# ESTUDIO DEL FUNCIONAMIENTO DE UN PLC

## INTRODUCCIÓN

El PLC, o Controlador Lógico Programable, se encarga de controlar y supervisar el funcionamiento de maquinarias y procesos, lo que lo convierte en una herramienta fundamental para la eficiencia y seguridad en la producción industrial. Es un dispositivo electrónico utilizado en la automatización industrial para controlar y monitorear procesos en tiempo real. Su función principal es recibir información de los sensores y actuadores, procesarla y enviar señales de control a los actuadores para que realicen las acciones necesarias.

## ARQUITECTURA

El PLC consta de:

* Una unidad procesadora (CPU) que interpreta las entradas, ejecuta el programa de control almacenado en la memoria y envía señales de salida.
* Una fuente de alimentación que convierte la tensión alterna en continua.
* Una unidad de memoria que almacena los datos de las entradas y el programa que debe ejecutar el procesador.
* Módulos de entrada y salida, en la que el controlador recibe y envía datos desde/hacia dispositivos externos.
* Una interfaz de comunicaciones para recibir y transmitir datos en redes de comunicación desde/hacia PLC remotos.

Los PLC requieren un dispositivo de programación que se utiliza para desarrollar y posteriormente descargar el programa creado en la memoria del controlador

Nuestro PLC es modular y ofrece espacio para módulos con distintas funciones, como la fuente de alimentación, el procesador, la selección de módulos de E/S y las interfaces de comunicación, que pueden personalizarse para cada aplicación concreta.

Las señales discretas (digitales) sólo pueden tener valor de encendido o apagado (1 o 0, verdadero o falso).

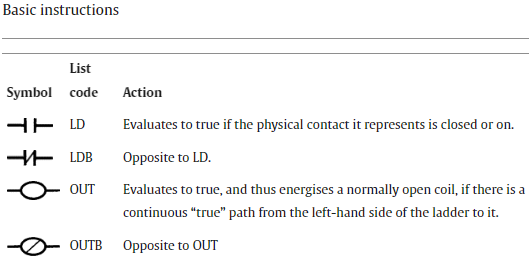
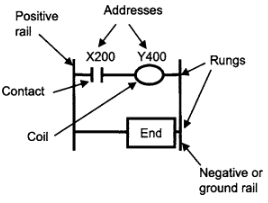
Las señales analógicas pueden utilizar voltaje o corriente proporcional al tamaño de la variable monitorizada y pueden tomar cualquier valor dentro de su escala. La presión, la temperatura, el caudal y el peso suelen representarse mediante señales analógicas. El PLC tomará este valor y lo transpondrá a las unidades deseadas del proceso para que el operador o el programa puedan leerlo.

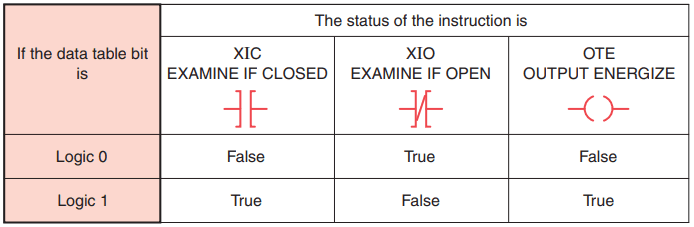
## LENGUAJES DE PROGRAMACIÓN

La programación de un PLC se realiza mediante un software específico que permite la creación de programas lógicos en lenguajes de programación. Una vez programado, el PLC puede funcionar de forma autónoma, sin necesidad de una supervisión constante. Para ello, se utilizan las siguientes técnicas:

### LÓGICA LADDER

Es el lenguaje más utilizado y consiste en una estructura de escalera por donde todo funciona a partir de dos carriles verticales, uno izquierdo (L1), el que recibe el voltaje (entrada) y deja pasar la energía al riel derecho (L2) que actúa como tierra (salida). Su lectura siempre sigue el mismo patrón, de izquierda a derecha y de arriba hacia abajo. En su interior se colocan los símbolos de contactos, relés, funciones de bloque y operaciones lógicas.





Más detallado en: <https://www.tud.ttu.ee/im/Andres.Rahni/Automaatika%20alused/77511_05_LAD_and_FBD.pdf>

### DIAGRAMAS DE BLOQUE DE FUNCIONES (SFD)

Todas las funciones se colocan en bloques de funciones. Todos tienen una o más entradas y salidas. El bloque de función se ilustra con un recuadro. En el centro del recuadro suele haber un símbolo o un texto. Este símbolo representa la funcionalidad real del bloque de función. Dependiendo de la función, puede haber un número indefinido de entradas y salidas. Se puede conectar la salida de un bloque de función a la entrada de otro. De este modo se crea un diagrama de bloques de función.

Existen muchos bloques de función estándar, pero también se pueden crear bloques de función propios. Por ejemplo, a veces habrá que usar el mismo fragmento varias veces en el programa y para ello se pueden crear bloques de función específicos y utilizarlos varias veces.

Visión general de los bloques más importantes:

<https://www.plcacademy.com/function-block-diagram-programming/?utm_content=cmp-true>

* Operaciones Lógicas (OR, AND, NOR, NAND, XOR)
* Operación de asignación (=)
* Set/Reset o Reset/Set
* Timer: TP, TON, TOF
* Counter: CTU (Up counter), CTD (Down counter), CTUD (Up Down counter)
* Edge detection: R\_Trig (Rising edge), F\_Trig (Falling edge)
* Equality, inequality, less than, greater than
* …

### DIAGRAMAS DE FUNCIONES SECUENCIALES (SFC)

Es una representación de secuencias de control en un programa en el que se pueden organizar subrutinas o etapas que van afectando el producto de las funciones posteriores. La energía fluye de un punto a otro siempre y cuando se haya cumplido una condición. Este lenguaje proviene del estándar GRAFCET que también utiliza etapas, transiciones y acciones para su funcionamiento.

Las secuencias SFC se representan por cajas rectangulares que contienen las etapas que están conectadas por líneas verticales llamadas transiciones, por último están las condiciones (verdadero o falso) que desbloquean la acción para seguir con las funciones siguientes.

## CX-PROGRAMMER

## SISTEMAS SCADA

## APLICACIONES EN CIBERSEGURIDAD

## SOBRE EL PLC FÍSICO DEL LABORATORIO

**OMRON SYSMAC CJ2M CPU31 PROGRAMMABLE CONTROLLER:**

<https://assets.omron.eu/downloads/latest/datasheet/en/p059_cj2-series_programmable_controller_datasheet_en.pdf?v=7>

| **Program capacity** | 25K steps (creo que es 5K) |
| --- | --- |
| **Data memory capacity** | 64 K words |
| **Logic execution time** | 0.04 µs |
| **Max. number of expansion units** | 40 |
| **Max. number of local I/O points** | 2560 |
| **Number of built-in digital I/Os** | 0 |
| **Communication port(s)** | EtherNet/IP, Ethernet TCP/IP, USB |

**CJ1W-PA202 / CJ2M CPU31 / CJ1W-PRM21 / CJ1W-ID211 / CJ1W-OD212 / CJ1W-MAD42**

### CARACTERÍSTICAS

**OMRON SYSMAC CJ2M CPU31 PROGRAMMABLE CONTROLLER:**

**CJ1W-PA202:** Fuente de alimentación 100 a 240Vca 5Vcc 2,8A Relé

<https://industrial.omron.es/es/products/CJ1W-PA202>

| **Type of module** | Power supply |
| --- | --- |
| **Type of voltage (input voltage)** | AC |
| **Power output** | 14 W |
| **Input voltage at AC 50 Hz** | 85-264 V |

**CJ1W-PRM21:** Módulo maestro Profibus DP

<https://industrial.omron.es/es/products/CJ1W-PRM21>

| **I/O system** | CJ I/O Bus |
| --- | --- |
| **Expansion unit type** | CPU Bus Unit |
| **Type of module** | Communication |
| **IO-Link master** | No |
| **Communication port(s)** | PROFIBUS DP Master |
| **Interfaz Profibus** | Conector sub D hembra de 9 patillas  equivalente al puerto RS-232C |

**CJ1W-ID211:** Basic I/O Units (Input Units)

<https://industrial.omron.es/es/products/CJ1W-ID211>

<https://assets.omron.eu/downloads/latest/datasheet/en/cj1w-id_ia_datasheet_en.pdf?v=6>

| **I/O system** | CJ I/O Bus |
| --- | --- |
| **Expansion unit type** | Basic I/O Unit |
| **Type of module** | Digital I/O |
| **Number of digital inputs** | 16 |
| **Digital input type** | PNP/NPN |
| **Permitted voltage at input** | 20.4-26.4 V |
| **OFF/ON delay** | 0-32 ms |
| **Number of digital outputs** | 0 |
| **I/O connection type** | Screw |

**CJ1W-OD212:** Módulo 16 Salidas PNP Term.

<https://industrial.omron.es/es/products/CJ1W-OD212>

<https://assets.omron.eu/downloads/latest/datasheet/en/cj1w-oc_oa_od_datasheet_en.pdf?v=6>

| **I/O system** | CJ I/O Bus |
| --- | --- |
| **Expansion unit type** | Basic I/O Unit |
| **Type of module** | Digital I/O |
| **Number of digital inputs** | 0 |
| **OFF/ON delay** | 0-32 ms |
| **Number of digital outputs** | 16 |
| **Digital output type** | PNP |
| **Permitted voltage at output** | 20.4-26.4 V |
| **Output current** | 0.5 A |
| **Short-circuit protected outputs** | SI |
| **I/O connection type** | Screw |
| **Number of I/O connectors** | 1 |
| **Detachable I/O connector** | SI |
| **Suitable for safety functions** | NO |
| **Number of IOV (V+) terminals** | 1 |
| **Number of IOG (V-) terminals** | 1 |
| **Number of COM terminals** | 0 |

**CJ1W-MAD42:** Módulo analógico mixto 4 entradas, 2 salidas

<https://industrial.omron.es/es/products/CJ1W-MAD42>

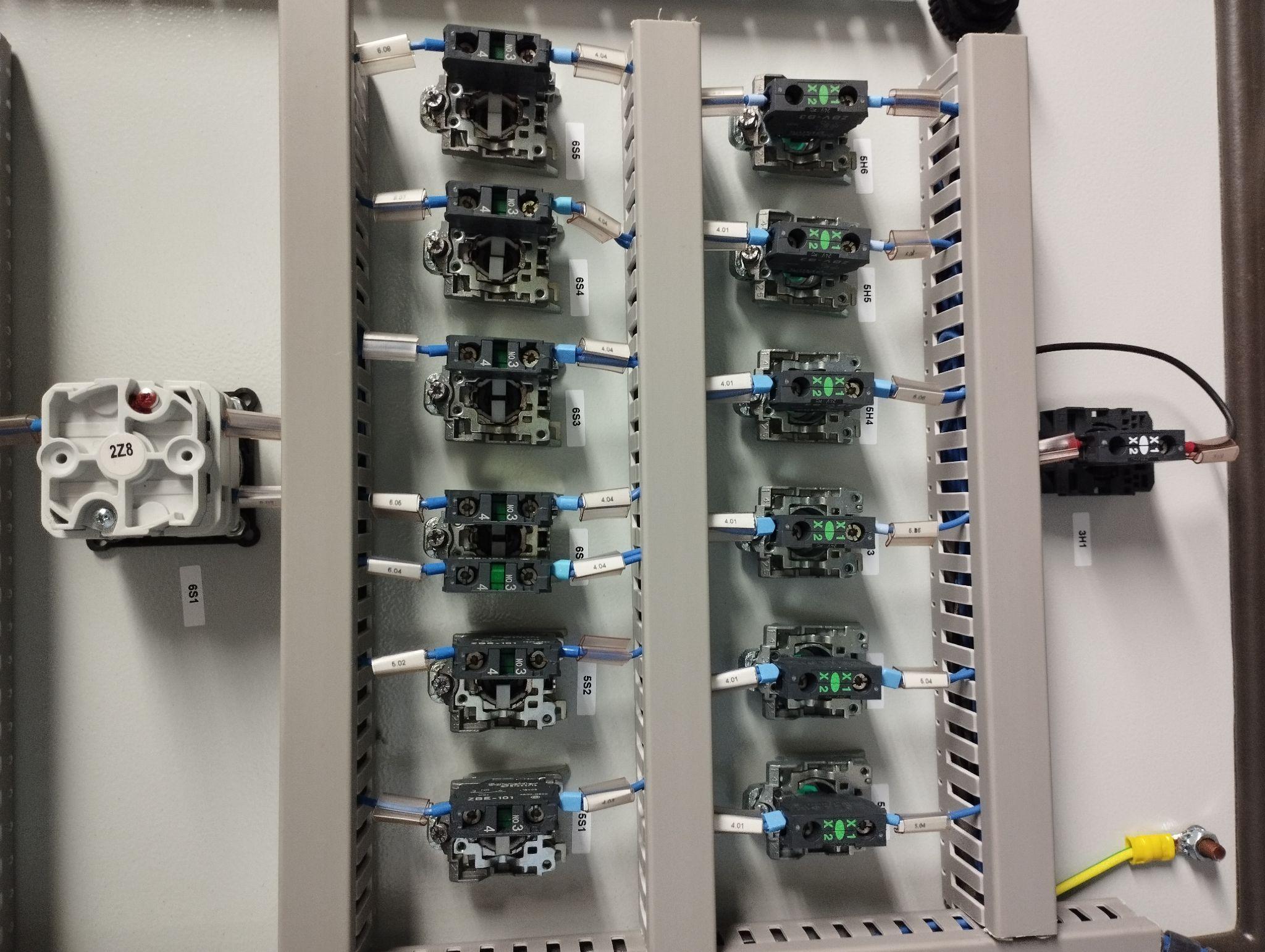
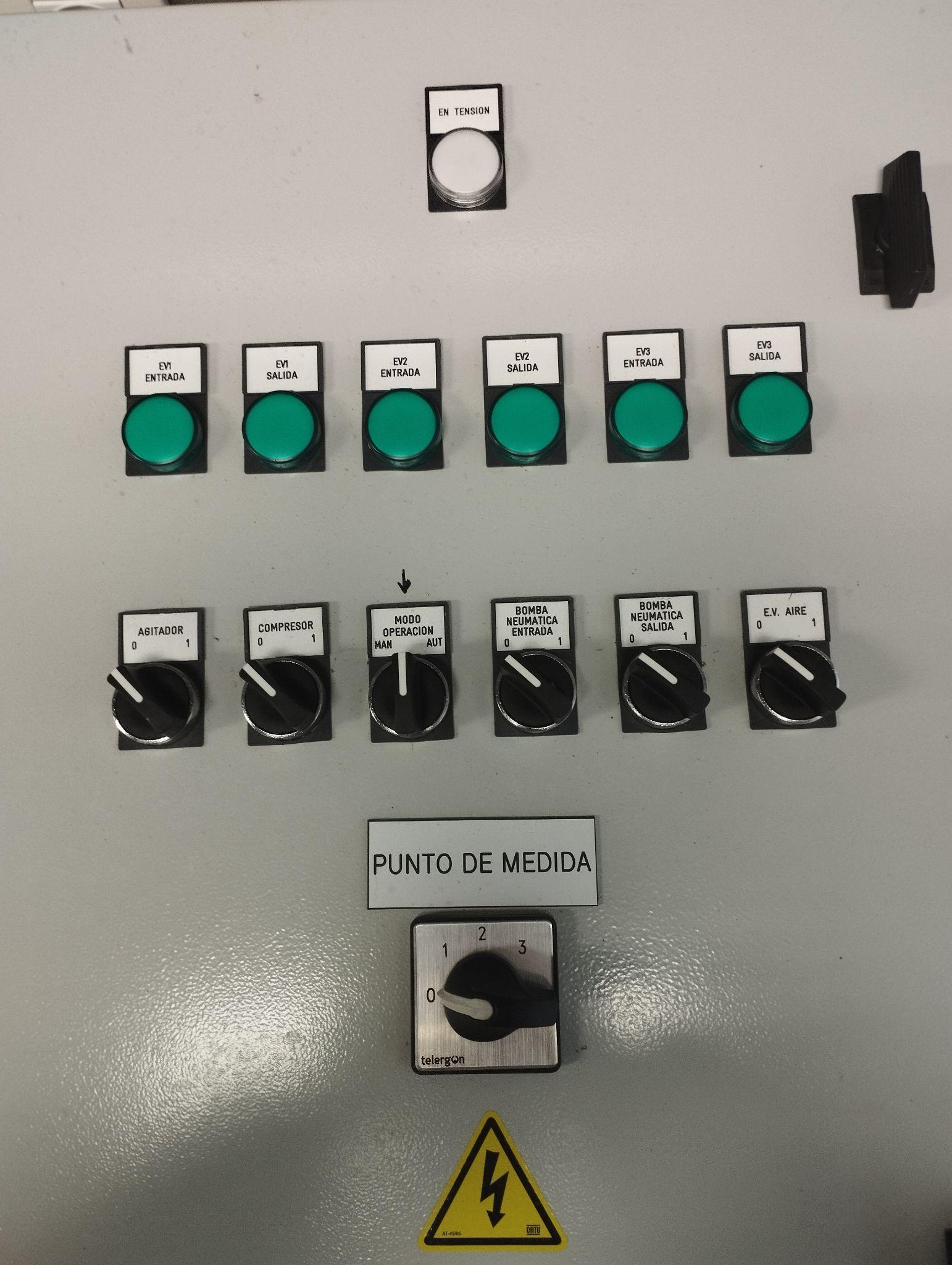
| **I/O system** | CJ I/O Bus |
| --- | --- |
| **Expansion unit type** | Special I/O Unit |
| **Type of module** | Analog I/O |
| **Number of analog inputs** | 4 |
| **Linear analog input type** | -10 to 10 V, 0 to 10 V, 0 to 5 V, 1 to 5 V, 4 to 20 mA |
| **Resolution of the analog inputs** | 13 Bit |
| **Number of analog outputs** | 2 |
| **Linear analog output type** | -10 to 10 V, 0 to 10 V, 0 to 5 V, 1 to 5 V, 4 to 20 mA |
| **Resolution of the analog outputs** | 13 Bit |
| **Conversion time** | 4000 ms/unit |
| **I/O connection type** | Screw |
| **Number of I/O connectors** | 1 |
| **Detachable I/O connector** | Si |

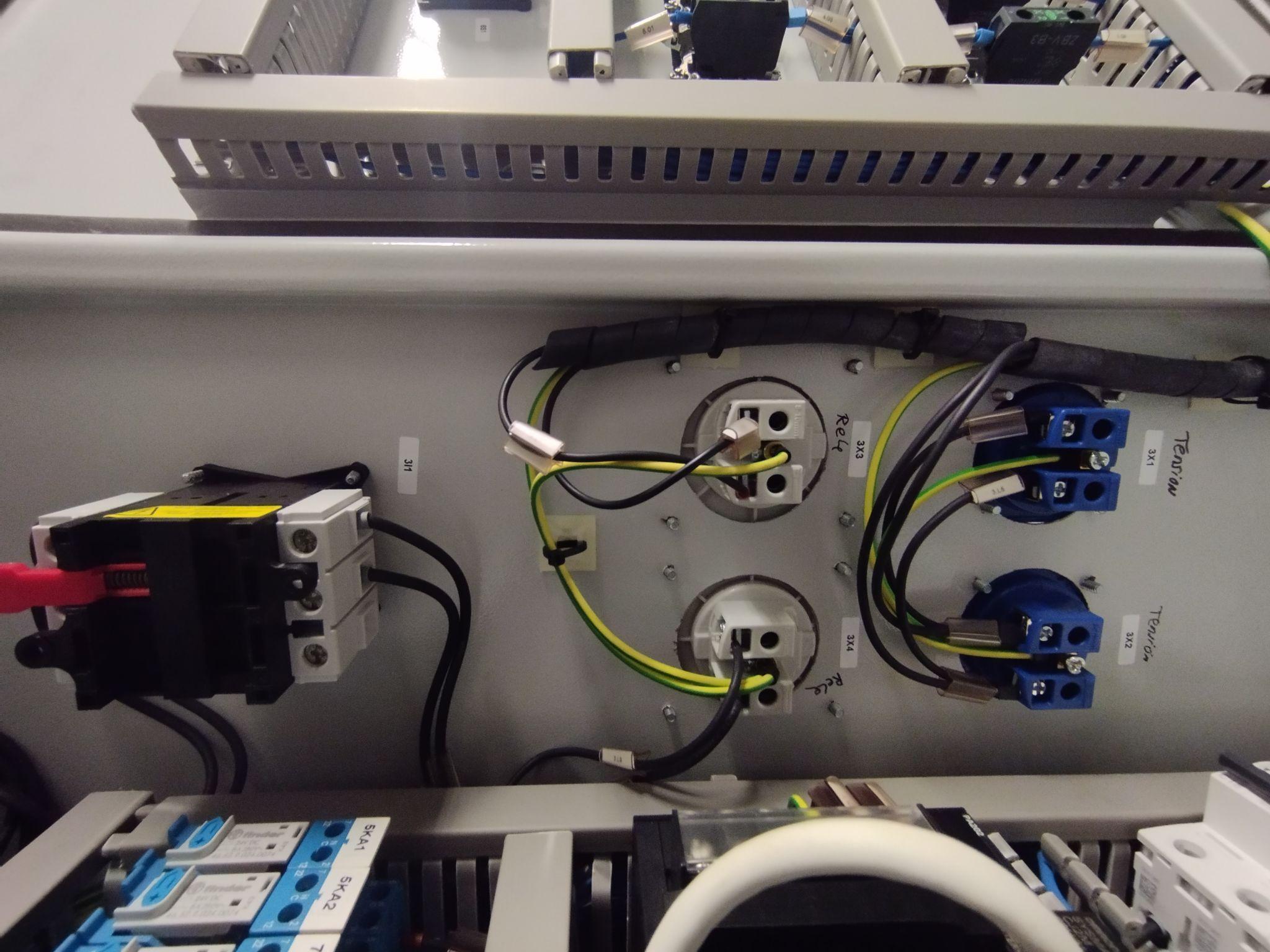
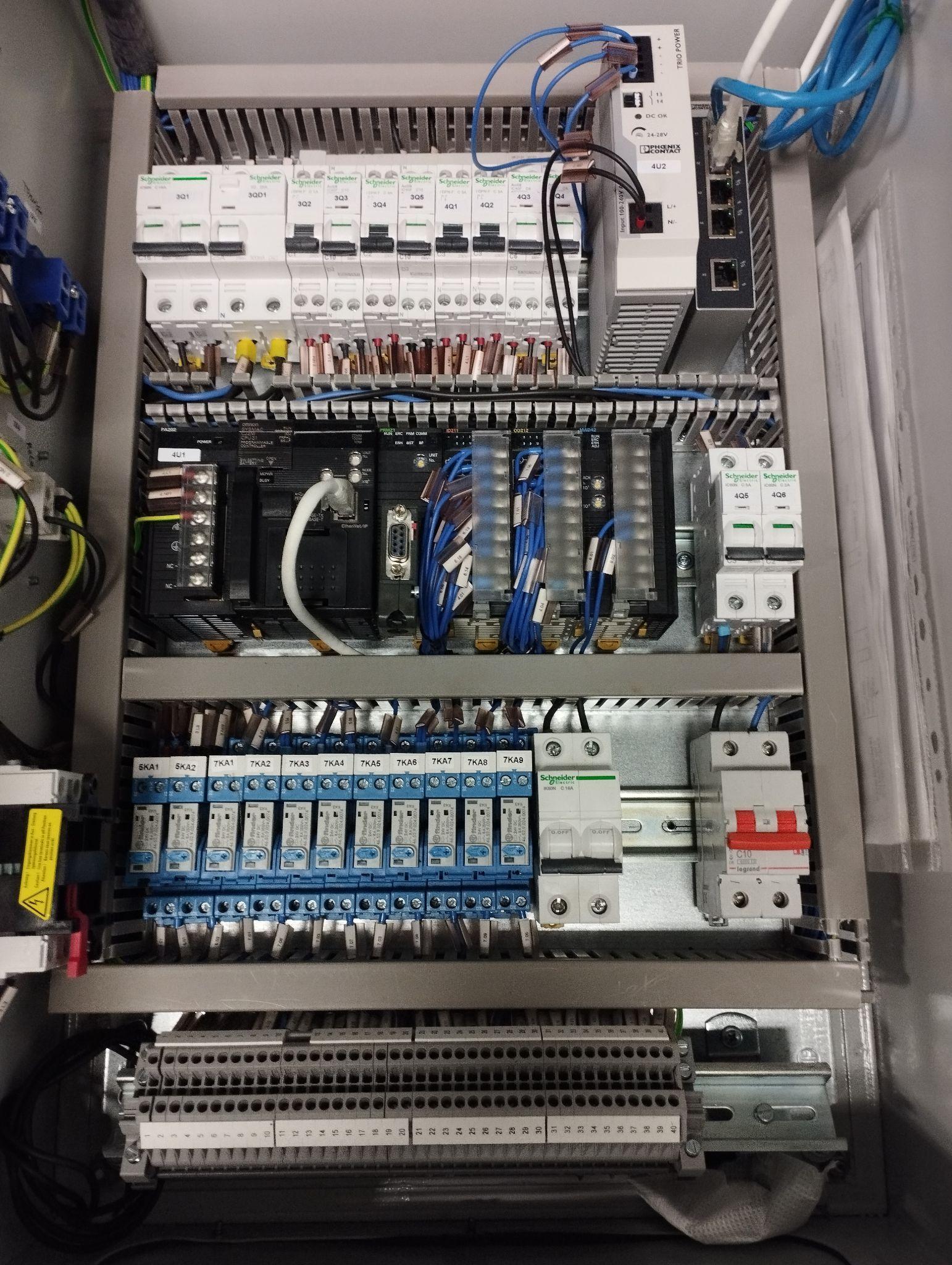
**TIPO DE PROGRAMACIÓN**

Por ahora entiendo que usaré CX-programmer por ser el que previamente he usado, es conocido por mucha gente y es creado por OMRON que es el fabricante también del PLC que usaremos.

# RECONOCIMIENTO DEL CUADRO ELECTRÓNICO

## IMAGEN GENERAL

****

****

## EXPLICACIÓN DE CADA APARATO

**Simbología:**

H → Dispositivos de señalización X → Bornas de conexión

KA → Contactos auxiliares S → Dispositivos de mando

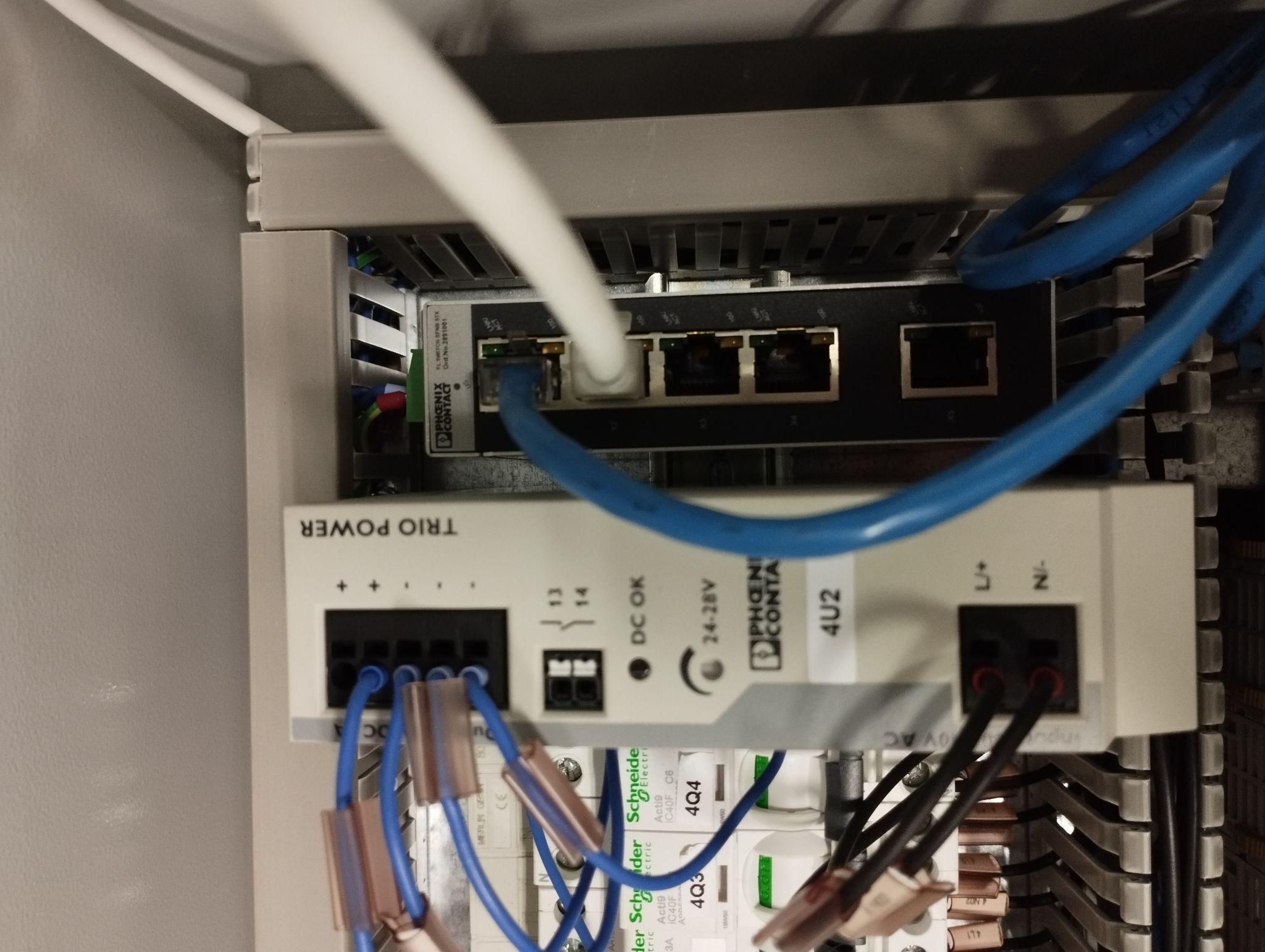
Q → Interruptores de potencia

U → Convertidores (AC/DC)

Puente de Graetz o puente rectificador de doble onda con 4 diodos.

**Explicación:**

**Interruptores automáticos, fuente de alimentación conmutada y switch:**

****

**3Q1, 4Q5, 4Q6:** iC60N C 16A: es un interruptor automático en miniatura (MCB) de baja tensión con dos polos. Protege los circuitos contra cortocircuitos y sobrecargas. 16A significa su corriente nominal.

**3QD1:** iID: Es un interruptor diferencial. Protege contra descargas eléctricas por contacto directo o indirecto y peligros de incendios. Realiza la función de desconexión de circuitos eléctricos en caso de fallo a tierra.

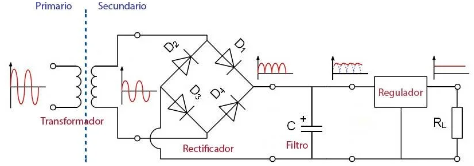
**3Q2, 3Q4, 4Q1, 4Q2:** iDPN:interruptor automático en miniatura

**3Q3, 3Q5, 4Q3, 4Q4:** iC40F: Este interruptor en miniatura combina funciones de protección de circuitos contra cortocircuito y sobrecarga de corriente, control y aislamiento

**4U2:** TRIO-PS-2G/1AC/24DC/5: Fuente de alimentación conmutada en primario. Entrada: monofásica, salida: 24 V DC/5 A.

Puente de Graetz o puente rectificador de doble onda con 4 diodos:

Se usa cuando se necesita convertir la corriente alterna (AC) en corriente continua (DC).



En principio, entiendo que será así.

Datos de entrada:

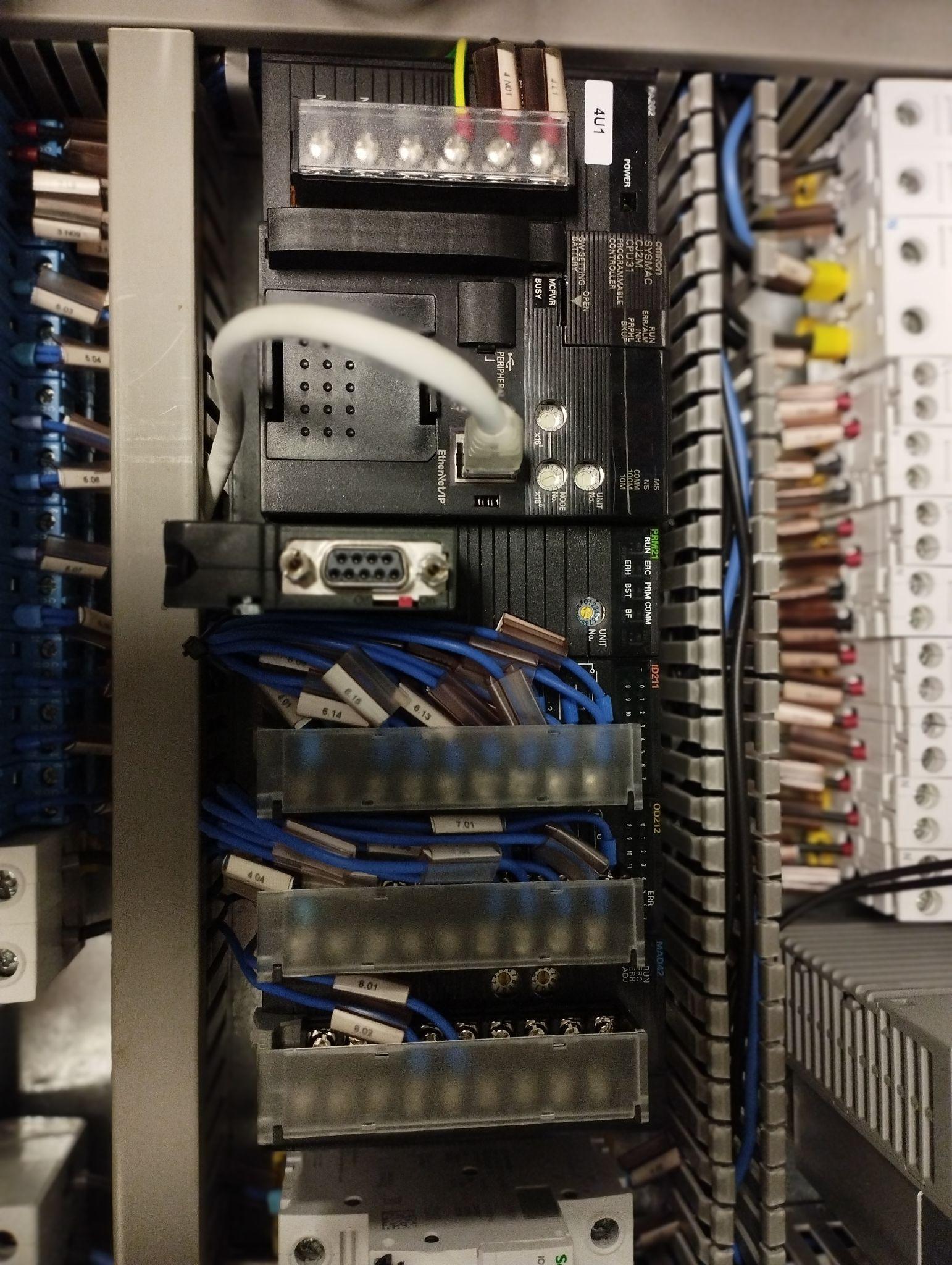
* Funcionamiento en AC:
  + Estructura de la red → en estrella
  + Margen de tensión nominal → 100V AC … 240V AC
  + Rango de tensión → 100V AC … 240V AC -15%... +10%
  + Margen de tensión → 85V AC … 264V AC
  + Tensión de red típica del país → 120V AC / 230V AC
  + Tipo de tensión de la alimentación → AC/DC
* Funcionamiento en DC:
  + Margen de tensión nominal → 110V DC … 250V DC
  + Rango de tensión → 99V DC … 275V DC
  + Tensión de funcionamiento → ≥ 88 V DC
  + Tensión de desconexión → < 60 V DC
  + Tipo de tensión de la alimentación → AC/DC

Datos de salida:

* + Rendimiento → > 90 % (con 230 V AC y valores nominales)
  + Tensión nominal → 24 V DC ±1 %
  + Corriente nominal → 5A
  + Posibilidad de conexión en paralelo para redundancia y aumento de potencia
  + Posibilidad de conexión en serie

**Phoenix contact FL Switch SFNB 5TX:** Red Interruptor - sin administrar 5 puertos IP20

**PLC (OMROM SYSMAC CJ2M CPU31) :**

****

**CJ1W-PA202 / CJ2M CPU31 / CJ1W-PRM21 / CJ1W-ID211 / CJ1W-OD212 / CJ1W-MAD42**

* **CJ1W-PA202 (4U1):** Fuente de alimentación 100 a 240Vca 5Vcc 2,8A Relé
* **CJ1W-PRM21:** Módulo maestro Profibus DP

Es un sistema maestro. Intercambia datos de E/S e información de comunicaciones y estado con la CPU del PLC. Para configurar el dispositivo CS1W-PRM21 se puede utilizar un puerto serie de la CPU. Pero, como la configuración se realiza a través de comunicación FINS, se puede usar prácticamente cualquier punto de acceso de la red de comunicaciones existente: Controller Link, Ethernet, intercambia datos y comandos con las estaciones PROFIBUS-DP esclavas a través de la red PROFIBUS.

* **CJ1W-ID211:** Basic I/O Units (Input Units)

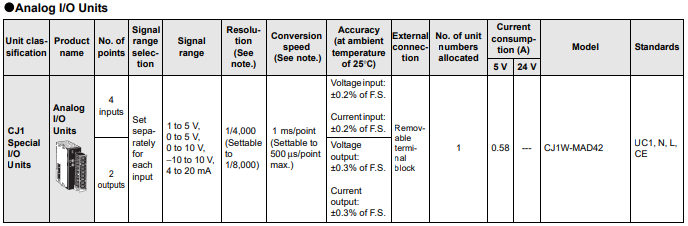
Sus unidades E/S funcionan únicamente como entrada

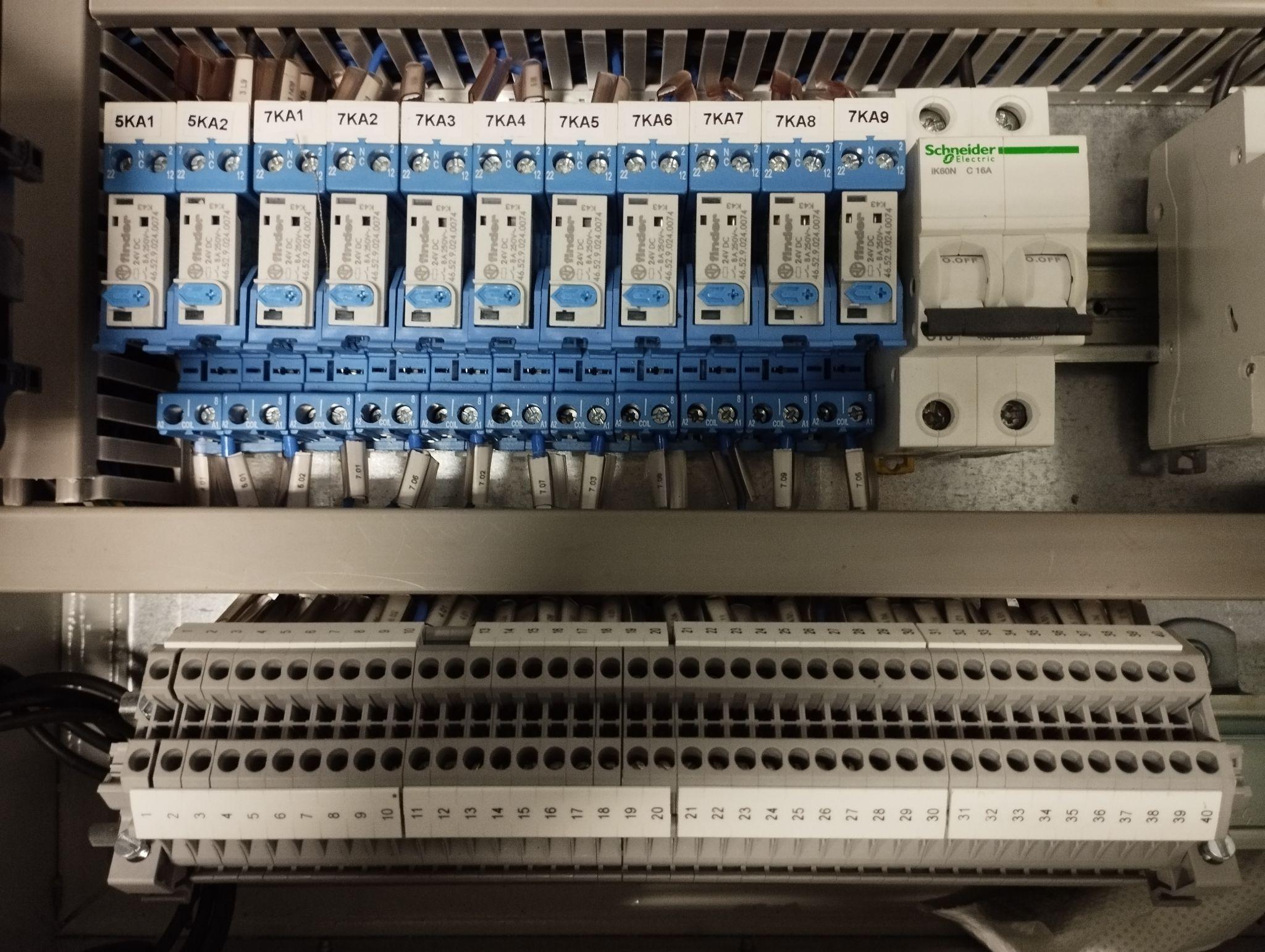
* **CJ1W-OD212:** Módulo 16 Salidas PNP Term.

Sus unidades E/S funcionan únicamente como salida

* **CJ1W-MAD42:**

4 inputs (1 to 5 V, 4 to 20 mA, etc.) 2 outputs (1 to 5 V, 4 to 20 mA, etc.)

****

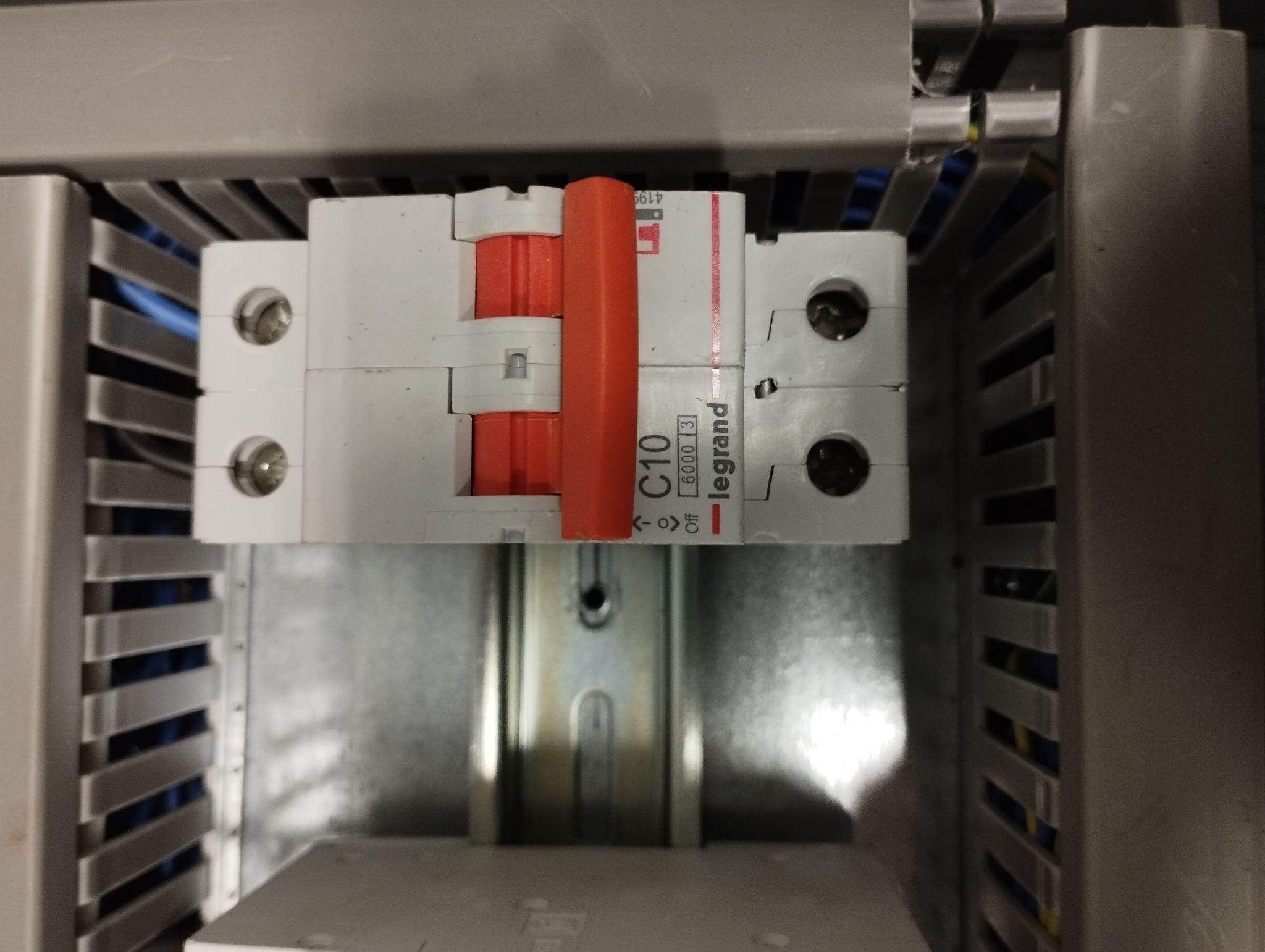
****

**46.52.9.024.0074 finder 24V DC 8A 250V**

**5KA1, 5KA2, 7KA1, …, 7KA9:** Relé electromagnéticos: La punta de plástico (situada justo debajo del botón de prueba) permanece intacta. En este caso, cuando se pulsa el botón de prueba, los contactos funcionan. Cuando se suelta el botón los contactos vuelven a su estado anterior.

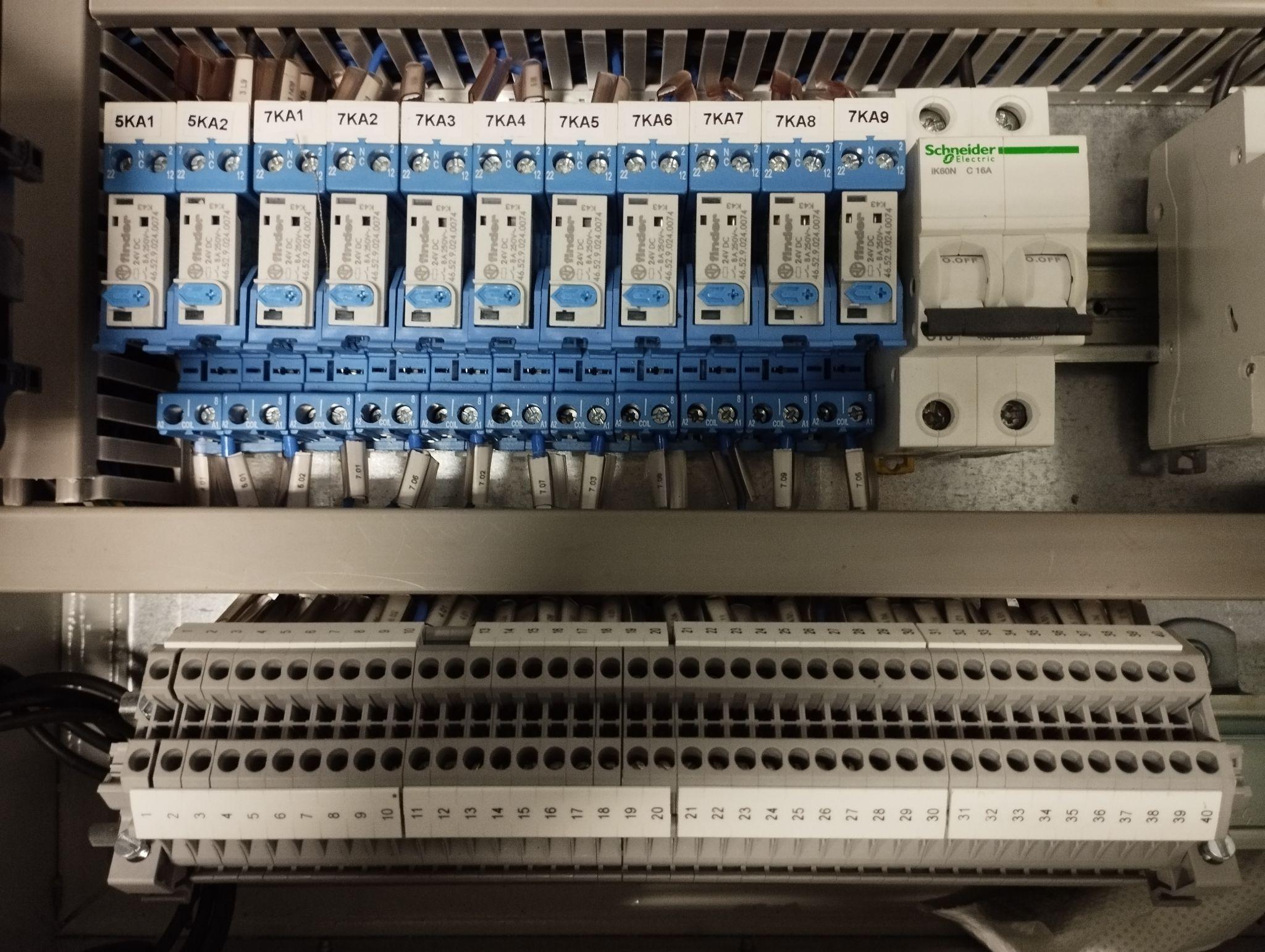
La configuración de los contactos es DPDT( Double Pole Double Throw)

Otro **Schneider:** iK60N: Este interruptor en miniatura combina funciones de protección de circuitos contra cortocircuito y sobrecarga de corriente (sin función por ahora)

****

**Magnetotérmico RX³ - 2P - 230/400 V~ - 10A - curva C**

Interruptor magnetotérmico para proteger las instalaciones eléctricas contra sobrecargas y cortocircuitos. También se puede utilizar para controlar y aislar la instalación. (sin función por ahora)

**UT 2,5 - Borne de paso:** (tipo de conexión: Conexión por tornillo)****

<https://www.phoenixcontact.com/es-es/productos/borne-de-paso-ut-25-3044076>

Borna de paso o bloques terminales: es un componente con un marco aislado que tiene el único propósito de fijar dos o más cables juntos. Los bloques de terminales ofrecen flexibilidad. Las modificaciones del cableado son sencillas porque los cables se pueden quitar o añadir rápidamente. El cableado del bloque de terminales es limpio y ordenado, lo que permite una rápida identificación y facilita las modificaciones y la localización de averías.

Método de conexión de cables utilizado: "Atornillado". Son aquellos que utilizan tornillos como método de sujeción de los cables. ¡Atención! Un apriete excesivo de los tornillos puede dañar los cables.

**Otros:**

**Circuitos de Maniobra:** Los circuitos de maniobra son los encargados de alimentar a los sensores y captadores, encargados de suministrar información en forma de señales eléctricas o digitales a los sistemas de Lógica Cableada (Contactores, relés, etc.) o Lógica Programada (Relés programables o autómatas programables). Estos circuitos son normalmente alimentados con tensiones de Muy Baja Tensión (MBT) o de Seguridad a 24V.

**Dispositivos de señalización**



En tensión (3H1) se enciende cuando activas 3Q2.

EV1 entrada(5H1)/salida(5H2) se encienden cuando el relé 7KA2 está activado.

EV2 entrada(5H3)/salida(5H4) se encienden cuando el relé 7KA4 está activado.

EV3 entrada(5H5)/salida(5H6) se encienden cuando el relé 7KA6 está activado.

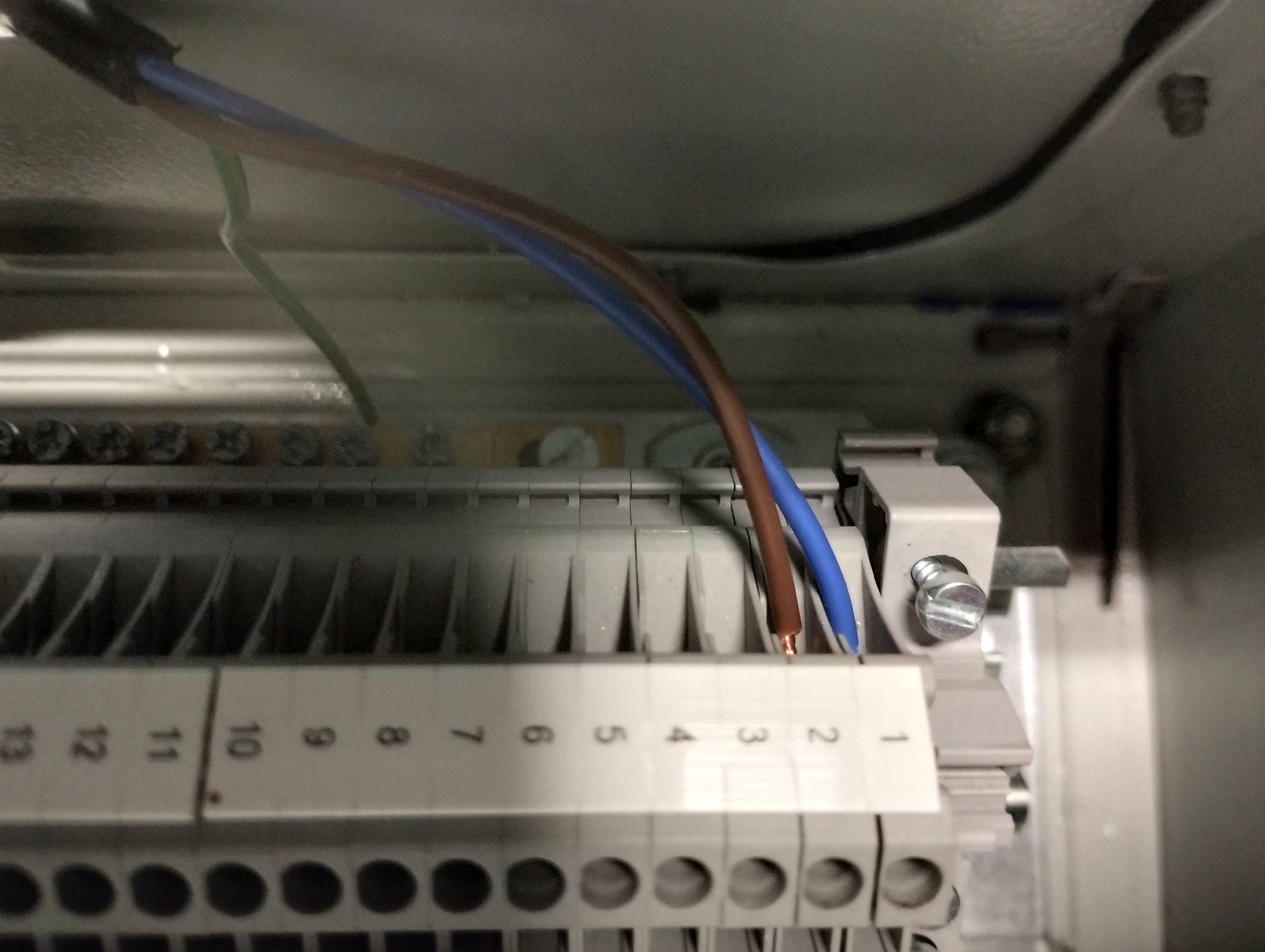
**Conexiones con el conmutador de dos o tres posiciones con el selector**



## MODO DE OPERACIÓN

1. **Alimentación del panel electrónico.**

Como se muestra en la imagen, el neutro (azul) al borne 1, la línea (marrón) al borne 2 y la tierra (verde y amarillo) a la conjuncion de tierra.



1. **Interruptores a accionar**

3Q3 → ENCHUFE AZUL (3X1) O (3X2)

5KA1 y 3Q4 → ENCHUFE GRIS (3x3) 5KA2 y 3Q5→(3X4)

3Q2 → Para encender luz de tensión (3H1) muestra presencia de la tensión

4U1 + 4Q1 → Alimentación de la CPU

4U2 + 4Q2 + 4Q5 → Alimentación maniobra

4U2 + 4Q2 + 4Q6 → Alimentación módulos PLC y switch

Es más visual en el manual

# ESTABLECIMIENTO DE CONECTIVIDAD CON PLCS VÍA RS232 - USB

## RS232 INTRODUCCIÓN

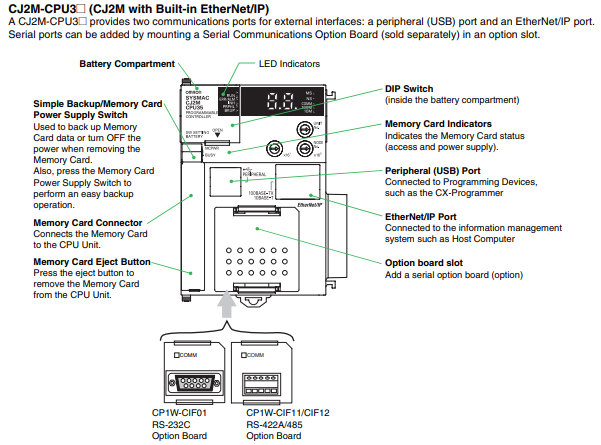
RS-232 (*Recommended Standard 232*), también conocido como [EIA](https://es.wikipedia.org/wiki/Electronic_Industries_Alliance)/[TIA](https://es.wikipedia.org/wiki/Telecommunications_Industry_Association) RS-232C, es una [interfaz](https://es.wikipedia.org/wiki/Interfaz_(electr%C3%B3nica)) que designa una [norma](https://es.wikipedia.org/wiki/Norma_(tecnolog%C3%ADa)) para el intercambio de [datos](https://es.wikipedia.org/wiki/Dato) [binarios](https://es.wikipedia.org/wiki/Binario) serie entre un [DTE](https://es.wikipedia.org/wiki/ETD) (*Data Terminal Equipment*, "Equipo [Terminal](https://es.wikipedia.org/wiki/Terminal_de_computadora) de Datos"), como por ejemplo una [computadora](https://es.wikipedia.org/wiki/Computadora), y un [DCE](https://es.wikipedia.org/wiki/ETCD) (*Data Communication Equipment*, "Equipo de Comunicación de Datos"), por ejemplo un [módem](https://es.wikipedia.org/wiki/M%C3%B3dem).

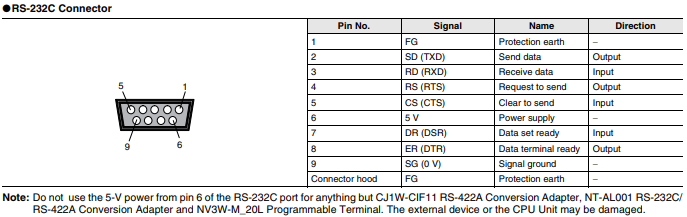
La interfaz RS-232 está diseñada para imprimir documentos para distancias cortas, de hasta 15 metros según la norma , y para velocidades de comunicación bajas, de no más de 20 [kbps](https://es.wikipedia.org/wiki/Kbps). A pesar de esto, muchas veces se utiliza a mayores velocidades con un resultado aceptable. La interfaz puede trabajar en comunicación [asíncrona](https://es.wikipedia.org/wiki/Transmisi%C3%B3n_as%C3%ADncrona) o [síncrona](https://es.wikipedia.org/wiki/Transmisi%C3%B3n_s%C3%ADncrona) y tipos de canal *simplex*, *half duplex* o *full duplex*. En un canal *simplex* los datos siempre viajarán en una dirección, por ejemplo desde DCE a DTE. En un canal *half duplex*, los datos pueden viajar en una u otra dirección, pero solo durante un determinado periodo de tiempo; luego la línea debe ser conmutada antes que los datos puedan viajar en la otra dirección. En un canal *full duplex*, los datos pueden viajar en ambos sentidos simultáneamente. Las líneas de *handshaking* de la RS-232 se usan para resolver los problemas asociados con este modo de operación, tal como en qué dirección los datos deben viajar en un instante determinado.

Si un dispositivo de los que están conectados a una interfaz RS-232 procesa los datos a una velocidad menor de la que los recibe deben de conectarse las líneas *handshaking* que permiten realizar un control de flujo tal que al dispositivo más lento le de tiempo de procesar la información. Las líneas de *hand shaking* que permiten hacer este control de flujo son las líneas RTS y CTS.

## CONEXIÓN CON PLC CJ2M-CPU32

El CJ2M-CPU31 no tiene puerto RS-232 incorporado, pero tiene una ranura opcional para la comunicación en serie. La referencia para la tarjeta opcional RS-232C es CP1W-CIF01:





De todas formas, en nuestro caso tenemos un módulo maestro con puerto RS-232 incorporado.