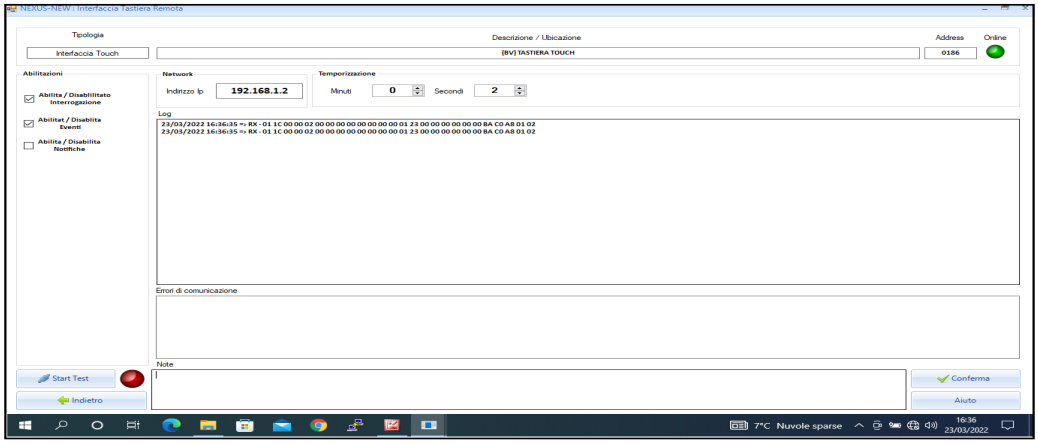
Description:
• Type: Indication of the type of device.
• Enable / Disable the interrogation of the device.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device
• Timing: The device is equipped with two actuation relays (Opening and Closing). The times are expressed in minutes, in the scale from 0'÷ 3', and in seconds, in the scale 01" ÷ 59"
• Relay Test: To perform the test:
◦ OPEN Relay Test: the green dot will turn red and the relay will switch for the programmed time
◦ Stop: Ends the Open Relay timing
◦ CLOSE Relay Test: the green dot will turn red and the relay will switch for the programmed time
◦ Stop: Ends the Open Relay timing
• Start Test: Query the Device
• Stop Test: End of Test
• Notes: Notes can be entered
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

Domo Interface Control Electricity Consumption - 1024/D5



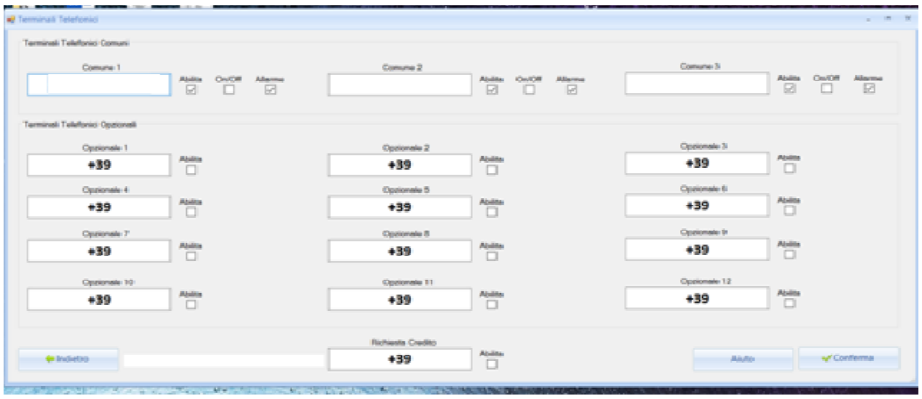
Description:
• Type: Indication of the device type.
• Enable / Disable the device query.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device
• Reading Consumption in Watts: Arrow key on the screen will display the instantaneous reading of the Absorption of the connected Electric user
• Drop-down menu: Allows you to set 5 alarm thresholds, when the set threshold is reached, the Control Unit will send an Alarm Notification
• Start Test: Query the Device
• Stop Test: End of Test
• Notes: Annotations can be inserted
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

Touch Display 1023/M3



The Touch device is managed by the control unit both from the BUS and from the TCPIP network
Description:
• Type: Indication of the type of device.
• Enable / Disable the interrogation of the device.
• Enable / Disable Events: Disabled the device does not generate events, they are stored in the History.
• Enable / Disable Notifications: Disables the sending of Events (APP, SMS, etc.)
• Description / Location: Allows the entry of a 20-character text to define the Function and/or Location.
• Address: Indicates the physical address of the device on the BUS
• IP Address: Indicates the network address that has been assigned to it
• Timing: Delay in the activation of the Security block to which it is associated. Times are expressed in minutes, in the scale from 0'÷ 3', and in seconds, in the scale 01" ÷ 59"
• Start Test: Device Interrogation
• Stop Test: End of Test
• Notes: Annotations can be inserted
• Edit: Save the entered data
• Help: Programming help page
• Back: Return to the previous menu

Telephone Terminal Programming



Programming Telephone Numbers
• The screen allows you to set telephone numbers for sending SMS messages.
• It is possible to program 16 Mobile Telephone numbers.
The numbers are divided into two categories:
1. Common Numbers: 3 telephone numbers enabled to send Alarm messages, ON/OFF Status Messages and Service Messages can be programmed. Once Enabled, they do not need to be associated with * codes to send the messages.
2. Optional Numbers: 12 numbers can be programmed. The optional numbers are enabled to send Alarm and ON/OFF status SMS messages and are associated with the individual security codes (see specific paragraph, programming codes)

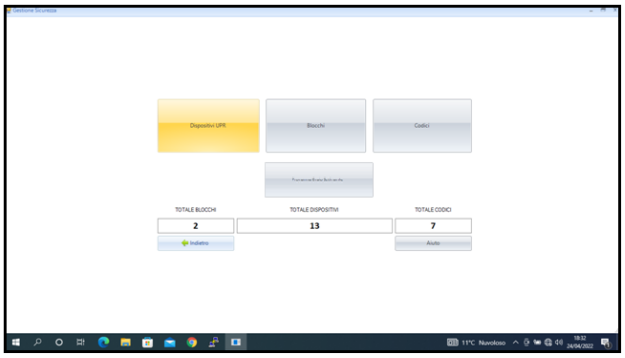
Common Terminals 1/2/3
By enabling the various options, the following can be sent to these numbers:
Service messages = 220 network presence/absence, Battery status, Faults, Maintenance
Use messages = Safety insertions/disinsertions
Alarm messages = Tampering, Alarms,
Transmission is in SMS format
• Enter the GSM telephone number
• Enable the number in the appropriate box

Optional Terminals: 1/2/3/4/5/6/7/8/9/10/11/12
Insert the Optional telephone numbers which will be associated with the individual Security Codes ((See chapter Security Codes) the event/message reception association is obtained,
The following can be sent to the numbers:
Use messages = Safety insertions/disinsertions
(enabling is done in the Code Programming function)
Alarm messages = Tampering , Alarms (enabling is done in the Code Programming function)

Transmission is in SMS format
• Confirm: Save the data entered
• Help: Programming help page
• Back: Save the data entered and Return to the previous menu

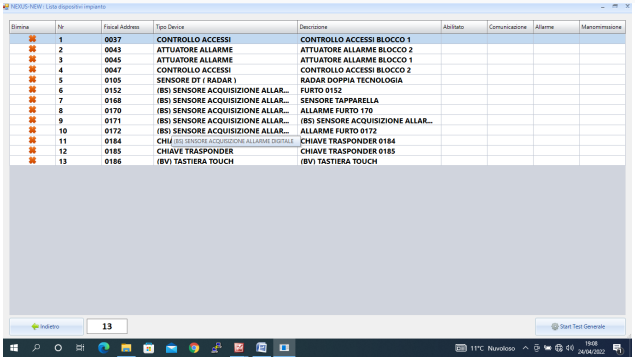
Security menu

From the main screen, select the Security Menu.



The security menu is composed of the following submenus:
• List of security devices
• Programming Security Blocks
• Programming Codes and Keys
• Automatic Security Programmer
• Help: Programming help page
• Back: Return to the previous menu

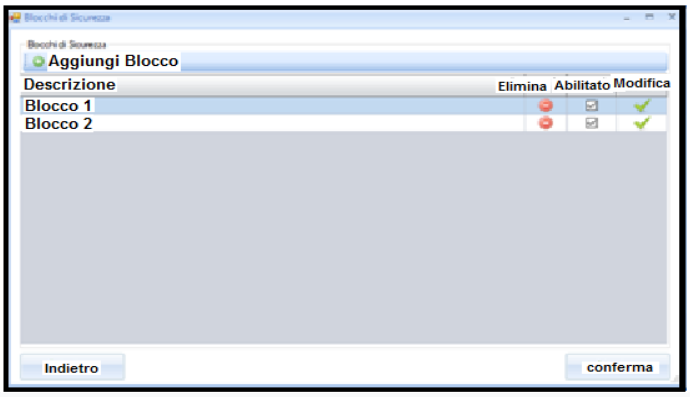
List of UPR Devices



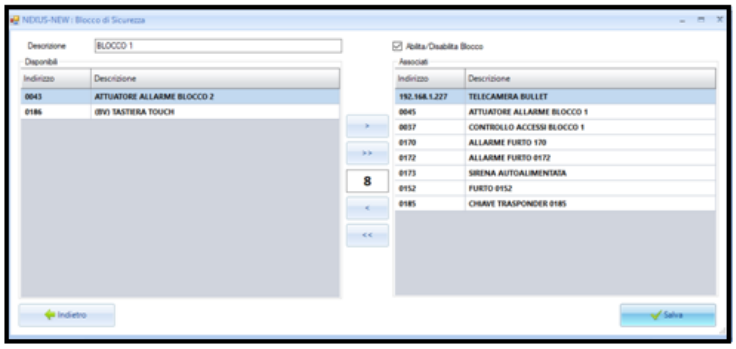
Elimina	Nr	Fiscal Address	Tipo Device	Descrizione	Abilitato	Comunicazione	Allarme	Manomimissione
	1	0037	CONTROLLO ACCESSI	CONTROLLO ACCESSI BLOCCO 1				
	2	0043	ATTUATORE ALLARME	ATTUATORE ALLARME BLOCCO 2				
	3	0045	ATTUATORE ALLARME	ATTUATORE ALLARME BLOCCO 1				
	4	0047	CONTROLLO ACCESSI	CONTROLLO ACCESSI BLOCCO 2				
	5	0105	SENSORE DT (RADAR)	RADAR DOPPIA TECNOLOGIA				
	6	0152	(BS) SENSORE ACQUISIZIONE ALLAR...	FURTO 0152				
	7	0168	(BS) SENSORE ACQUISIZIONE ALLAR...	SENSORE TAPPARELLA				
	8	0170	(BS) SENSORE ACQUISIZIONE ALLAR...	ALLARME FURTO 170				
	9	0171	(BS) SENSORE ACQUISIZIONE ALLAR...	(BS) SENSORE ACQUISIZIONE ALLAR...				
	10	0172	(BS) SENSORE ACQUISIZIONE ALLAR...	ALLARME FURTO 0172				
	11	0184	CHIA (BS) SENSORE ACQUISIZIONE ALLARME ENSTALE	CHIAVE TRASPONDER 0184				
	12	0185	CHIAVE TRASPONDER	CHIAVE TRASPONDER 0185				
	13	0186	(BV) TASTIERA TOUCH	(BV) TASTIERA TOUCH				

The list contains the devices programmed and configured as Security Devices and is a repetition of the General Devices list. With this function it is possible to make any changes to the programming of the devices and to test them. The procedures are those indicated for the individual devices.

Programming Safety Blocks
The control unit allows you to program 30 Safety blocks (Areas) that will behave as autonomous subsystems.
Associating the various devices
From the main screen select Safety Blocks. The following screen will open:
The screen allows you to create the blocks (association Sensors/Actuators/Key Sockets).



Where:
• Add Block: Creates a new block
• Delete: Deletes an existing block
• Enable: Allows you to Enable/Disable the Block
• Edit: Allows you to enter the Block Programming and make changes



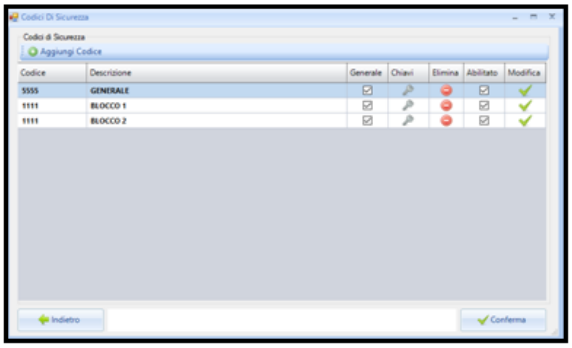
ADD NEW BLOCK

• Description: Enter a 20-character text to identify the Block function
• Enable/Disable Block: Allows you to Enable/Disable the block for Operation
• Available: List of Devices for both the BUS and the Cameras
≥: By selecting a single device, the Button moves it from the Available list to the Associated list
≥≥: By clicking the Button, it moves all of them from the Available list to the Associated list
≤: By selecting a single device, the Button allows you to move it from the Associated list to the Available list

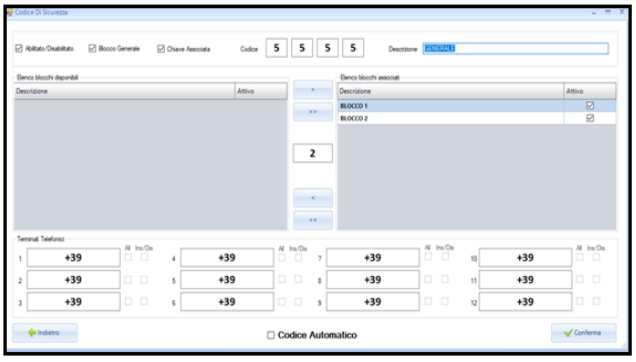
≤≤: The Button moves all of the Associated Devices from the list to the Available list for the block **8**: Indicates the number of devices associated with the Block
• Help: Programming help notes
• Save: Saves the programmed configuration
• Back: Returns to the previous screen

NOTE:
• The devices configured for ROBBERY do not appear in the list of Available devices;
These are always active.
• Keyboards do not appear in the list of Available devices,
• They are always common to all blocks
• Sensor devices (Sensors; DT Radar, PIR Radar, Cameras), Keys and Access Control devices can be associated with only one block (Inserted in a Block they will no longer appear in the Available List)
• Actuator devices can be associated with multiple blocks.

Programming Codes: Codes can be of two types:
General (They control all the Blocks)
Partial (They control only the Blocks that will be associated with the Code)
Automatic Code, The code will be used by the weekly Automatic Programmer

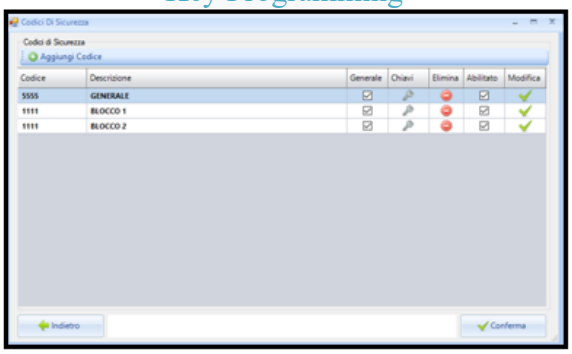


The screen allows you to program:
• Codes for Activation/Deactivation of security locks: 250 codes can be programmed
• Up to 25 Transponder Keys can be associated with each code
• Associate the locks it must control with each code
• Associate the Optional telephone numbers to which SMS messages are to be sent with each code
• Associate a 20-character text with each code to identify the user who uses it (Access Control Function)
• Associate a Transponder Key with each code
• NB: The codes to be displayed in the APPs must have the APP Text in the description……
Add Code

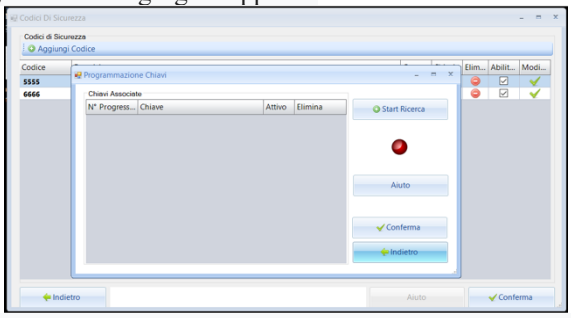


• Enable/Disable : Check Enable = Code Enabled ; Check Disable = Code Disabled
• General Block : All Blocks will be moved to the Associated Blocks List
Check Enable = General Code Enabled ; Check deactivate = Partial Code
• Code: Enter a 4-digit Code XXXX (the same will be used to perform the Insertions/Disinsertions from the LCD Keypad and Touch Display
• Description: Enter a 20-character text (For example the name of the person who will use the code (each operation carried out with that code will generate a Historical event that will be Stored in the Events History and remotely sent via SMS and Notification)
• Telephone Terminals: the Section displays the optional telephone numbers previously Enabled. Enable the type of message to be sent via SMS
ALL = Sending of Alarm Messages; Ins/Dis = Sending of Insertion/Disinsertion messages of the Blocks associated with that Code
• Partial Block: With the General Block deactivated check, the Code is Partial. Move the block that the code must control from the list of available blocks to the list of associated Blocks.
• Automatic Code: The Code can be either General or Partial and will be Displayed in the Automatic Weekly Safety Programmer Codes list
• Help: Programming help notes
• Save: Saves the programmed configuration
• Back: Returns to the previous screen

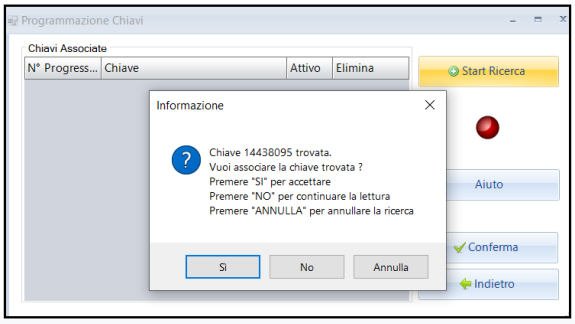
Key Programming



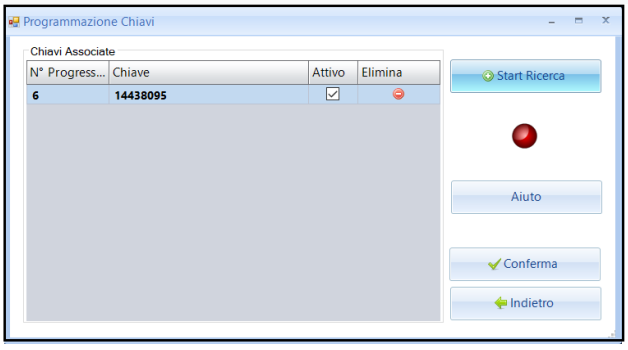
From the Screen: Press the key symbol, the following figure appears:



a) Bring a Transponder Key close to an RFI reader
b) Press the START SEARCH button
c) When the Key is read, the following screen appears



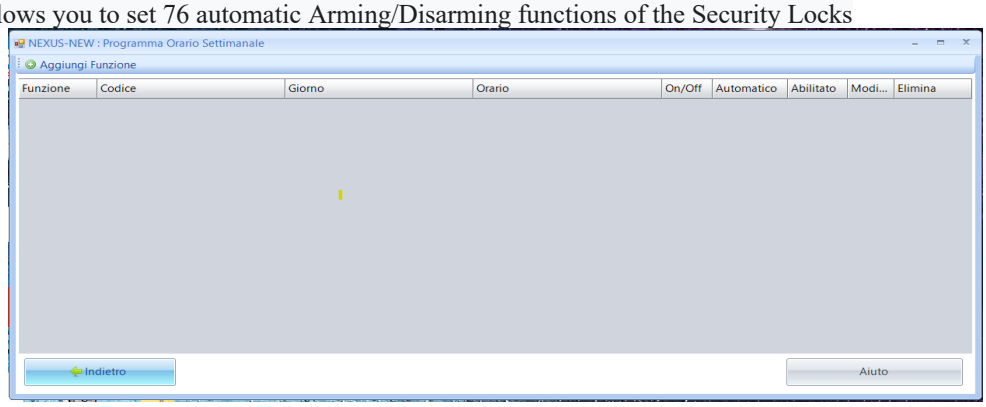
a) Check that the serial number is correct by comparing it with the one indicated on the Key
b) Press the YES button
c) The next screen appears



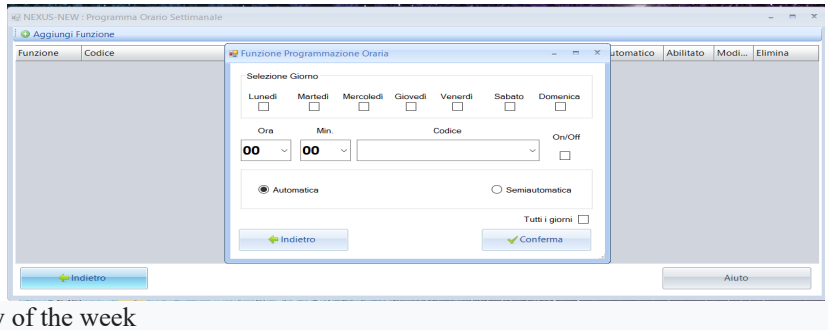
a) Press the CONFIRM button
b) Proceed with the next Key

Weekly Security Time Programmer

The Programmer allows you to set 76 automatic Arming/Disarming functions of the Security Locks



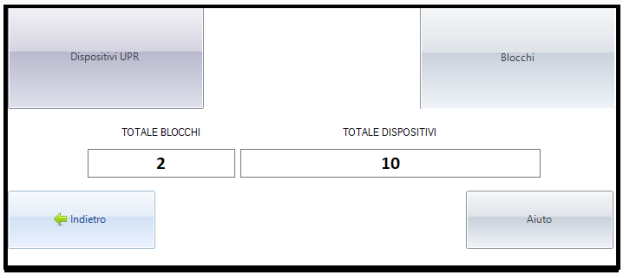
Where:
• Add Function: Allows you to program a new function (see next screen)
• Functions: List of functions already programmed
• Day of the week: Indication of the day of the week associated with the function
• Time: Indication of the Time
• ON/OFF: Indication of the Arming/Disarming that the operation must perform
• Automatic: the Function has two operating options:
- Automatic, if activated the reference block will be deactivated only by a subsequent Automatic operation (the Control Unit will NOT accept any other disarming option)
- Semi-automatic, the control unit accepts all supports to disarm the reference block.
• Enabled: Function Enabled/Disabled for operation
• Edit: Modification of the operating parameters (see next screen)
• Every Day: Replicates the first operation for all days of the week
• Delete: Deletes the selected function
• Back: Returns to the previous screen
• Help: Programming help page



• Select Day: Select the day of the week
• Time: Set the Hour from the drop-down menu
• Minutes: Set the Minutes from the drop-down menu
• Code: The drop-down menu shows the Codes defined as Automatic in Code Programming. Select the Code
• ON/OFF: Select the type of operation that the Code must perform Arming/Disarming
• Automatic/Semi-automatic: Select the Function (See previous paragraph)
• Every day: Replicates the settings made on all days of the Week
• Help: Programming help page
• Confirm: Saves the settings made
• Back: Returns to the previous page

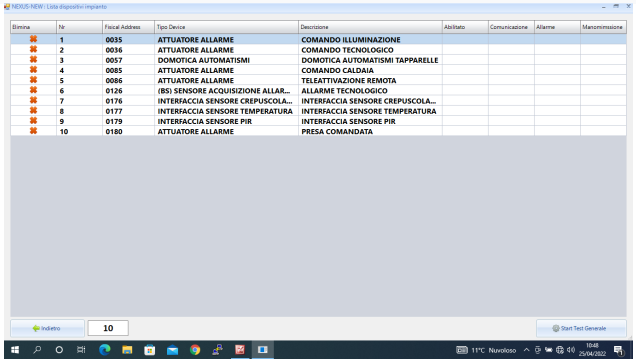
Home Automation / Technology Menu

From the main screen, select the D menu.



It is composed of the following submenus:

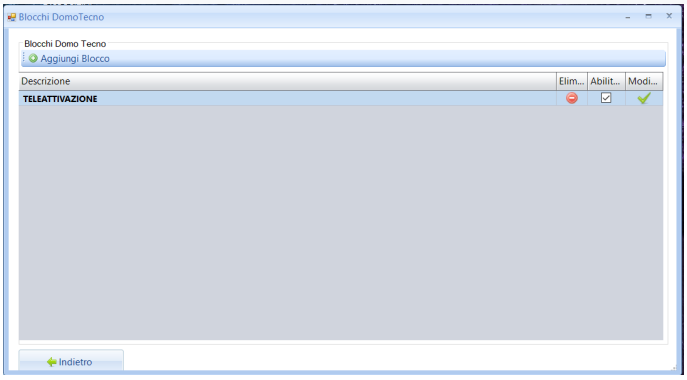
• Domo/Technological Devices List



Elimina	Nr	Fiscal Address	Tipo Device	Descrizione	Abilitato	Comunicazione	Allarme	Manomissione
	1	0035	ATTUATORE ALLARME	COMANDO ILLUMINAZIONE				
	2	0036	ATTUATORE ALLARME	COMANDO TECNOLOGICO				
	3	0057	DOMOTICA AUTOMATISMI	DOMOTICA AUTOMATISMI TAPPARELLE				
	4	0085	ATTUATORE ALLARME	COMANDO CALDAIA				
	5	0086	ATTUATORE ALLARME	TELEATTIVAZIONE REMOTA				
	6	0126	(BS) SENSORE ACQUISIZIONE ALLAR...	ALLARME TECNOLOGICO				
	7	0176	INTERFACCIA SENSORE CREPUSCOLA...	INTERFACCIA SENSORE CREPUSCOLA...				
	8	0177	INTERFACCIA SENSORE TEMPERATURA	INTERFACCIA SENSORE TEMPERATURA				
	9	0179	INTERFACCIA SENSORE PIR	INTERFACCIA SENSORE PIR				
	10	0180	ATTUATORE ALLARME	PRESA COMANDATA				

The list contains the devices programmed and configured as Technological Domes and is a repetition of the General Devices list. With this function it is possible to make any changes to the programming of the devices and perform the Test. The procedures are those indicated for the individual devices.

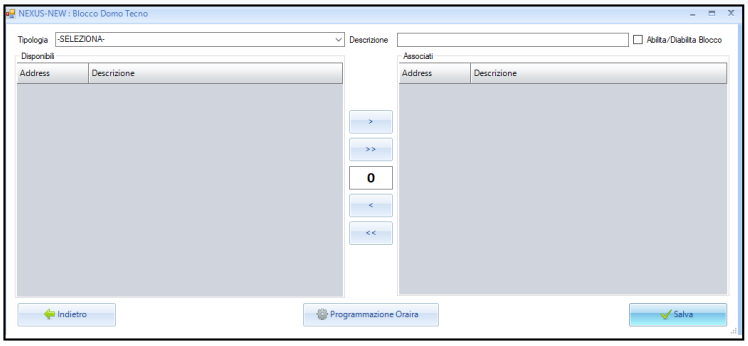
• Block Programming



The Screen displays any Blocks already Programmed.

Programming new Block, The Control Unit allows the Programming of 60 Blocks in the Type:
• REMOTE ACTIVATION = Allows you to send ON/OFF commands to activate electrical devices etc.
(manages interfaces for configured Domotic Actuators and controlled Sockets)
• DOMOTIC FUNCTIONS = Allows you to activate Domotic functions
(manages interfaces for Automation, Climate, Lighting, Heating etc.
• TECHNOLOGICAL CONTROLS = Possibility of Managing Alarms and Technological controls on Devices
(Sensors, Actuators)

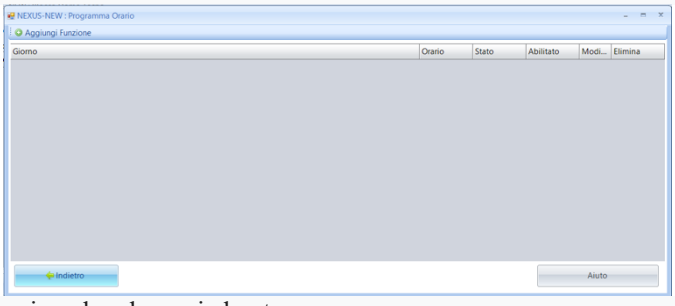
Add new block



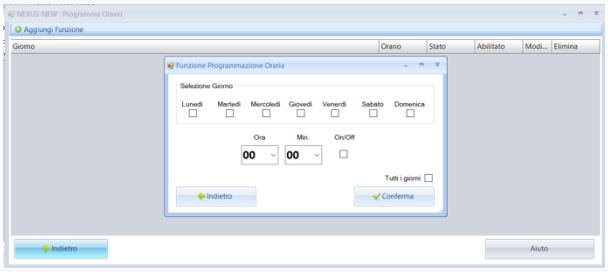
SELECT: Drop-down menu, displays the type of block you want to program
• REMOTE ACTIVATION
• HOME AUTOMATION FUNCTIONS
• TECHNOLOGICAL CONTROLS

Once the selection has been made: The devices programmed for that function will appear in the list of available devices.
• Use the arrow key to select and move the devices to the Associated list
• DESCRIPTION: Enter a 20-character text to define the Block function
• ENABLE/DISABLE: Enable the Block to function
• TIME PROGRAMMING: the Control Unit allows you to associate a Time/Weekly programmer to each block for the Activation/Deactivation of the single Block
• SAVE: Save the data entered
• HELP: Help page for programming

Automatic Programmer



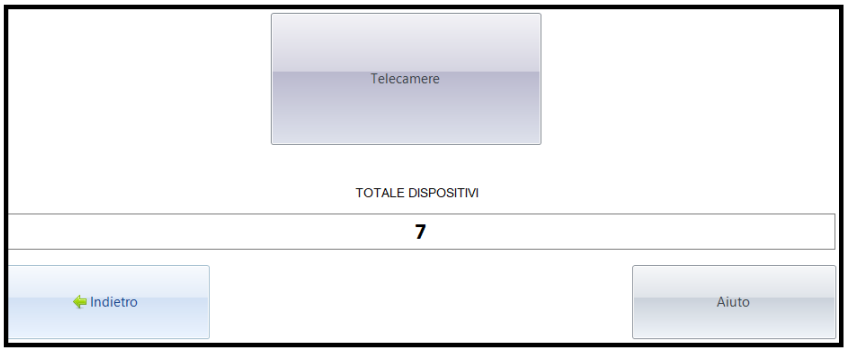
• The Screen Displays any programming already carried out
• To Add new functions
• Add function button, the screen appears



• Day of the week: Indication of the day of the week associated with the function
• Time: Enter Hour/Minute
• ON/OFF: Select the type of operation, Activation/Deactivation
• Every Day: Replicates the first operation for all days of the week
• Delete: Deletes the selected function
• Back: Returns to the previous screen
• Help: Programming help page

Video Surveillance Menu

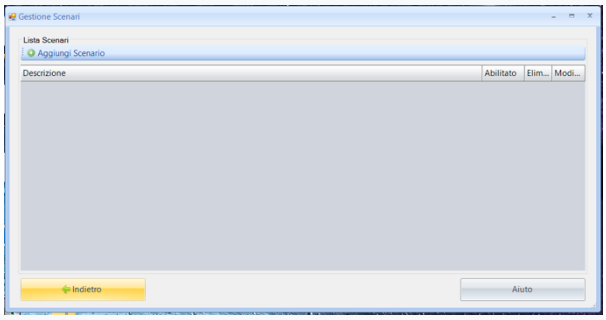
• Cameras



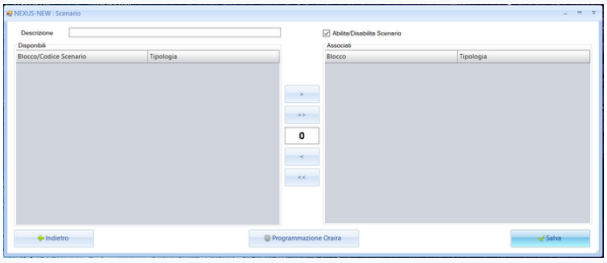
• Cameras: The list contains the programmed Cameras devices and is a repetition of the General Devices list. With this function it is possible to make any changes to the programming of the devices and perform the Test. The procedures are those indicated for the individual devices.
• Back: Return to the previous screen
• Help: Programming help page

Scenarios

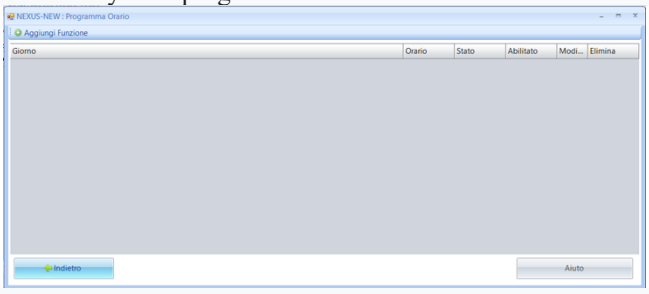
The menu allows you to create Super Blocks that include both Security Blocks and Home Automation.
The activation of the scenarios can be done from the LCD Keyboard, from Touch and from the APP
A single operation to Activate/Deactivate a series of functions that would otherwise be done one at a time



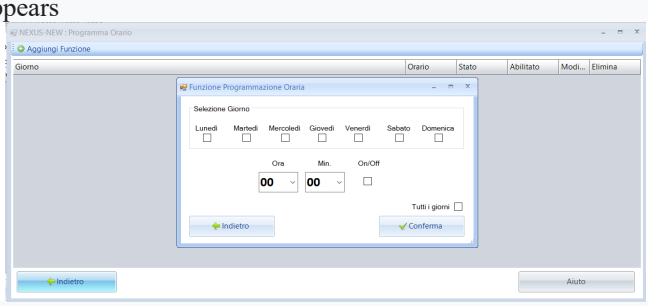
• Scenario List: The list contains the Super Blocks already programmed
• Enable: By clicking on the Scenario it is possible to perform the following operations:
Enable/Disable it - Delete the Scenario - Modify the composition of the Scenario
• Add scenario:



• Description: Enter a 20-character text to define the function
• Available: List of all Programmed Blocks, both Security and Home Automation
Select and Move the blocks you want to insert in the Associated list
• Save: Save the entered data
Also for the Scenarios the control unit allows you to program Automatic Activations/Deactivations



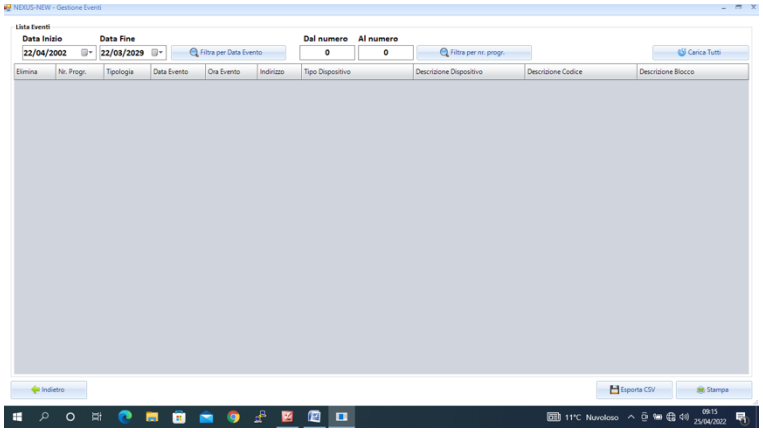
• The Screen Displays any programming already performed
• Add function button, the screen appears



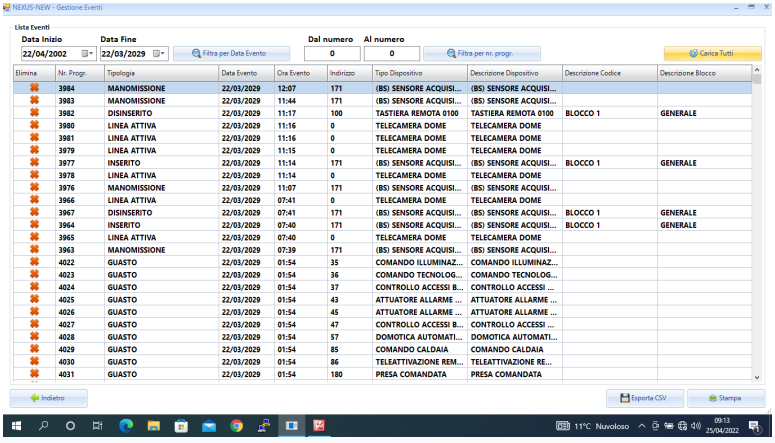
• Day of the week: Indication of the day of the week associated with the function
• Time: Enter Hour/Minute
• ON/OFF: Select the type of operation, Activation/Deactivation
• Every Day: Replicates the first operation for all days of the week
• Delete: Deletes the selected function
• Back: Returns to the previous screen
• Help: Programming help page

Security Event History

The Control Panel cyclically stores the last 1000 events that occur in the System Life.
From the main screen, select Historical Memory.



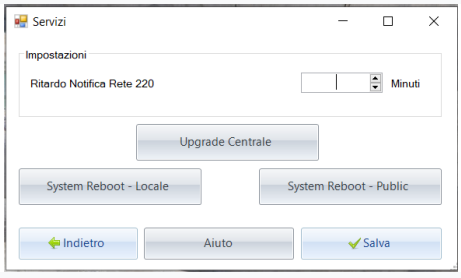
- Start Date/ End Date: Event Search by date
- Filter by Event Date/ From Number to Number: Event Search by date, Select start date and end date
- Filter by Progressive Number: Event Search by progressive number
- Load All: Load all events
- Delete: Possibility to delete one or more events from the history
- Export CSV: Possibility to export the list of Events to a support (USB)
- Print: Possibility to print the Events
- Back: Return to the previous screen



- Start/End Date: Filters the event search by date, enter the data and click
- From number to number: Filters the event search by chronological number, enter the data and click
- Load all: Loads all events
- Delete: Allows you to delete the event from the history
- Progressive Number: Chronological order of events
- Type: Type of event (Theft, fire, robberies, insertions, disinsertions, service events, etc.)
- Event Date: Indicates the date when the event occurred
- Event Time: Indicates the time when the event occurred
- Address: Indicates the physical address of the device that caused the event
- Device Type: Indicates the type of device (Sensor, Actuator, Siren, RFI reader, Keyboard, etc.)
- Device Description: Reports the description associated with the device
- Code Description: Events of Arm/Disarm, indicates the description associated with the Security Code
- Block Description: For Arm/Disarm Events, indicates the Armed/Disarmed block

Services Menu

The Services Menu is composed of the following submenus:
• Network notification delay 200 Vac Absence/Return of network
• Central Upgrade
• Local System Reboot
• System Reboot - Public



220Vac Network Filter

The function allows you to insert a time filter (expressed in minutes) before sending the notification and the SMS message of the absence of the Primary network on the Control Unit.
from the drop-down menu select the delay time.

Central Upgrade

Command key: It connects autonomously to the server and performs the Firmware update
(the Central is supplied with the latest updated Firmware, perform this Operation only in agreement with the manufacturer)

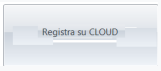
System Reboot- Local

Command key: Allows you to reset the Control Panel (DOES NOT delete any Configuration)

System Reboot- Public

• Command key: Allows you to reset remotely (DOES NOT delete any Configuration)

Record on Cloud

Once all the programming has been done, click on the menu. 

The operation transfers to the remote Server:
a) Customer registration
b) System Configuration Archive
c) Creation of the User to manage the APP

End Connection

Perform all the operations described up to this point (the Programming of the Control Unit is complete)

Click on the End Connection Button 

The following screen appears, it asks you to confirm saving the programming carried out
Make your choice.
The following screen appears, in this phase the PC downloads the programming carried out on the Control Unit
At the end of downloading, move the switch (as shown in the figure) to the ACTIVE STATUS position



Confirm with the OK button, END PROGRAMMING.

Print Configuration

The function allows you to download the configuration of the Control Panel to create paper documentation

The Active State

The Active State is the Normal operating condition of the Control Panel.

Device failure

The control unit constantly polls the devices connected to both the BUS and the LAN network and constantly checks their correct functioning.
In the event of poor communication or device failure, the following events occur:
• Disconnection of the device from the network BUS
• All green LEDs on the keypads and key switches come on
• The event is reported in the Historical Memory
• Display of the event on the keypads with the indication of the address and the text indicating its location or function
• Sending of the Failure message to common telephone terminals with the indication of the address and text
• Sending of the failure notification on the APP with the indication of the address and text
• The device is no longer controlled by the control unit

Tampering

All Security devices (Bosch Sensors, Actuators, Cameras) have an anti-tampering control input.
In the event of opening of the line:

Tampering with a device that is part of a non-inserted block

The following events occur:
• All green LEDs on the keypads and key devices come on
• The event is reported in the Historical Memory
• Display on the keypads with the address and text indicating the location
• Sending of the tampering message to the common and optional telephone terminals associated with the block with the address and text indicating the location
• Sending of the notification on the App

Tampering with a device that is part of an inserted block

The following events occur:
• All green LEDs on the keypads and key devices come on
• Activation of all actuator devices that are part of the block to which the device is associated
• The event is reported in the Historical Memory
• Display on the keypads with the address and text indicating the location
• Sending of the tampering message to the common and optional telephone terminals associated with the block with the address and text indicating the location
• Sending notification on the App

Central Tampering

The control unit is protected by an anti-opening switch, the event causes:
• All green LEDs on the keypads and key sockets turn on
• The event is reported in Historical Memory
• Display on the keypad display with the address and text indicating its location
• Sending of the tampering message to the common and optional telephone terminals associated with the block with the address and text indicating its location
• Sending of the notification on the App

Alarm of a NOT enabled device configured as THEFT/FIRE belonging to an activated block

• The event is reported in Historical Memory

Alarms

Alarm of a device configured as THEFT/FIRE belonging to an inserted block
• Flashing of the red LED on the key devices belonging to the block
• Display on the keypads with the indication of the address and the text indicating its location
• Activation of all the actuator devices belonging to the block to which the device is associated
• The event is reported in the Historical Memory
• Sending of the message on the common and optional telephone terminals associated with the block if enabled to receive such messages with the indication of the address and the text indicating its location
• Sending of the notification on the App.
• In the event of an alarm from the Camera, sending of the Video Clip relating to the monitored area on the APP (The same will be stored in a Server Archive)

Robbery Alarm

The devices configured as ROBBERY are not associated with any Block because they are always active. An alarm of yours:
• The event is reported in Historical Memory
• Sending the message to common telephone terminals with the indication of the address and the text
• Sending the notification on the APP, in case of an alarm from a sensor associated with a Camera, the Video Clip relating to the monitored area will be sent to the APP (The same will be stored on a Server Archive)

Technological Alarm

The alarm of a TECHNOLOGICAL configured device belonging to an inserted block:
• Display on the keyboard display with the address and the text indicating its location
• Activation of all the actuator devices belonging to the block to which the device is associated
• Sending the message to the optional telephone terminals associated with the block if enabled to receive such messages with the address and the text indicating its location
• Sending the notification on the App. In the event of an alarm from a sensor associated with a Camera, a Video Clip relating to the monitored area will be sent to the APP (The same will be stored in a server archive)

220 Vac Network Failure on the Control Panel Power Supply and Remote Power Devices

• The Control Panel will carry out the operations described below after the time filter set in Programming
• Event display on the keyboard display
• All green LEDs on the keyboards and RFI readers will light up
• Message sent to common telephone terminals
• Notification sent to the App.

220 Vac Mains Return on the Central Power Supply and on Remote Power Devices

• Event Display on the keyboard display
• All green LEDs on the keyboards and RFI readers turn off
• Message sent to Common telephone terminals
• Notification sent to the App.

Central Battery with Low Voltage

In the event of a prolonged absence of the primary 220 Vac mains on the central power supply, if the battery voltage drops below the level of 11. Vdc, the following Events occur:
• Out of Service message sent to common telephone terminals
• Out of Service notification sent to the App.
• The Central Blocks All Its Functions

Maintenance Entry from LCD or Touch Keypad

• Enter the Installer Code (SEL XXXX ENT) The Display Shows the event,
• Sending the message to the Common telephone terminals
• Sending the notification to the App.

End Maintenance from LCD or Touch Keypad

• Press the DEL/ESC key
• Sending the message to the Common telephone terminals
• Sending the notification to the App.

Remote assistance

• On the user's Home page, in the Server Address box, enter 2.42.36.38 and in the local address, enter 2.42.36.38
• Put the control unit in maintenance mode
• Connect to the control unit with REMOTE CONNECTION

Reset procedure in the event of control unit default

• Put the switch into commissioning
• From the programming tool, select the system and click on the RESET button, wait for the control unit to restart (the restart LED flashes)
• The control unit starts with the default address 192.168.1.107 and all data reset