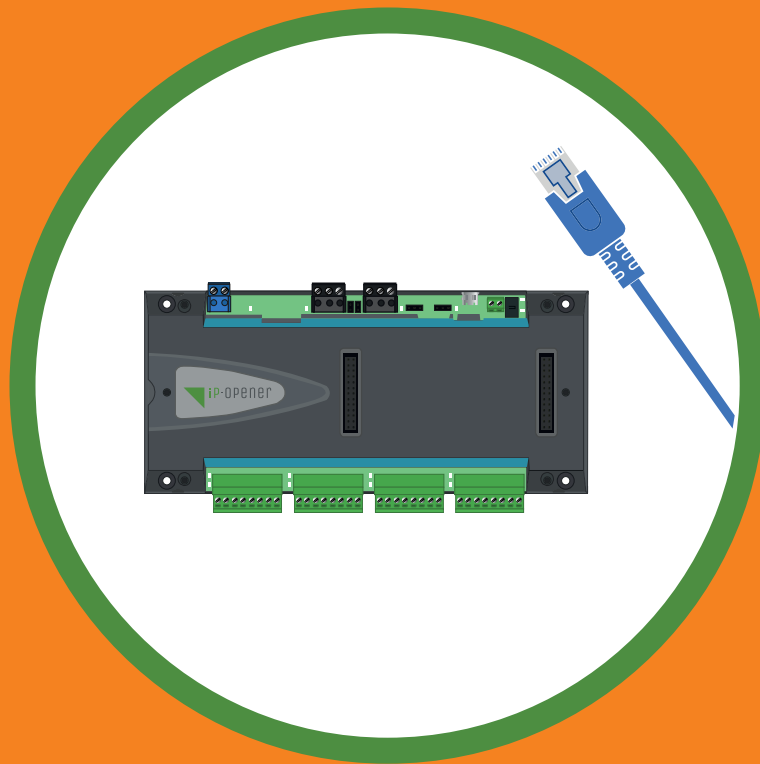




GM-IPOP



CONNECTION QUICK GUIDE

1.TABLE OF CONTENTS

1.Table of contents.....2

2.Introduccion3

3.Controller connection.....3

 3.1.Networks3

 3.2.Controllers5

4.Controller on iP Openner Manager5

5.Troubleshooting6

 5.1.The installation does not operate stably6

 5.2 iP-Opener Manager does not detect the controller.7

 5.3.Fixed IP configuration9

 5.4.Hard reset9

6.Connection diagrams.....10

7.Video intercom connection diagrams.....17

2.INTRODUCTION

This guide contains all the information of interest concerning the connection of the iP Opener system.

3.CONTROLLER CONNECTION

3.1. Networks

There are different connection topologies. These networks can be TCP/IP, RS485 or a combination of both:

- UTP.
- RS485.
- UTP + RS485.

Notes

- There will be more than one network when the devices to be connected are not in the same installation (same internet connection network).

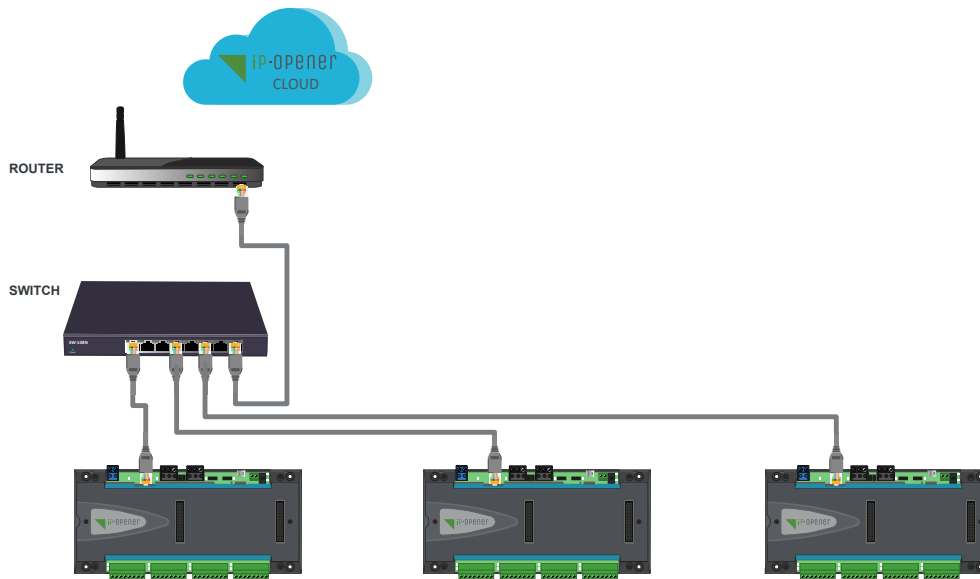
Example:

In offices with a unique Internet connection, a single network must be generated in iP-Opener. On the other hand, in a company composed of a head office and several branches, a network per location must be generated.

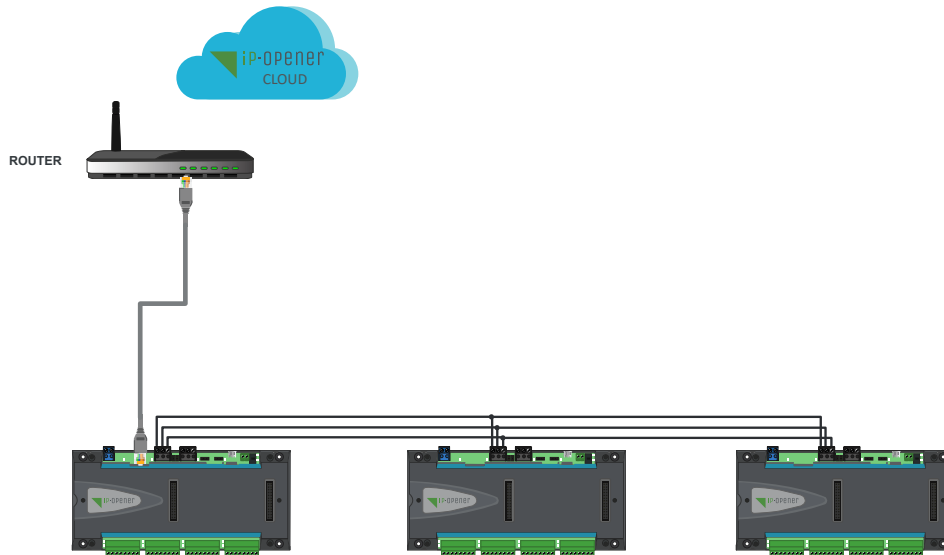
*In offices with a unique Internet connection, a single network must be generated in iP-Opener. On the other hand, in a company composed of a head office and several branches, a network per location must be generated.

Connection topologies for remote management:

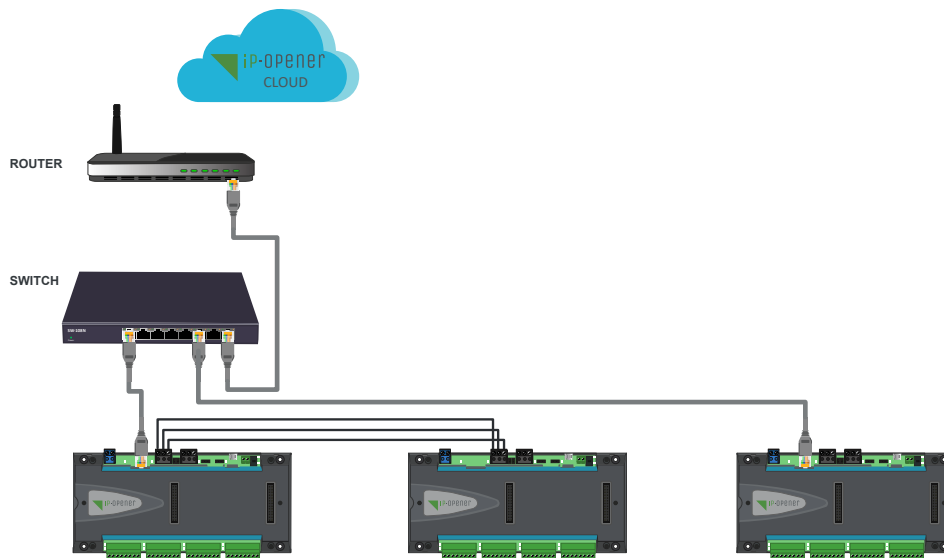
- UTP connection




- RS485 connection

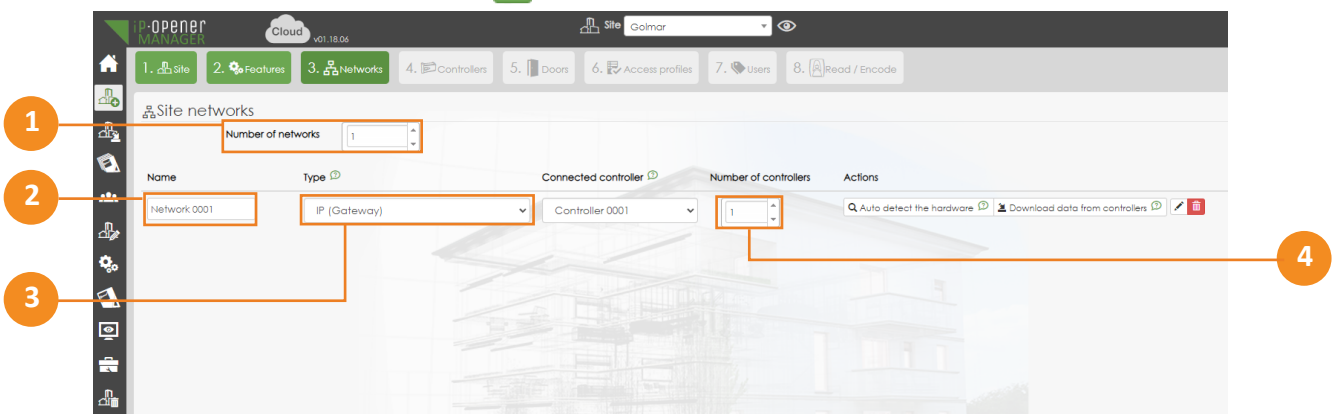


- Mixed connection: UTP + RS485

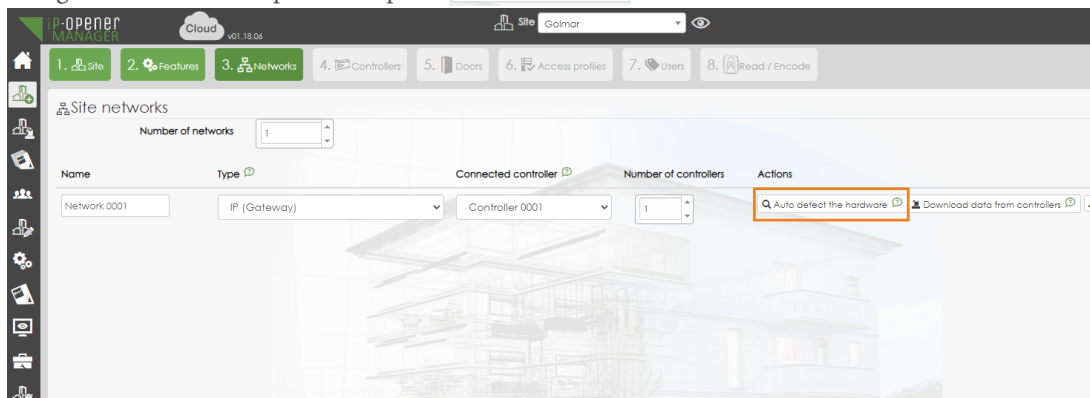


Generate a site as described in the iP-Opener Manager user manual. Taking into account the topics “3.Networks” and “5.Centrals” detailed below:

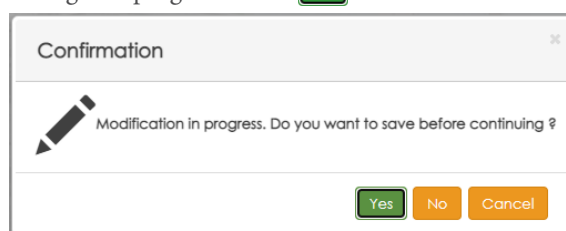
- 1 - Indicate the number of networks “1”.
- 2 - Set a name for the network to be generated that you can identify.
- 3 - Select “IP - Remote” type.
- 4 - Indicate the number of controllers you have in the installation connected by UTP cable to the switch or router. After this step, confirm the changes by clicking on .



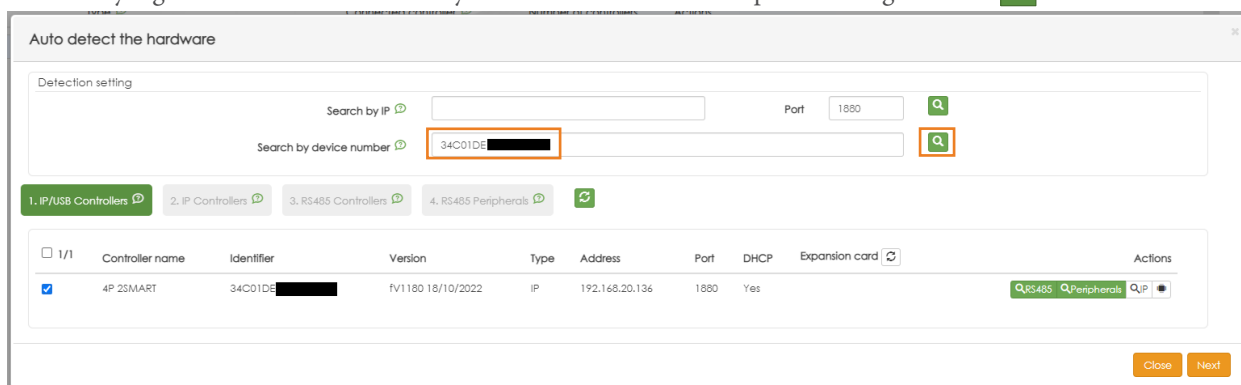
Once the changes have been done, press the option  to detect the controller.



In case you receive a warning about changes in progress. Click .

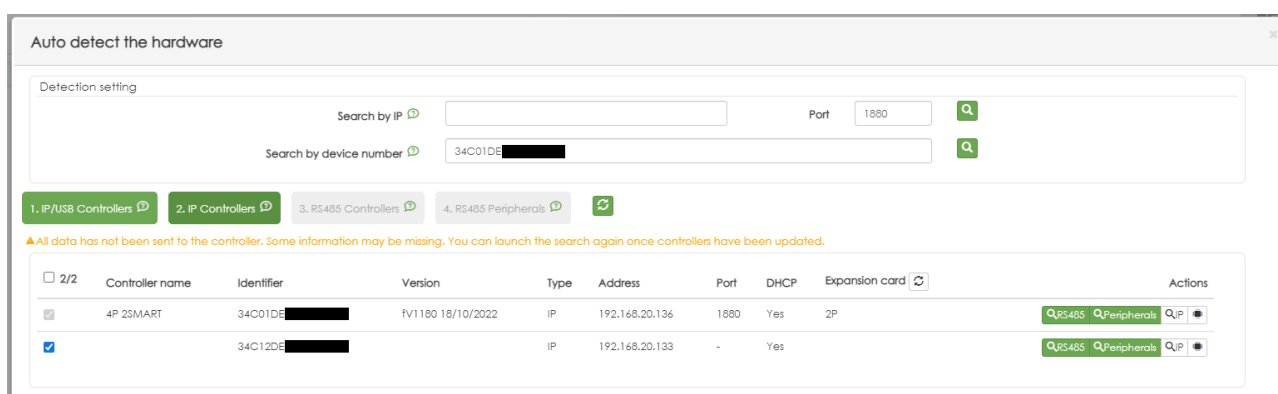


Enter in “Search by login” the ID of the controller you want to connect to iP-Opener Manager. Click .





Select the detected controller  and press .

It will now detect other IP controllers that are on the same network.



Select the rest of the detected IP controllers  and press .

The following detection steps: “3. RS485 controllers” and “4. RS485 peripherals” would be more oriented to a mixed “IP&RS485” type installation.

In the example shown here, there are no devices connected via RS485. Advance these two steps by pressing  and  in the last phase of the detection process.

3.2. Controllers

1 - Indicate a name to identify each of the controllers. Example: controller nº1.

2 - Registered controller ID.

3 - Controller model.

Controller “2 wire / IP controller V2”: For controllers with 2SAFE bus and TCP/IP communication.

Controller “Wiegand / IP controller V2”: For controllers with Wiegand protocol and TCP/IP communication.

4 - Expander coupled to controller. If an expander is attached to the controller, specify the type of model:

12 relays 5A. Reference GM-IPOP-EXP12S.

12 analog inputs. Reference GM-IPOP-EXP12E.

4 Wiegand doors. Reference GM-IPOP-EXP4PW.

2SAFE doors (b2f). Reference GM-IPOP-EXP2P.

5 - Doors. Number of doors of the controller:

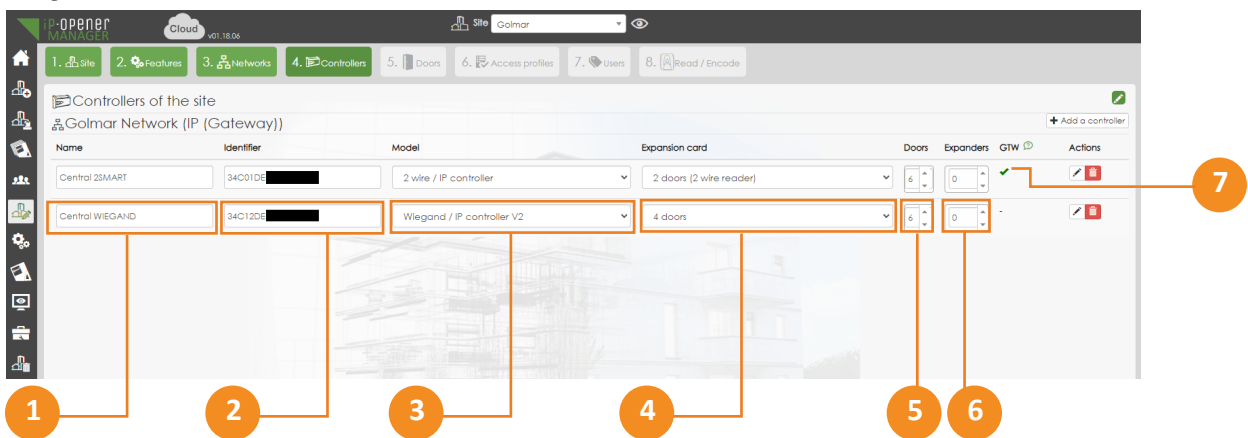
GM-IPOP-1P. 1 Door.

GM-IPOP-4P. 4 Doors.

GM-IPOP-2P-WIEG. 2 Doors.

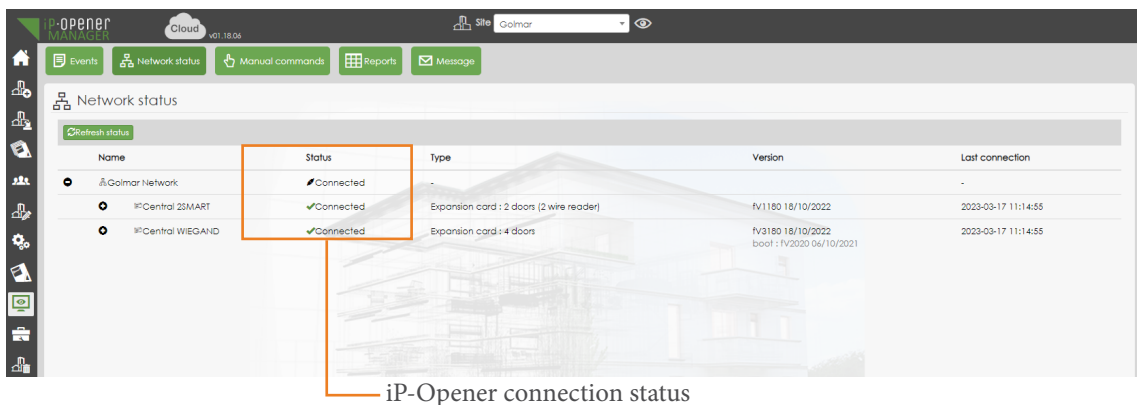
6 - In case any RS485 module is connected, indicate the quantity in the “Expanders” field and fill in the data of the module to be added.

7 - Tick indicating the controller that connects to the server.



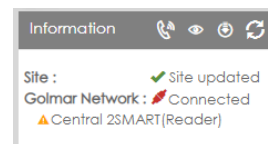
4. CONTROLLER ON IP-OPENER MANAGER

Once the network has been generated and the controllers have been added, you can check if iP-Opener has communication with each one of them. To do so, access the “supervision” section and then click on the “network status” option .



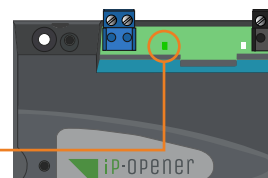
iP-Opener connection status

It is also possible to access “network status” by clicking on “site” or “network” in the information block:



IMPORTANT

The controller that communicates with the iP-Opener will keep the LED next to the power supply terminal board illuminated in green.



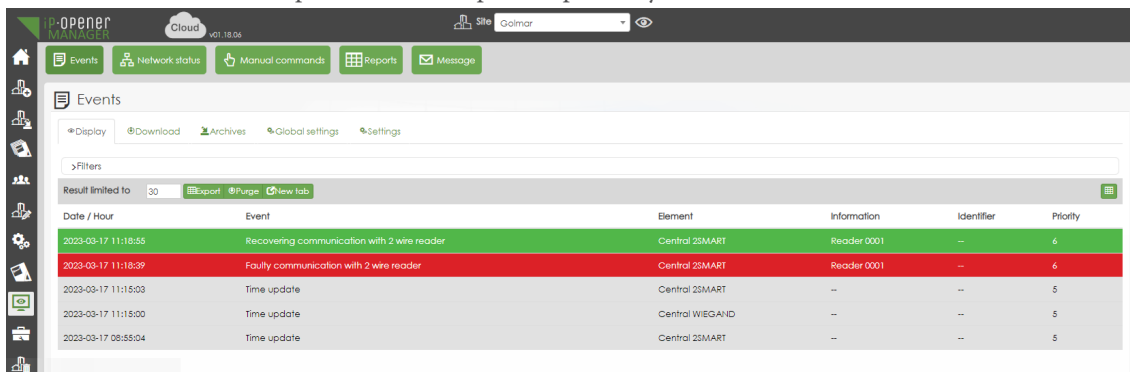
5.TROUBLESHOOTING

5.1. The installation does not operate stably

1) Check that the cable used is suitable for the installation:

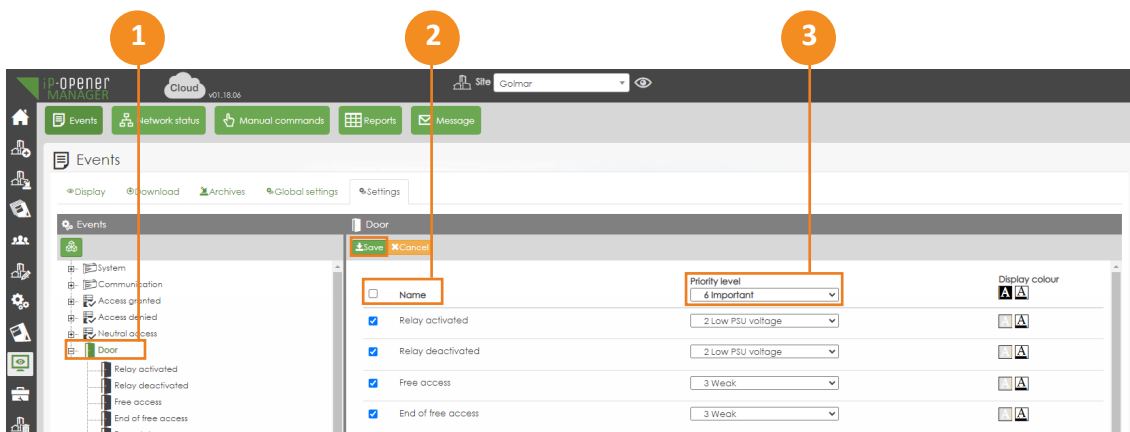
Type of connection	Type of hardware	Type and characteristics of the cables
Ethernet bus	Controllers, switch/router	UTP CAT 5 to CAT 7 (SFTP or FTP). Max. distance 90m. It is recommended to use UTP-CAT6ELH cable.
RS485 bus	Controllers, I/O expanders	STP. It is recommended to use M-26CALH cable.
2SAFE BUS	Peripherals, readers, 2SAFE receivers	FTP or SFTP. It is recommended to use M-26CALH cable.
Wiegand	Readers	UTP/STP or SFTP up to 100m. It is recommended to use M-26CALH cable.
Power supply		2 wires x 1 mm diameter.

2) Check in the “events” section of “supervision” if iP-Opener reports any incident:



By default iP-Opener displays alerts related to “system” and “communication”. If the incident is of a different nature, it can display alerts from other categories as follows:

- 1 - Select the type of alert you want to be able to monitor.
- 2 - Select the specific alert to receive or check “last name” to select all.
- 3 - Check priority 5 or higher for the alert to be displayed in the monitoring “view” tab.



This way it will be possible to locate the failure and see the indicated fault.

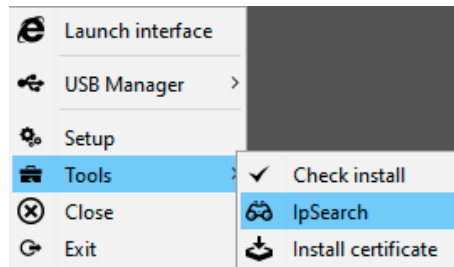
5.2. iP-Opener Manager does not detect the controller

1) Check that the controller(s) are on the network.

The default IP of the controllers is 192.168.1.250 but these come from the factory in DHCP. So if the network to which they are connected works with DHCP, the router will assign a different IP to the controller. We will be able to identify the IP with iP-Opener's own search application: IP Search.

It is possible to run IP Search in two ways:

- From the "tools" folder of the program installation path. Example: C:\ip-opener_client_tools
- By running the iP-Opener Client and opening the Tools>IP Search function.



To detect controllers on IP Search we must be connected to a PC in the same network and click on the "refresh" option. At this point it should show the controller(s) connected to the network:

 A screenshot of the 'Search IP component by UDP - 2.14.0' application window. The window has a title bar with standard Windows controls and a 'Golmar' logo. Below the title bar are buttons for 'Refresh', 'Advanced filter', and 'Find an address'. The main area contains a table with the following data:

Mac address	Application	IP address	Mask	Gateway	Version	Date	Name	Hard version	Date/time
00:26:DE:13:55:80	Ip-opener (0x4c)	192.168.1.185	255.255.255.0	192.168.1.1	V1.122	25/02/2021	34C01DE1355B06E9	2 1	06/04/2021 11:...

In case the controller/s of the installation appears we will have the certainty that the problem is not in the communication of the controller with the network of the installation.

2) Check that the controller(s) communicate with iP-Opener.

Once it is known that the controller/s are connected to the network, the next process to perform would be a Ping to the iP-Opener DNS server: ping `srv.ip-opener.com` (from the windows command console). In case the 4 packets sent are shown as received. We will have the confirmation that the network has communication with iP-Opener.

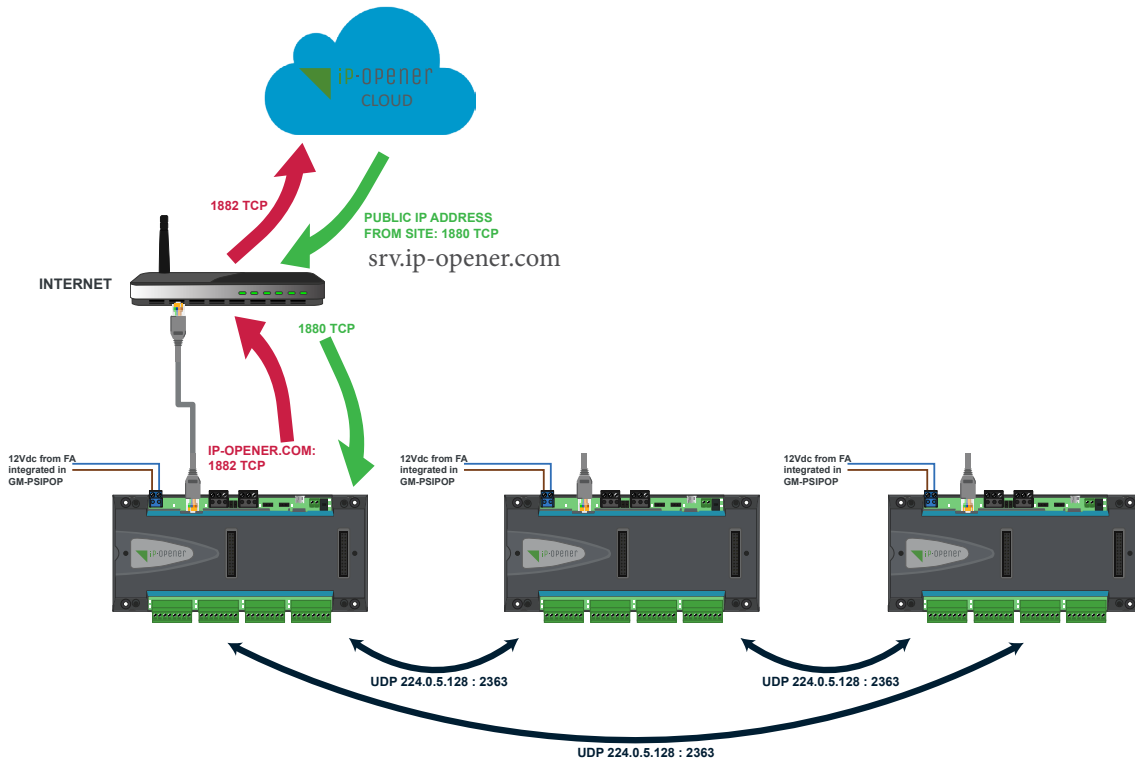
 A screenshot of a Windows command prompt window titled 'Símbolo del sistema'. The user has entered the command 'ping srv.ip-opener.com'. The output shows four successful ping responses from 54.37.103.95, each with 32 bytes of data, a response time of 35ms, and a TTL of 46. Below the responses, statistics are shown: 'Estadísticas de ping para 54.37.103.95: Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos). Tiempos aproximados de ida y vuelta en milisegundos: Mínimo = 35ms, Máximo = 35ms, Media = 35ms'. The prompt is now ready for the next command.

3) Check network configuration.

If the result of any of the two previous points is not satisfactory (controller is not on the network or does not connect with iP-Opener) pay special attention to the network configuration (router).

- In the iP-Opener system, it is the controller that opens the communication with the server. By default, the controller tries to connect to Ip-Opener.com through port 1882. This means that **port 1882 has to be open** from Ethernet to the Internet.
- In most computer networks, only the incoming ports are blocked by the firewall/router, but in case the controller does not connect to the Ip-Opener.com server, this has to be checked.
- Since it is the controller that opens communication with the server, we do not need to create a NAT on the router or set an IP address. **This can be DHCP.**
- At least one controller per site will act as a gateway for the others, it will receive the information from iP-Opener through port 1880. So this incoming port must be open.
- These communication ports can be modified through iP-Opener manager or IP Search.
- The controllers communicate with each other via UDP 224.0.5.128 :2363.

In the following diagram you can see how the communications work:



4) Reset controller to factory defaults.

This guide describes what is necessary to connect a controller or system to iP-Opener. In case the controller to be connected had previously worked in a local configuration or there is a problem with the controller, you can reset the controller to factory defaults, as indicated below:

Access to IP Search (defined as access in point 1) and select the controller to be reset:

Search IP component by UDP - 2.14.0

Mac address	Application	IP address	Mask	Gateway	Version	Date	Name	Hard version	Date/time
00:26:DE:13:55:80	Ip-opener (0x4c)	192.168.1.185	255.255.255.0	192.168.1.1	FV 1.122	25/02/2021	34C01DE1355806E9	2 1	06/04/2021 11:...

In the “Commands” tab select “delete database” and then “Send”:

TCP/IP configuration Communication server UPNP configuration **Commands**

Restart controller.
 Delete database. Send
 Send a sentinel
 Test server communication

End of treatment Close

A small pop-up window will appear, prompting for a password, enter 0000 and click “Connect”.

Connexion

Login: admin

Password: 0000

Then it will indicate that the command has been sent. At this point the controller will be reset to factory defaults.

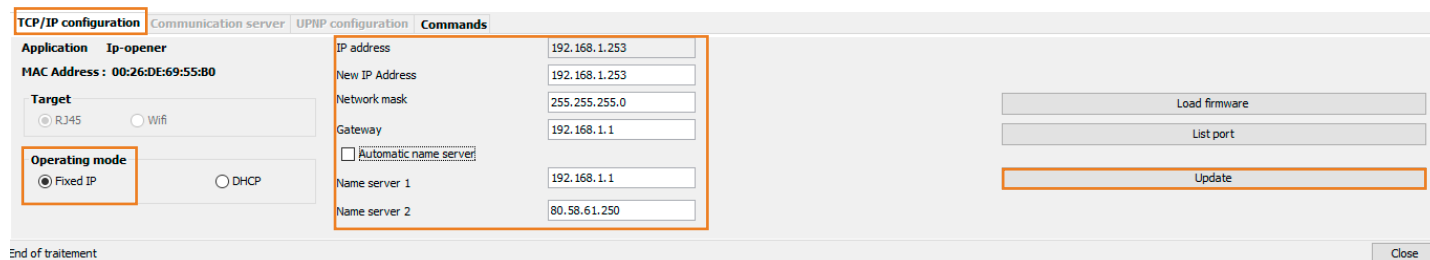
Configuration

5.3. Fixed IP configuration

If the network to which the controller(s) is connected operates exclusively with fixed IPs you can change this from:

1) IP Search

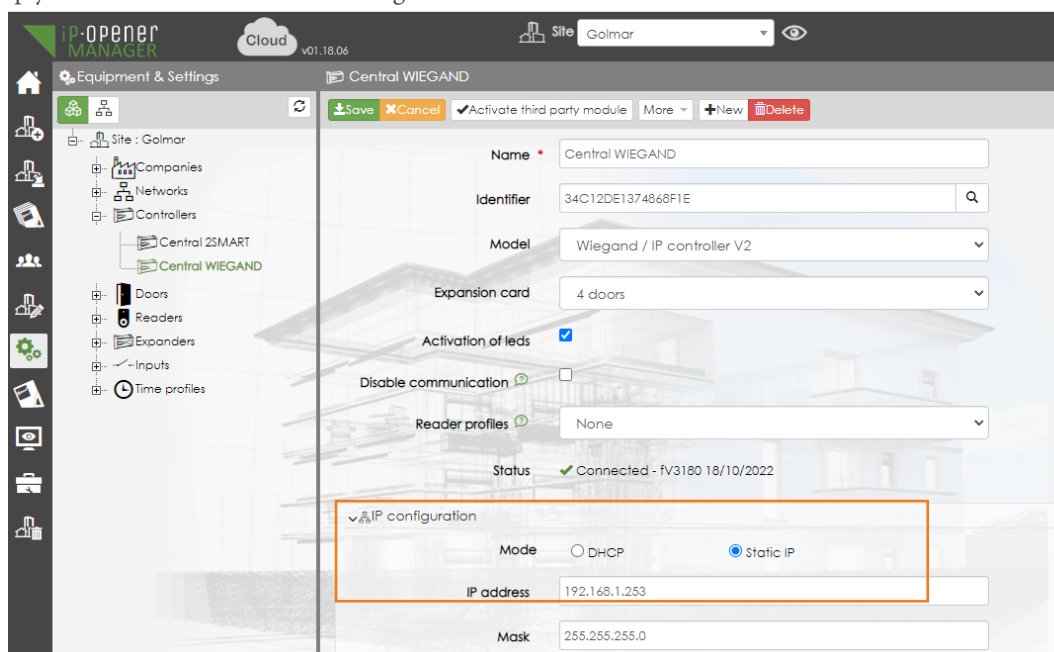
By selecting a controller in the “TCP/IP configuration” tab at the bottom of the screen, you can set the “Fixed IP” operating mode. Then enter the fixed IP to be set and your network parameters. If you do not know the server IPs to be used, activate the “automatic name server” option. Once you have completed the data, validate the changes by clicking “Update”.



2) iP-Opener manager

In iP-Opener manager you can perform the same operation by going to the “Configuration” section. To do so, once in this section, click on “Controllers” and then select the controller you wish to change the type of connection.

At this point simply select “Fixed IP” in the “IP Configuration” section.



5.4. Hard reset

The reset from iPSearch clears the database, but does not reestablish the IP interface configuration of the controller. In case it is necessary to reestablish a controller completely, it is possible to perform a hard reset. The sequence for this is shown below:

- 1- Turn OFF the controller.
- 2- Make a link (a jump) between maintenance terminals 1 & 2 (*).
- 3- Turn ON the controller.
- 4- Within the 2 first seconds, release the link and link again terminals n° 1 & 2.
- 5- The red led (normal behaviour = 1/ 3seconds) will flash 3/second.
- 6- The controller will stop and restart.
- 7- The controller will have been reestablished.
- 8- Return the jumper to the factory position (PIN 2 and 3).

(*) To do so, remove the jumper and make the bridge with the same jumper or with a screwdriver.



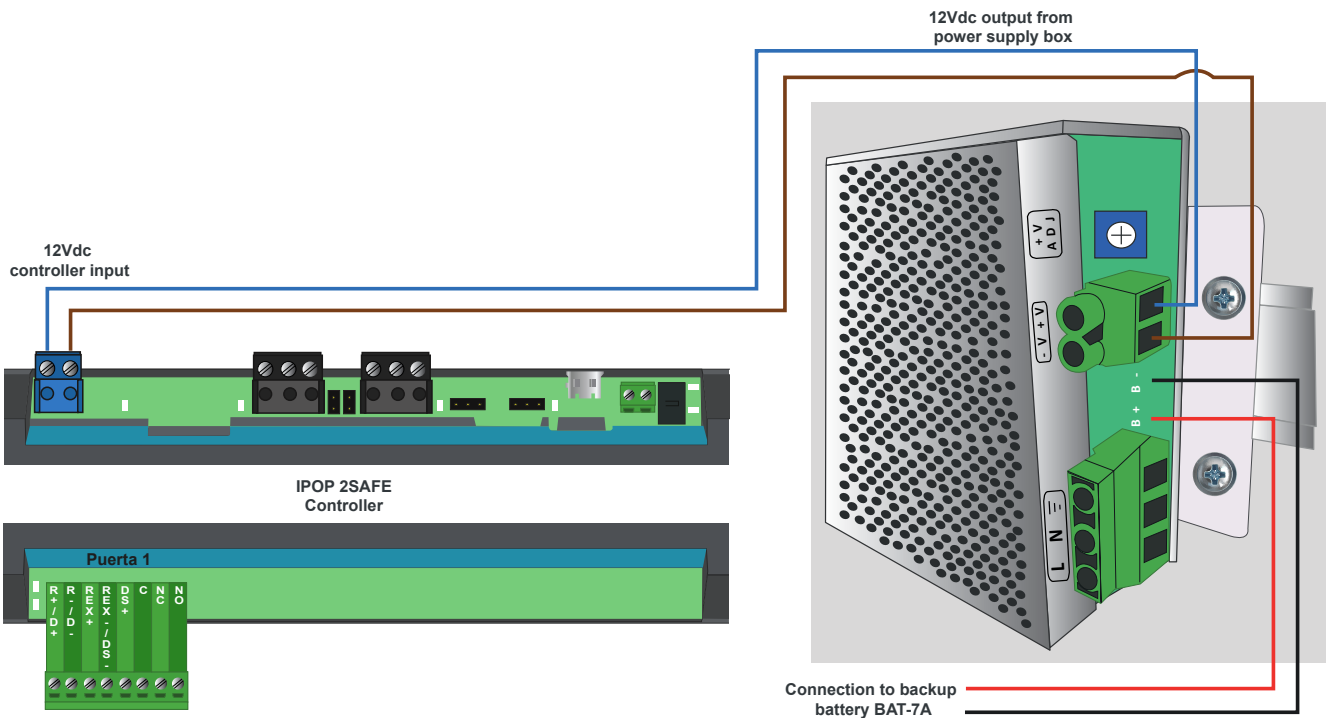
6.CONNECTION DIAGRAMS

BEFORE TO START

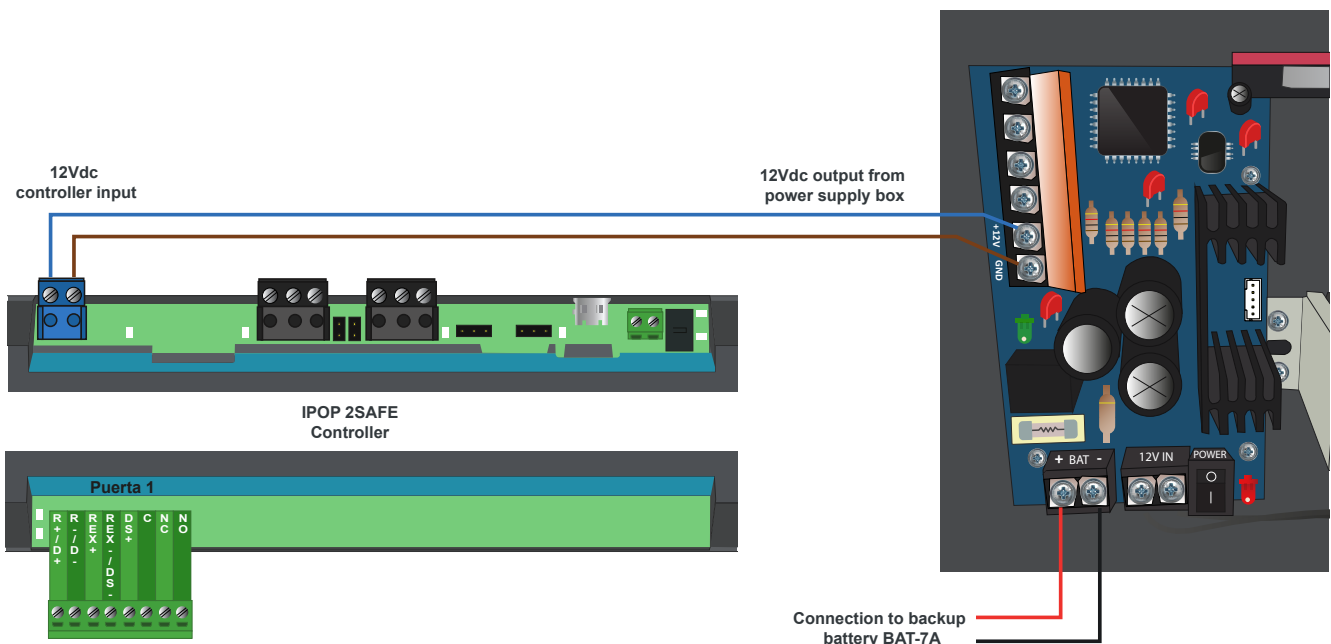
- Use the supplied voltage protectors to protect the system from voltage spikes (see connection in the following diagrams).
- IMPORTANT:** In 2SAFE technology the protector will be supplied together with the readers, while in WIEGAND technology the protectors are supplied with the controller.
- In case of setting long opening times, acquire automatic door openers (with memory) such as the CV-24 and set the opening time to 1sec. Long opening times of more than 15 seconds can damage the opener.
 - In cases where high consumption devices (such as motorized gates) are connected, it will be necessary to add a SAR-12/24 relay. See diagram "230V device connection".

Power connection with controller

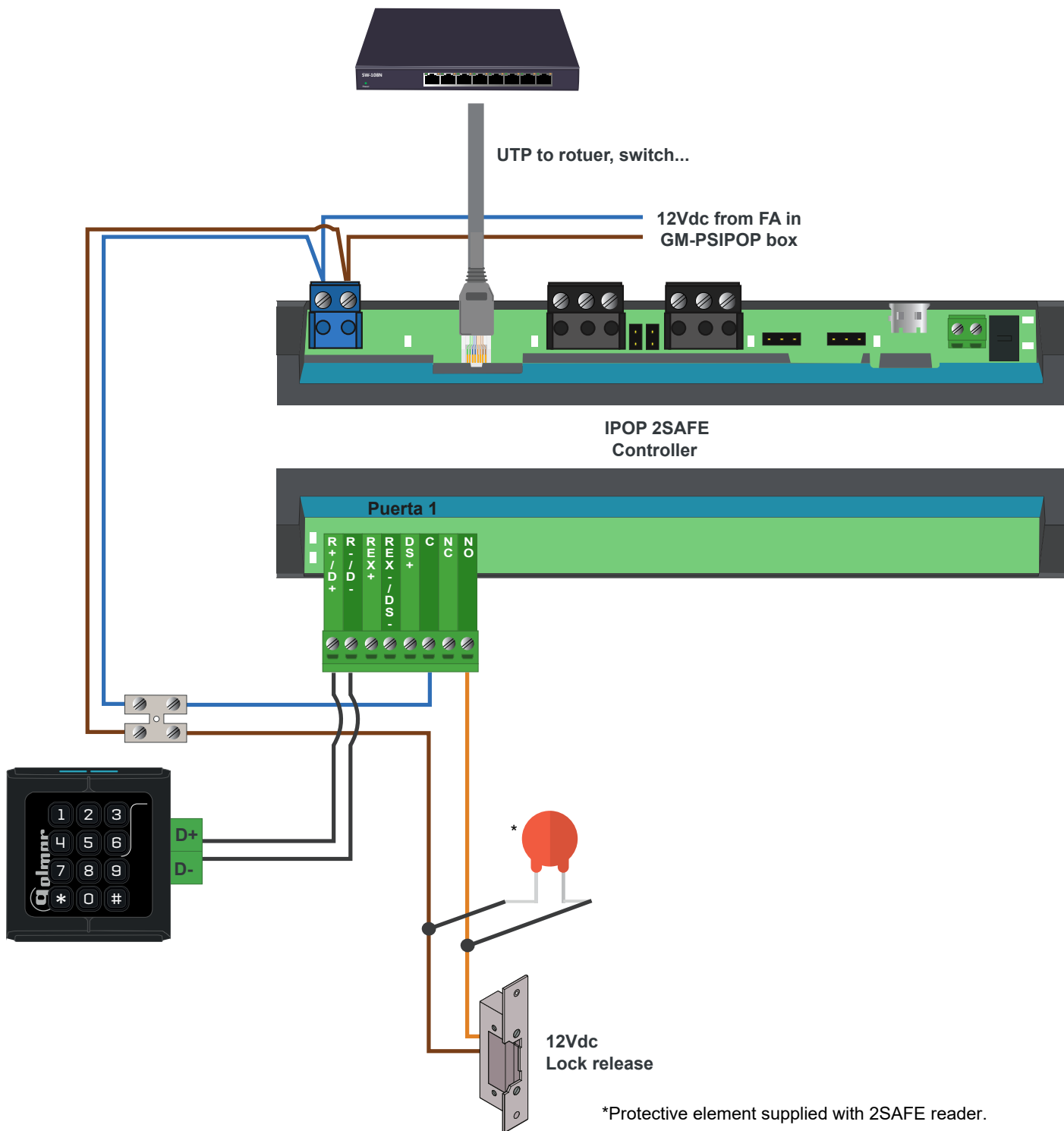
Controller power supply when using GM-PSIPOP (20780203) and GM-PSIPOP-G (20780125) boxes.



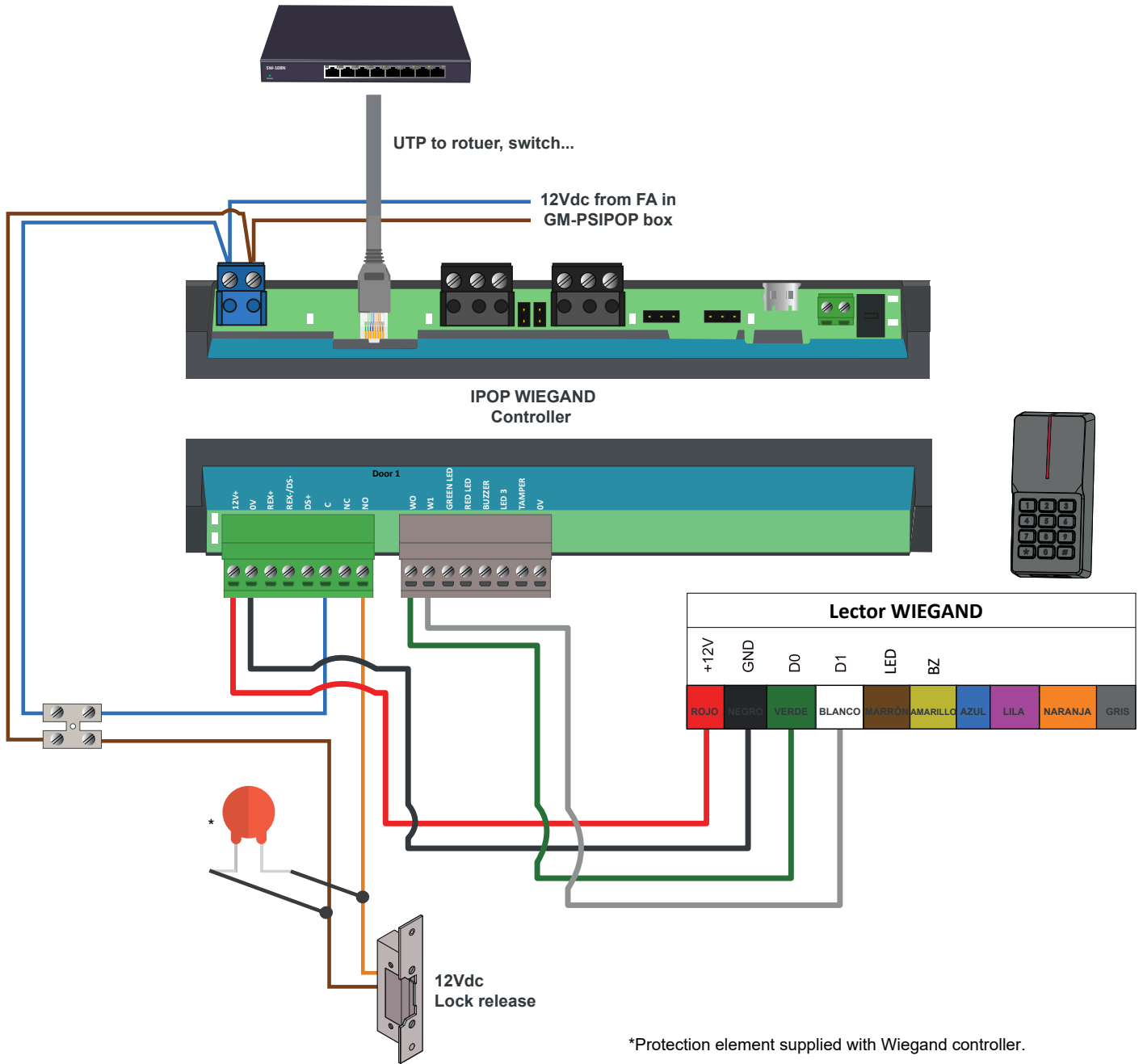
Controller power supply when using GM-PSIPOP-P boxes (20700011).



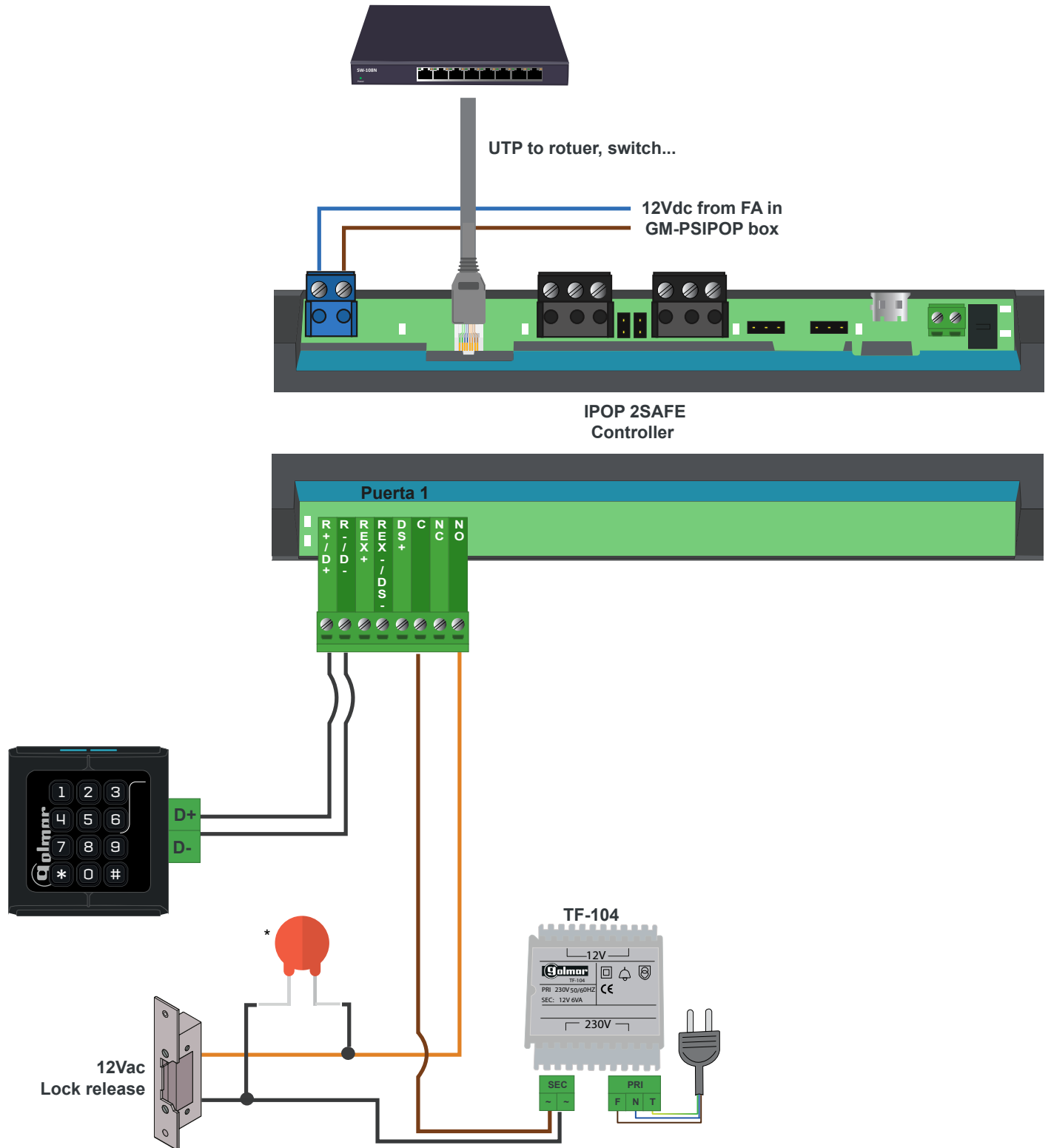
2SAFE reader and DC electric lock release



WIEGAND reader and DC electric lock release

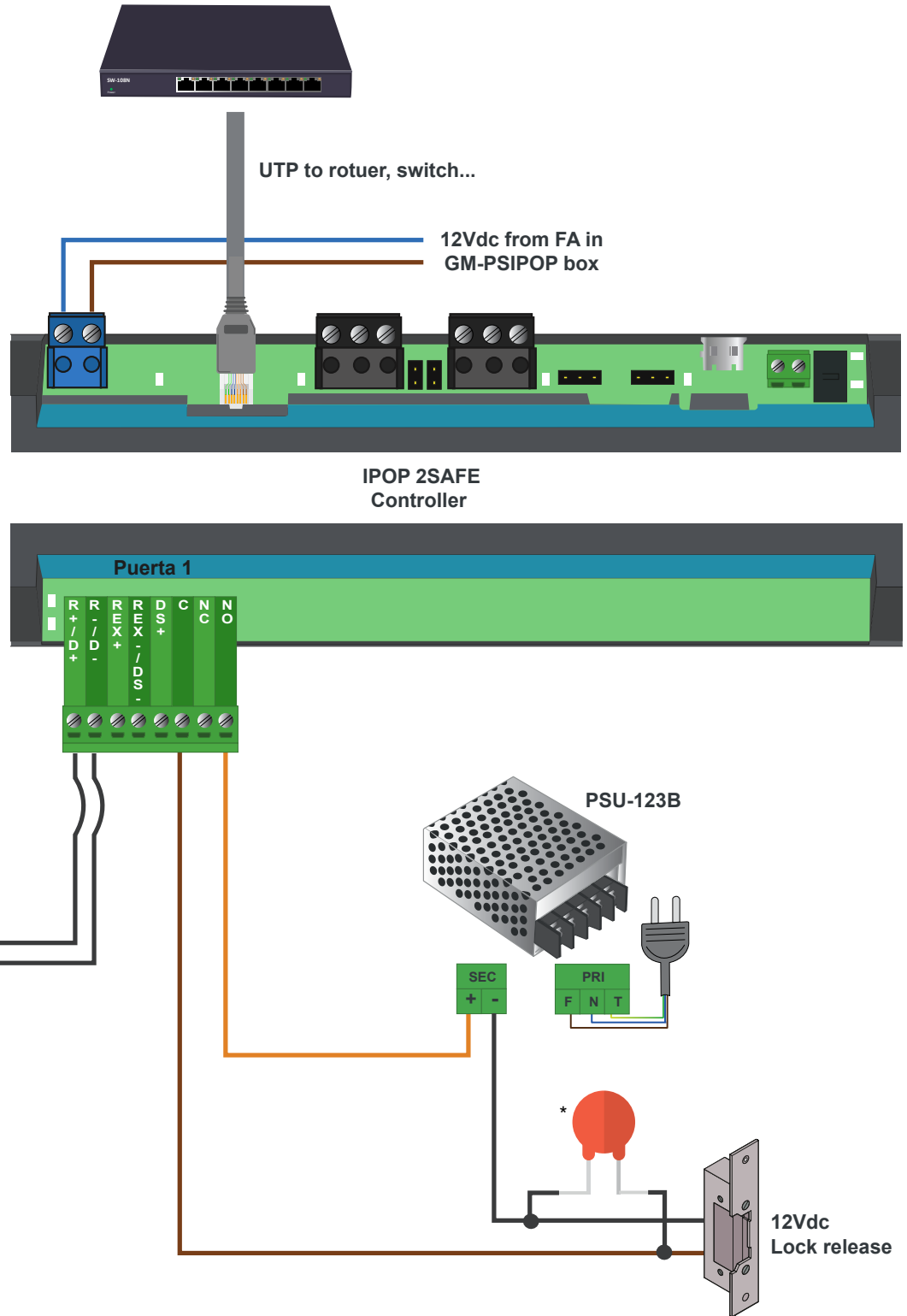


2SAFE reader and AC electric lock release



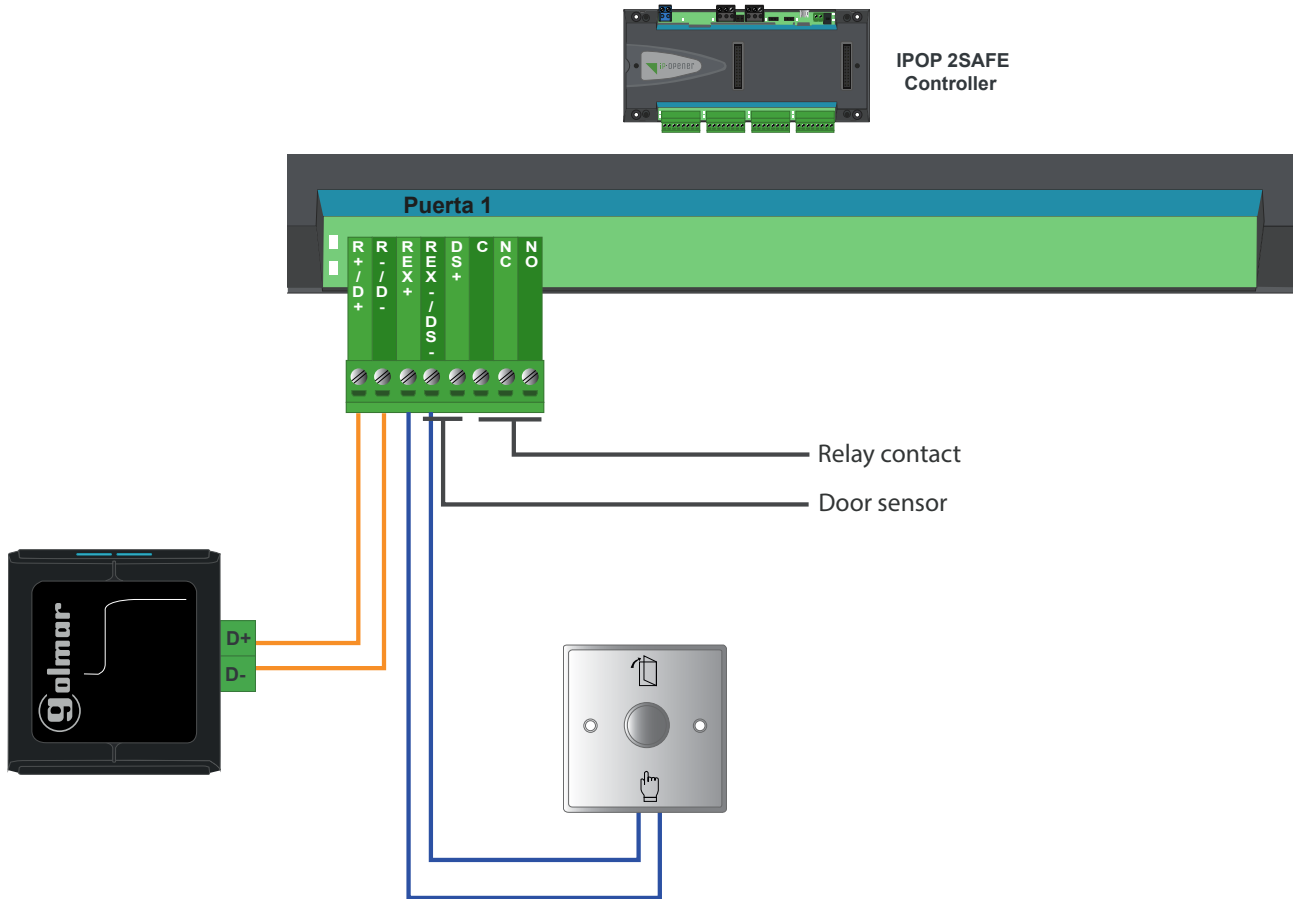
*Protective element supplied with 2SAFE reader.

2SAFE reader and DC electric lock release with independent power supply

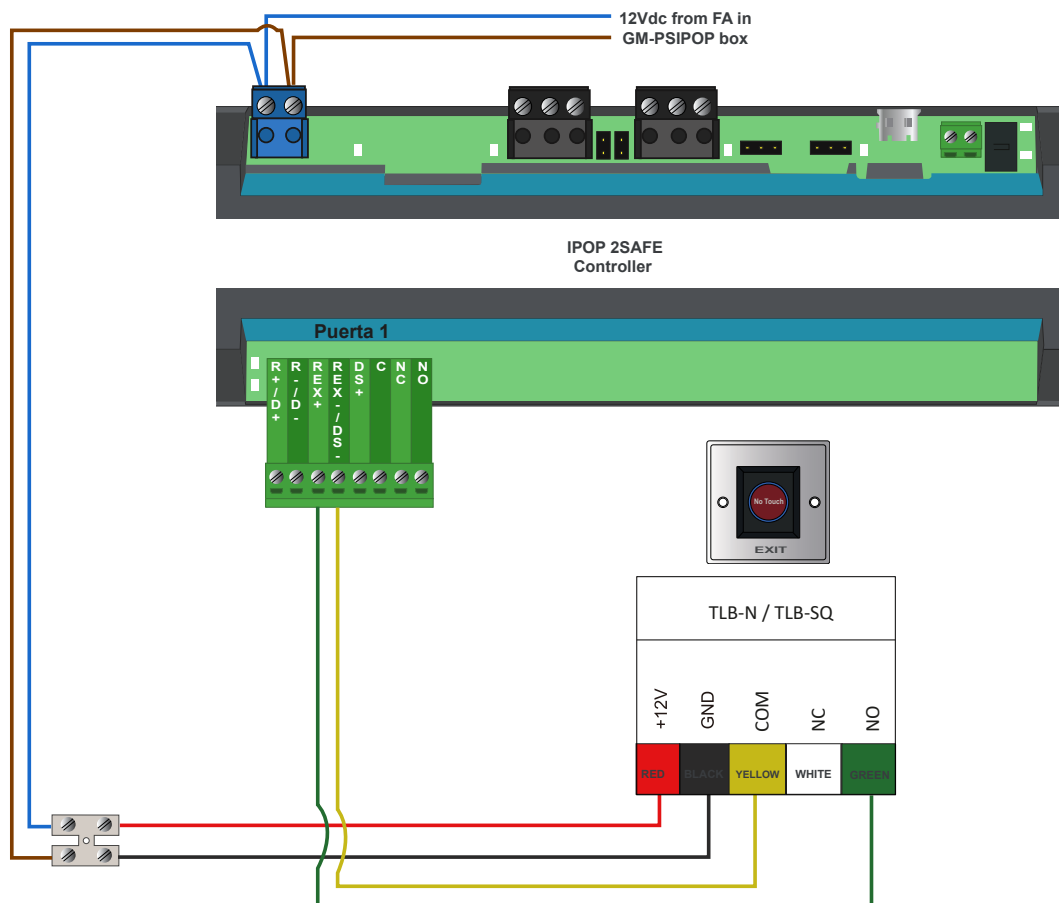


*Protective element supplied with 2SAFE reader.

Output pushbutton connection



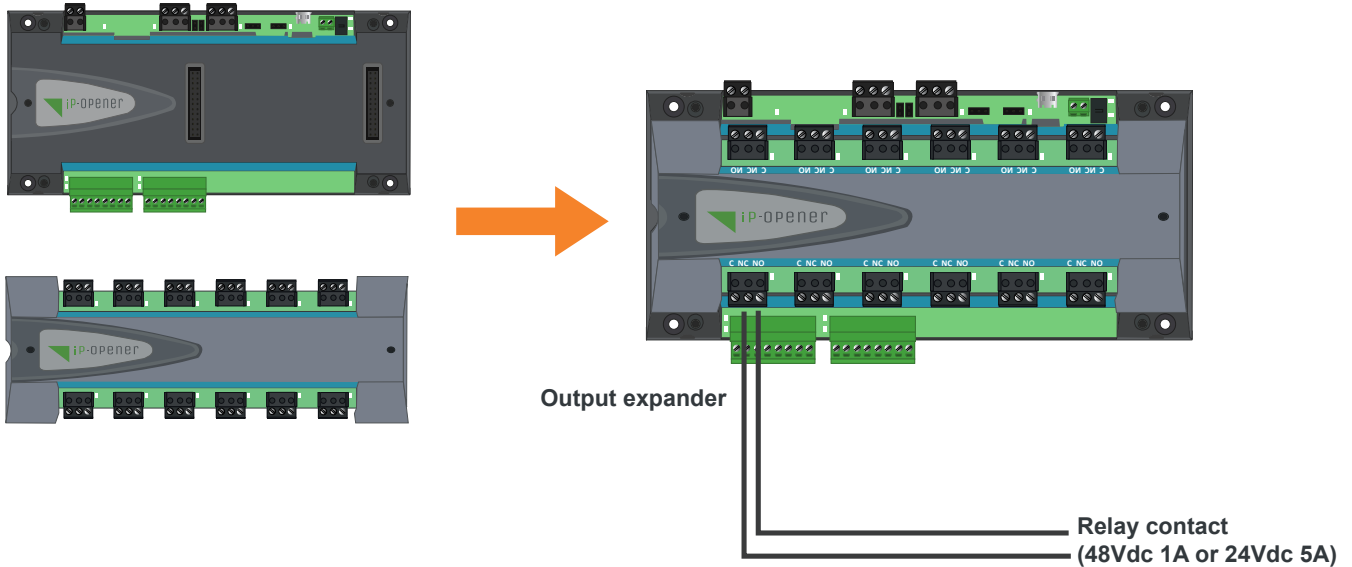
Proximity exit button connection



Relay expander connection

For the connection of expanders, these must be coupled on the controller. Below is an example of connection with the expander GM-IPOP-EXP12S.

Coupling output expander GM-IPOP-EXP12S with IPOP controller:



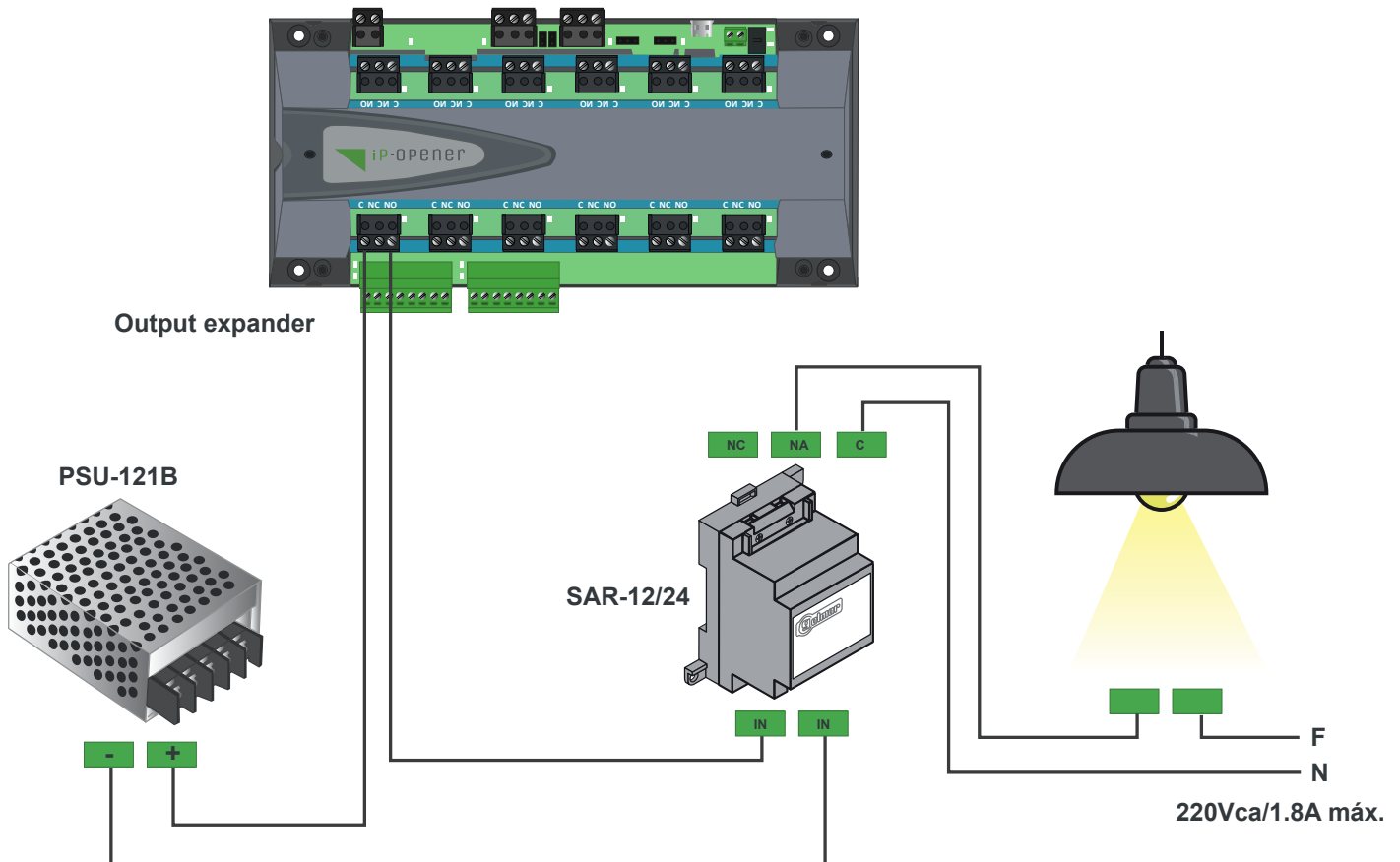
Connection of high consumption devices

IMPORTANT

The outputs of the GM-IPOP-10S-RS485 module and the GM-IPOP-EXP12S expander support up to 5A:

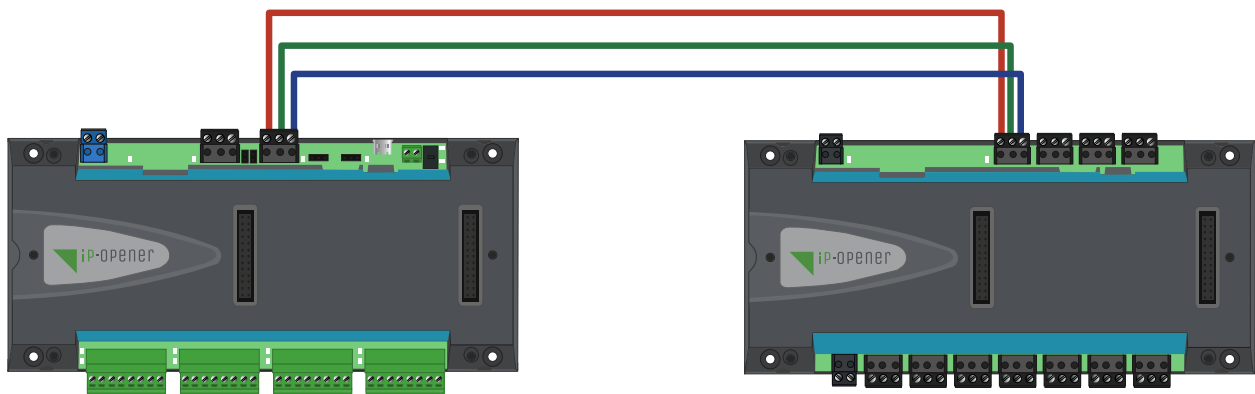
- 5A with 24Vdc power supply
- 1A with 48Vac power supply

In case a higher consumption has to be run, a relay must be added at the output. See example diagram below:



RS485 module connection

RS485

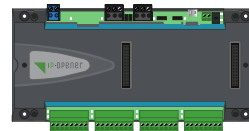


iP OPENER
CONTROLLER

INPUT OR OUTPUT
MODULE

7.VIDEO INTERCOM CONNECTION DIAGRAMS

6502 and 6507 2SAFE panel connection



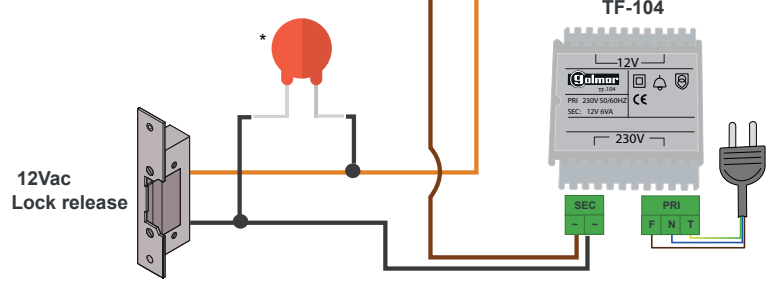
IPOP 2SAFE
controller



6502 and 6507
2SAFE panels

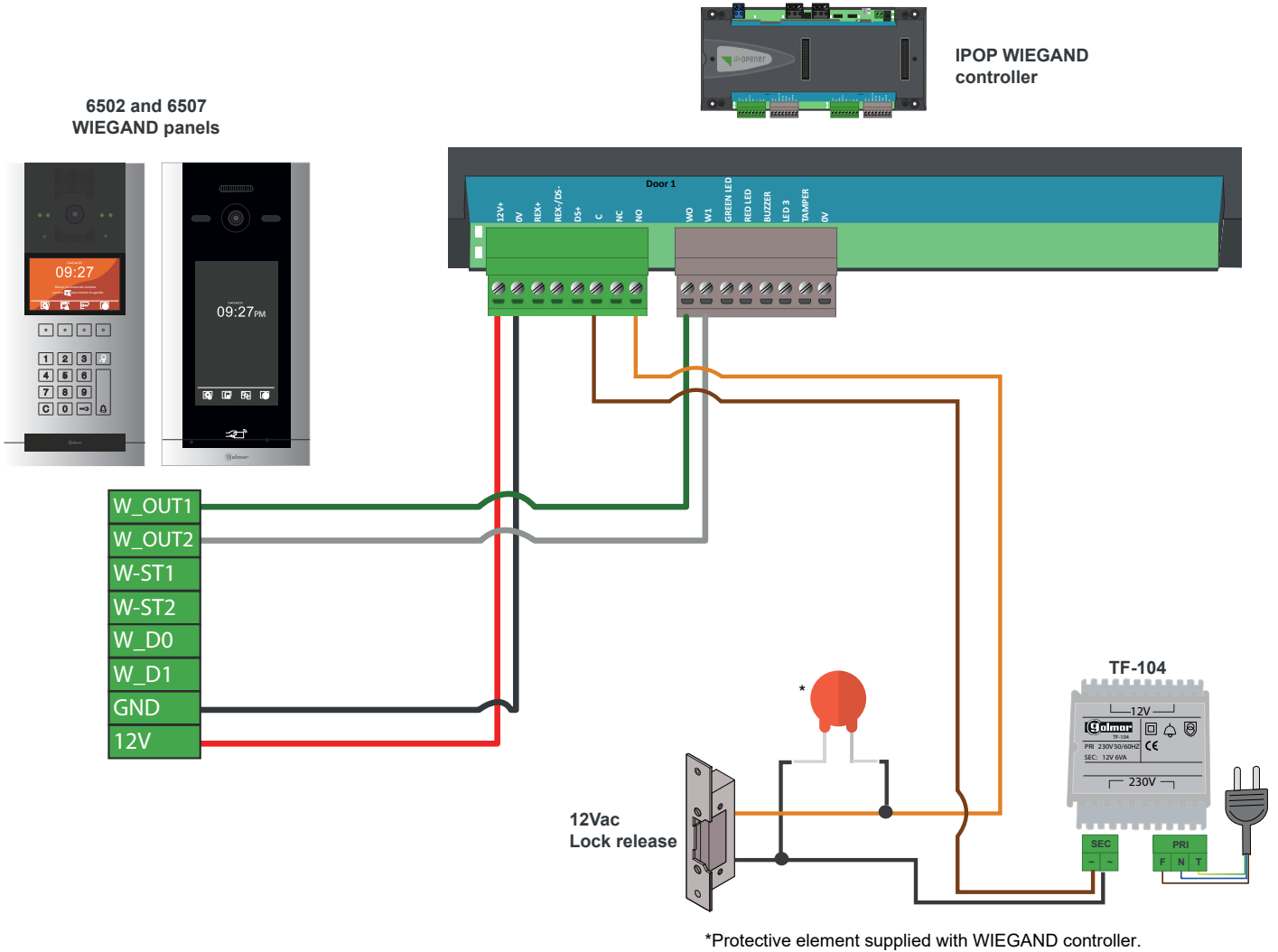


- TX_OUT
- RX_OUT
- GND
- R+/D+
- R-/D-
- 485-B
- 485-A
- GND

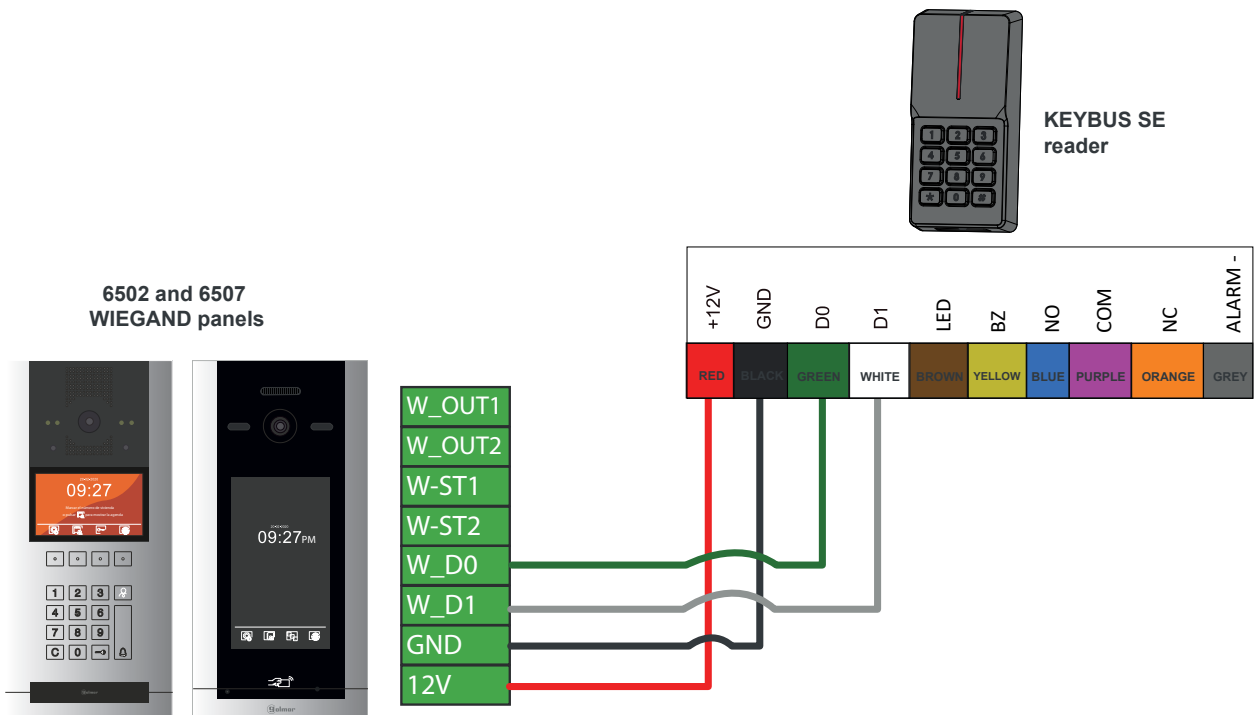


*Protective element supplied with 2SAFE reader.

6502 and 6507 Wiegand panel connection



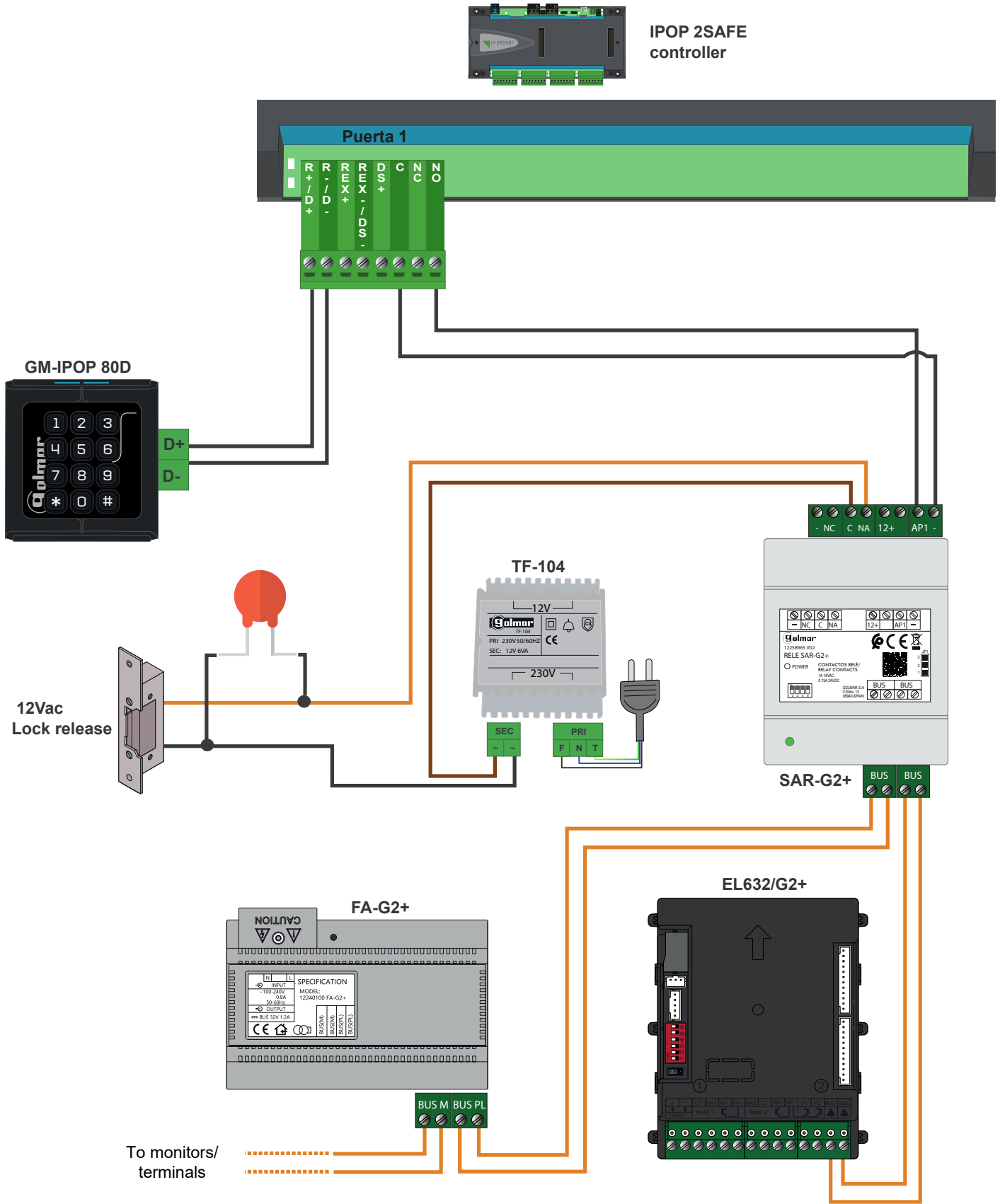
NOTE: The 6502 and 6507 panels in standalone operation (without controller) can manage a slave reader:



For more detailed information see the Intercom panel manual.

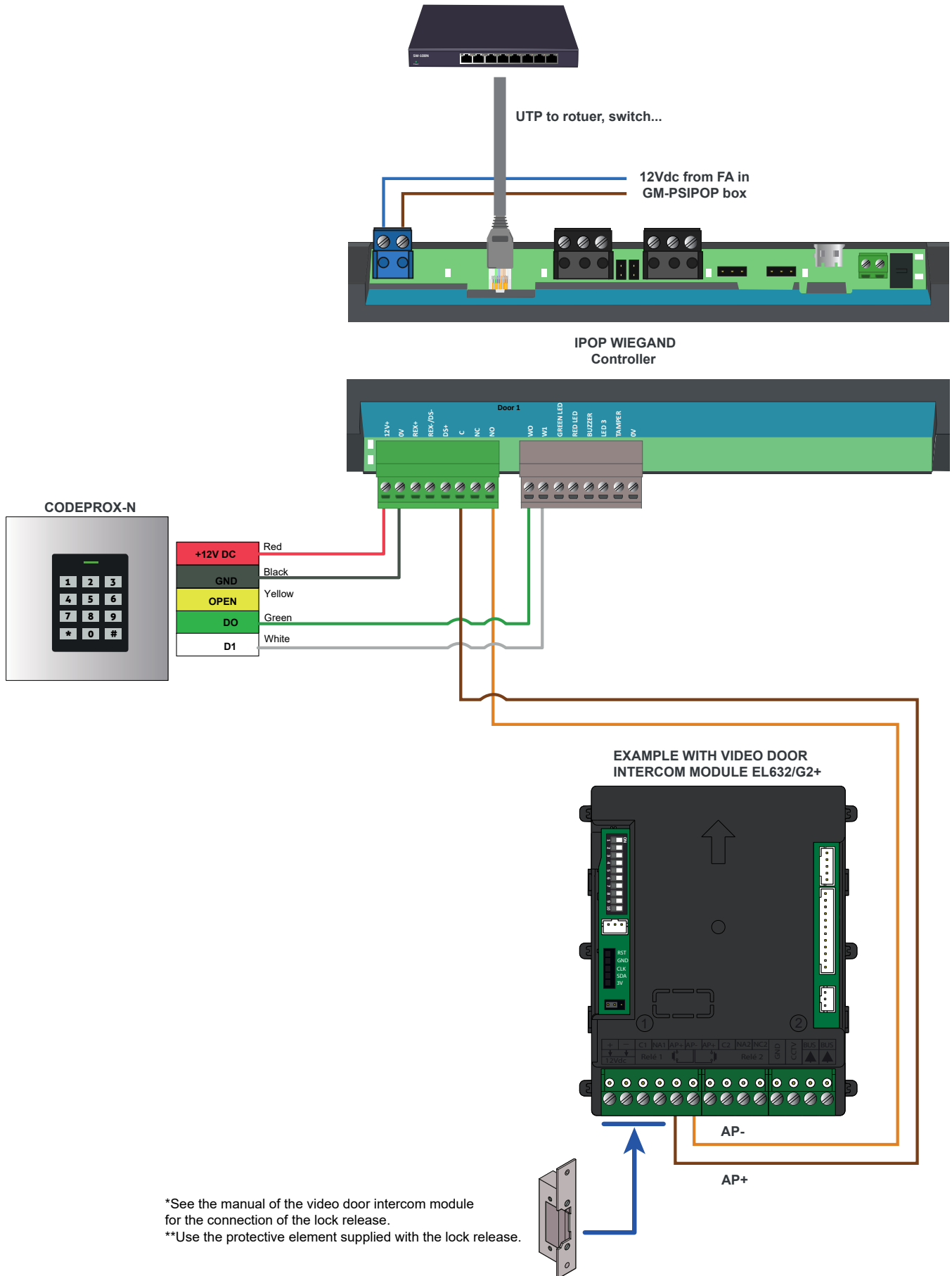
SAR-G2+ relay connection

The SAR-G2+ relay (as well as the SAR-G+) allows remote activation of the lock. This solution is interesting among other things for the fact that the element that performs the opening (SAR-G2+ or SAR-G+ relay) can be located in a different location from the video door entry panel, avoiding any possible tampering and unwanted opening.



iP Opener Wiegand system connection with video door entry system - Option A

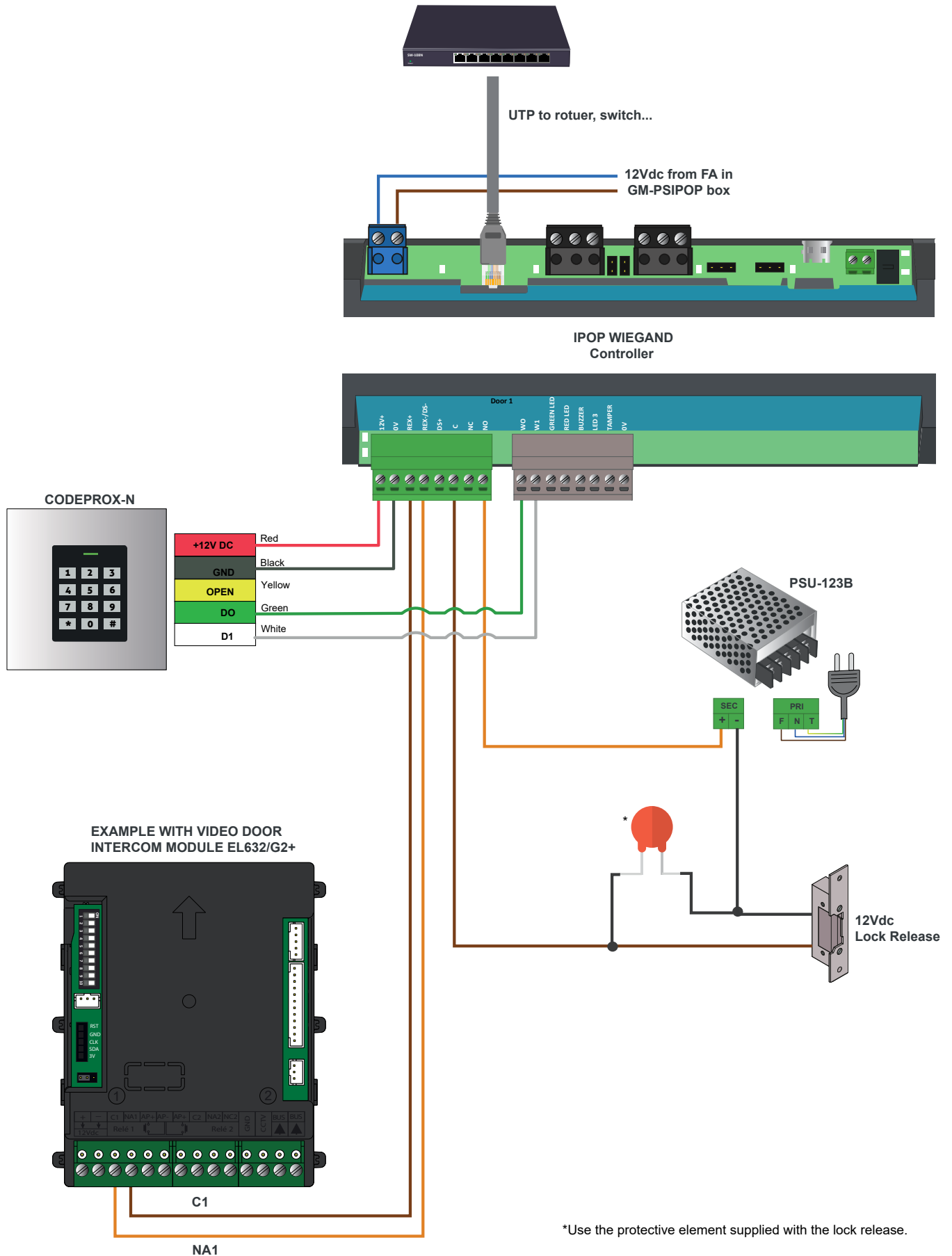
In this connection the door opener is connected to the video door intercom control module, any activation (either from a system monitor or access control reader) will emit the corresponding messages to the voice synthesis.



*See the manual of the video door intercom module for the connection of the lock release.
 **Use the protective element supplied with the lock release.

iP O opener Wiegand system connection with video door entry system - Option B

In this other connection option, the lock release is connected to the controller, so the voice synthesis will exist when the opening is done via the video door intercom monitor and not when the opening is done through the credential validation in the reader.





iP-OPENER



C/ Silici 13. Poligon Industrial Famadas
08940 – Cornellà del Llobregat – Spain
golmar@golmar.es
Tel: 93 480 06 96
www.golmar-seguridad.es



Golmar deserves the right for any modification without prior notice.