



Allen-Bradley

by ROCKWELL AUTOMATION

Use of standard outputs in safety loops of PLC-based control systems

Table of contents

- 1. About this paper**
- 2. Grouping and zoning**
- 3. Fault exclusion**
- 4. Zoning when using contactors**
- 5. Zoning when using distributed outputs**
- 6. Verification, documentation and PL-Calculation**
- 7. Which type of standard outputs can be used**
- 8. Wiring example**

1. About this paper

This document describes how to use standard outputs in safety circuits and which standard outputs fulfill the requirements for such an application.

These standard outputs are used in safety circuits, but they do not fulfill any safety-related function.

Further this document describes how to verify, document and consider this in the Performance Level calculation.

IMPORTANT:

These standard outputs do not switch off safely. The safety function will be supplied by other safety-related products.

Due to the statements inside the standards and technical reports, we focus on examples with fault exclusion to be limited to PLd. Looking deeper into TR 62061, 7.2.2.3, PLe is not impossible in junction with fault exclusion, but it is not typical to rely upon fault exclusions alone to achieve this level of performance. Therefore, it is essential that the designer takes additional care in the use of fault exclusions as PL or SIL increases, but this out of the scope of this document.

2. Grouping and zoning

To avoid high numbers of safety devices in a system and to simplify validation of the safety system, it is possible to group safety actuators together. You can combine a group of outputs and shut them down safely as one group. For example, you can safely shut down a power-supply to a group of outputs controlling several actuators.

This technique also allows the use of standard output devices with special features e.g., fast outputs or outputs with high output current.

3. Design consideration and fault exclusion

To achieve the required PL (PL_r) of your safety function, you have options by using different categories (B, 1 to 4) as well as MTTF_D, DC and other values. These categories have requirements like zero- or one-fault tolerance. Therefore, you have to consider each failure that theoretically can happen. If one failure occurs and you are not able to stop the hazard, consider zero-failure tolerance. If you still can stop the machine safely with one failure occurring, consider single failure tolerance.

Sometimes failures could possibly and theoretically happen but looking deeper into the technique these failures seem almost to be impossible. These failures may be excluded. ISO 13849-1 describes this approach, which is called fault exclusion.

Faults may be excluded based on

- the technical improbability of occurrence of some faults,
- generally accepted technical experience, independent of the considered application, and
- technical requirements related to the application and the specific hazard.

If you perform a fault exclusion, you should record this in your technical documents with a detailed justification.

A long list of allowed and forbidden fault exclusions is published in annexes of ISO 13849-2.

According to the technical report IEC/TR 62061-1 (chapter 7.2.2.3), it is not typical to rely upon fault exclusions alone to achieve PLe or SIL 3. Therefore, safety functions with fault exclusions are normally, but not necessarily, limited to PLd.

For more details on fault exclusion, please see ISO 13849-1 and -2.

4. Zoning when using contactors

To understand grouping and fault exclusion let us have a look to switching off motors by using contactors.

Safe switching off from 3 motors can be done by using a conventional method with 2 contactors for each single motor:

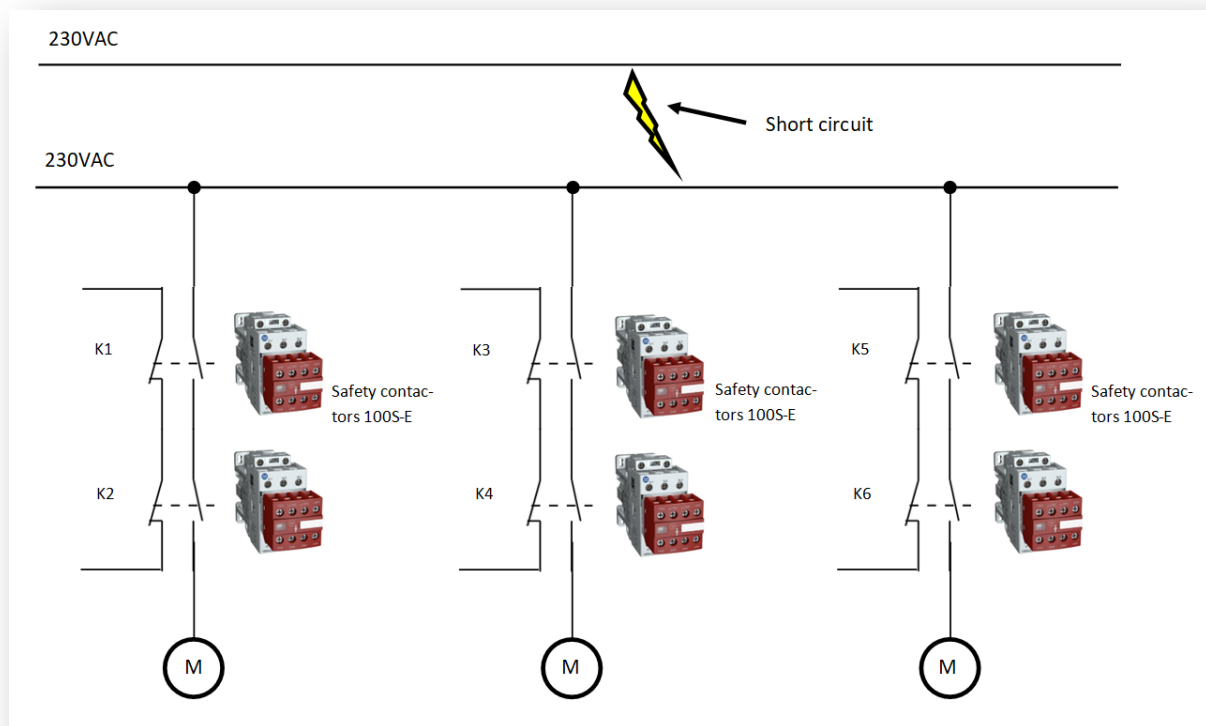


Figure 1

A possible short circuit between the two 230V-lines (in Figure 1) is not a dangerous failure, because the contactors can still switch off each motor safely.

This solution is capable up to PLe, depending on other values like $MTTF_D$, $B10_D$, DC etc.

When using grouping, you can shut down the power supply for all 3 motors by using 2 contactors. Each motor can be started and stopped separately “nonsafe” by a solid-state contactor.

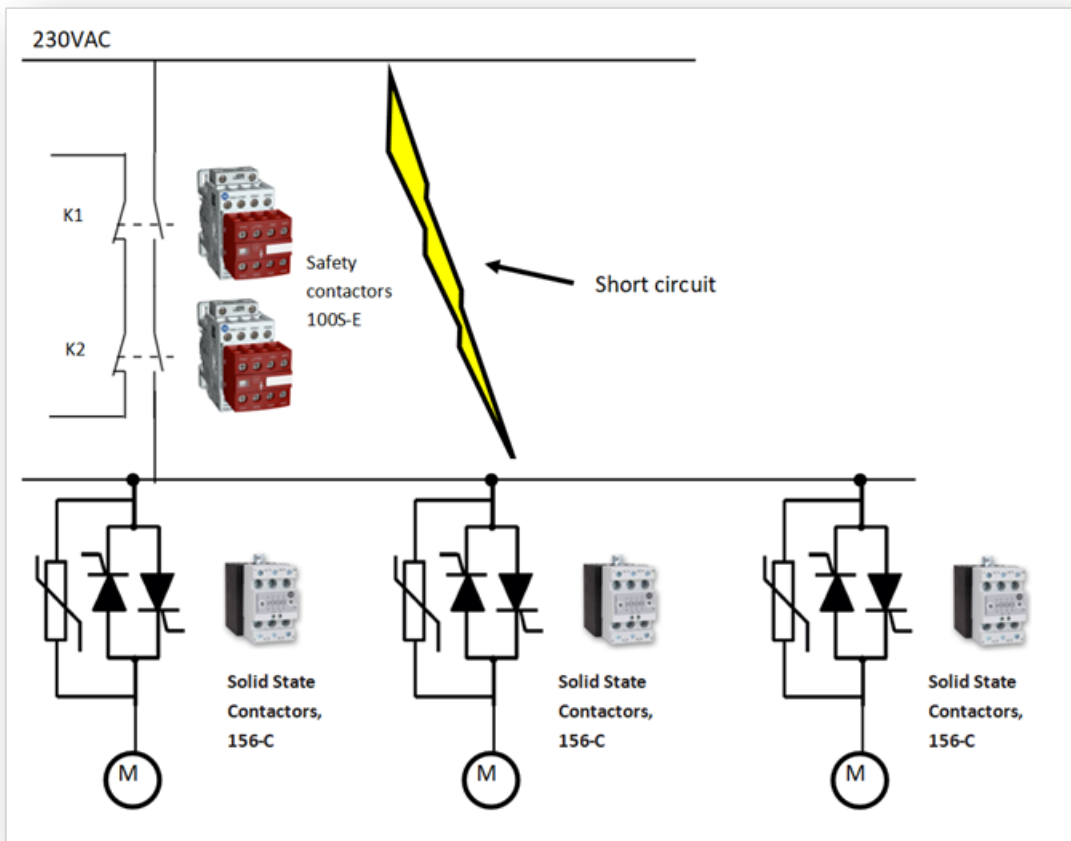


Figure 2:

A single dangerous failure could be a short circuit bypassing the safety contactors shown in figure 2. If this occurs, a safe stop may be impossible. In this case you may exclude the possible fault of a short circuit from 230V by bypassing the contactors down to the motor supply line. Requirements for such an exclusion are based on table D.4 in ISO 13849-2:

Short circuit between any two conductors may have been excluded if they are permanently connected and protected against external damage, e.g. by cable ducting, armoring, separate multicore cables and within an electrical enclosure, which meets the requirements of IEC 60204-1. (For exact and complete wording, please see the standards.)

These requirements can be approved by PanelBuilder® software.

This fault exclusion limits the PL normally to PLd.

Let's consider transferring the output-devices of a PLC-system with local or network-based output devices.

To shut down the actuators safely, you can place 2 safety relays or contactors between the standard output and the actuator:

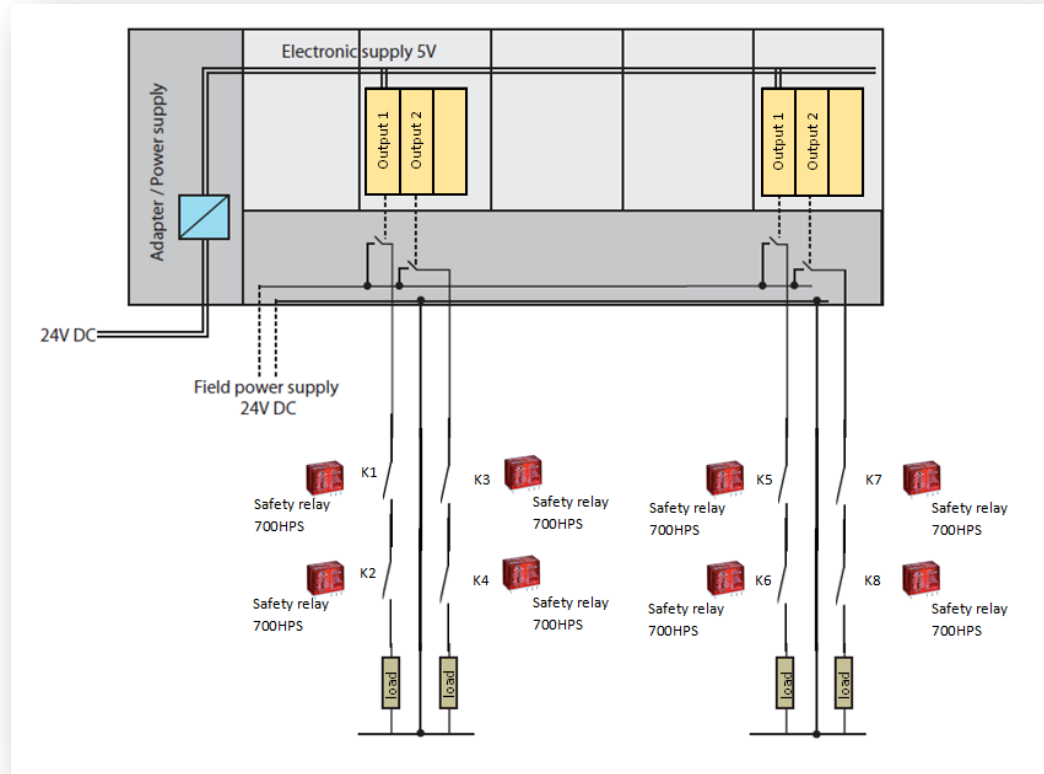


Figure 3 (load can be contactor, valve, STO-input or another device)

Each load is switched off safely by using a dual channel (Figure 3). This solution is capable for up to PLe, depending on DC, MTTF_D, CCF and so on.

Depending on your application and type of output devices, it might be necessary to use 2 actuators (contactor or valve) to achieve PLe. (see chapter 6)

If you want to group these outputs together, you can shut down the field power supply of the standard outputs by using 2 safety relays or contactors:

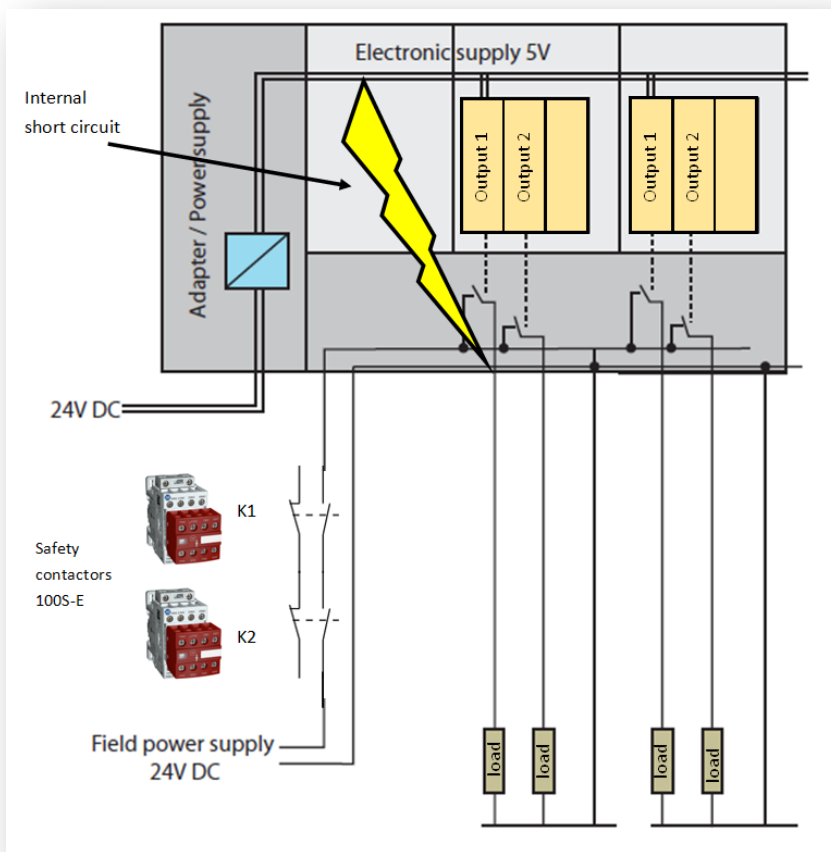


Figure 4 (load can be contactor, valve, STO-input or another device)

The safe shutdown of the actuators is done by the 2 contactors/relays in the field power supply (Figure 4). The standard outputs themselves are not part of the safety function, they start and stop the actuators controlled by the standard PLC.

A possible dangerous failure could be an internal short circuit between electronic power supply and field power supply on the printed circuit boards or to the direct output (Figure 4). In this case you must exclude the possible fault of the internal short circuit on the PCB between.

Requirements for this exclusion are based on table D.5 in ISO 13849-2:

Short circuit between two adjacent tracks or pads may be excluded if the base material, EP GC according to IEC 60893-1 is used as a minimum. The clearances and creepage distances are dimensioned to at least IEC 60664-5 (IEC 60664-1 for distances greater than 2 mm) with pollution degree 2/ overvoltage category III; if both tracks are powered by a SELV/PELV power supply, pollution degree 2/ overvoltage category II applies, with a minimum clearance of 0,1 mm.

The assembled board is mounted in an enclosure giving protection against conductive contamination, e.g. an enclosure with a protection of at least IP54, and the printed side(s) is (are) coated with an ageing-resistant varnish or protective layer covering all conductor paths.

(For exact and complete wording please see the standards.)

These requirements cannot be approved by PanelBuilder alone; you need to know the details of the output devices given by its manufacturer. The manufacturer must confirm that all requirements for the PCB, according to table D.5, are fulfilled.

Typically, this fault exclusion limits the PL to PLd.

Depending on your application and type of output devices it might be necessary to use 2 actuators (contactor or valve) to achieve PLd. (See chapter 6.)

5.Documentation and PL-calculation

When performing fault exclusion, you must state and justify this within your technical documentation. If the used output device is listed in chapter 7 of this document, you can refer to it to justify the fault exclusion.

If this failure is declared as impossible, you do not have to resolve it at your Performance Level calculation.

Let's look at the following example.

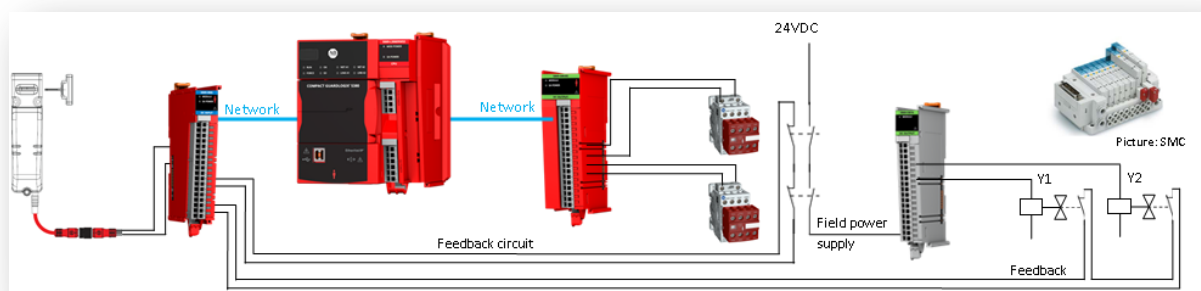


Figure 5, symbolic wiring diagram

The safety interlock switch is wired to the safety-input, which is connected to the safety PLC. The safety PLC controls safety outputs and the outputs control safety contactors. The safety contactors shut down the field power supply of standard outputs. The standard outputs control pneumatic valves. The valves control the pneumatic power of a cylinder. Feedback circuits may be needed to get diagnostics, DC.

These devices are involved:

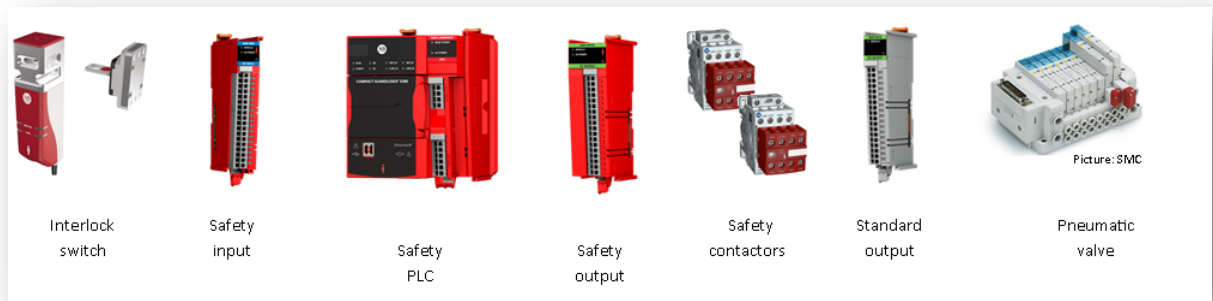


Figure 6

Not all devices need to be considered for the safety function. The standard outputs do not shut down safely. As described above, the fault exclusion for the internal short circuit needs to be completed and documented.

The safety-related components and block diagram for PL-calculation are as follows:



Figure 7

Block diagram:

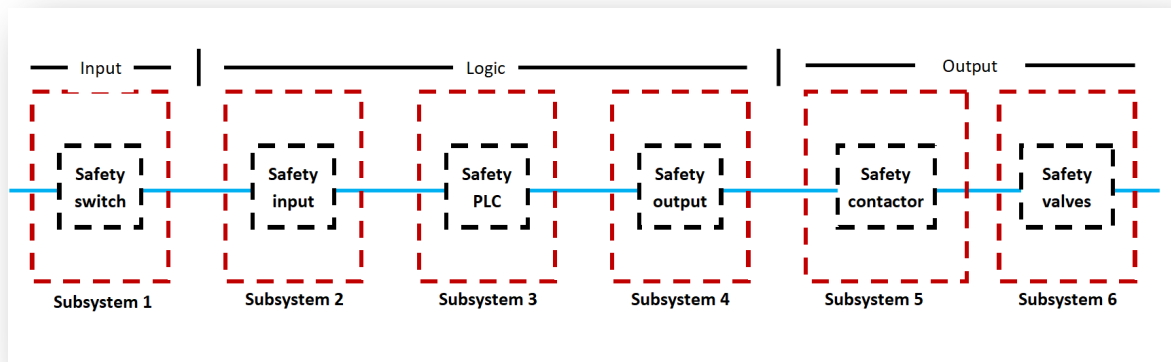


Figure 8

The devices/subsystems have to be considered for PL-calculation.

Note that the Performance Level is not only a value for the subsystems, but also for the whole safety function. Depending on your application and devices it might be necessary to use dual channel devices in each subsystem to achieve the required Performance Level.

Do not forget to validate your safety function by complete PL-calculation.

Different software tools are available for PL-calculation, like SISTEMA (IFA) and Safety Automation Builder® software (Rockwell Automation).

6. The following types of standard outputs fulfill the requirements according to IOS 13849-2, table D.5, line 1, and can be used for such applications with fault exclusion up to PLd.

5069 Compact 5000™ I/O modules

- 5069-OB8
- 5069-OB16
- 5069-OB16K
- 5069-OB16F
- 5069-OW4I
- 5069-OW16
- 5069-OX4I
- 5069-OA16

5094 FLEX 5000™ I/O modules

- 5094-OB8
- 5094-OB8XT
- 5094-OB16,
- 5094-OB16XT
- 5094-OB32
- 5094-OB32XT
- 5094-OW8I
- 5094-OW8IXT

1732E ArmorBlock® I/O modules

- 1732E-OB8M8SR
- 1732E-8CFG8M8R
- 1732E-OF4M12R

1734 POINT I/O™ modules

- 1734-OB2
- 1734-OB2E
- 1734-OB2EP
- 1734-OB4
- 1734-OB4E
- 1734-OB8
- 1734-OB8E

1756 local IO modules

- 1756-OA16I
- 1756-OA8D
- 1756-OB16D
- 1756-OB16I
- 1756-OB32
- 1756-OB8EI
- 1756-OW16I
- 1756-OX8I

1794 FLEX™ I/O modules

- 1794-IB10XOB6
- 1794-OB8EP
- 1794-OB16
- 1794-OB16P
- 1794-OW8

7. Wiring examples

5069 Compact I/O™ modules

-

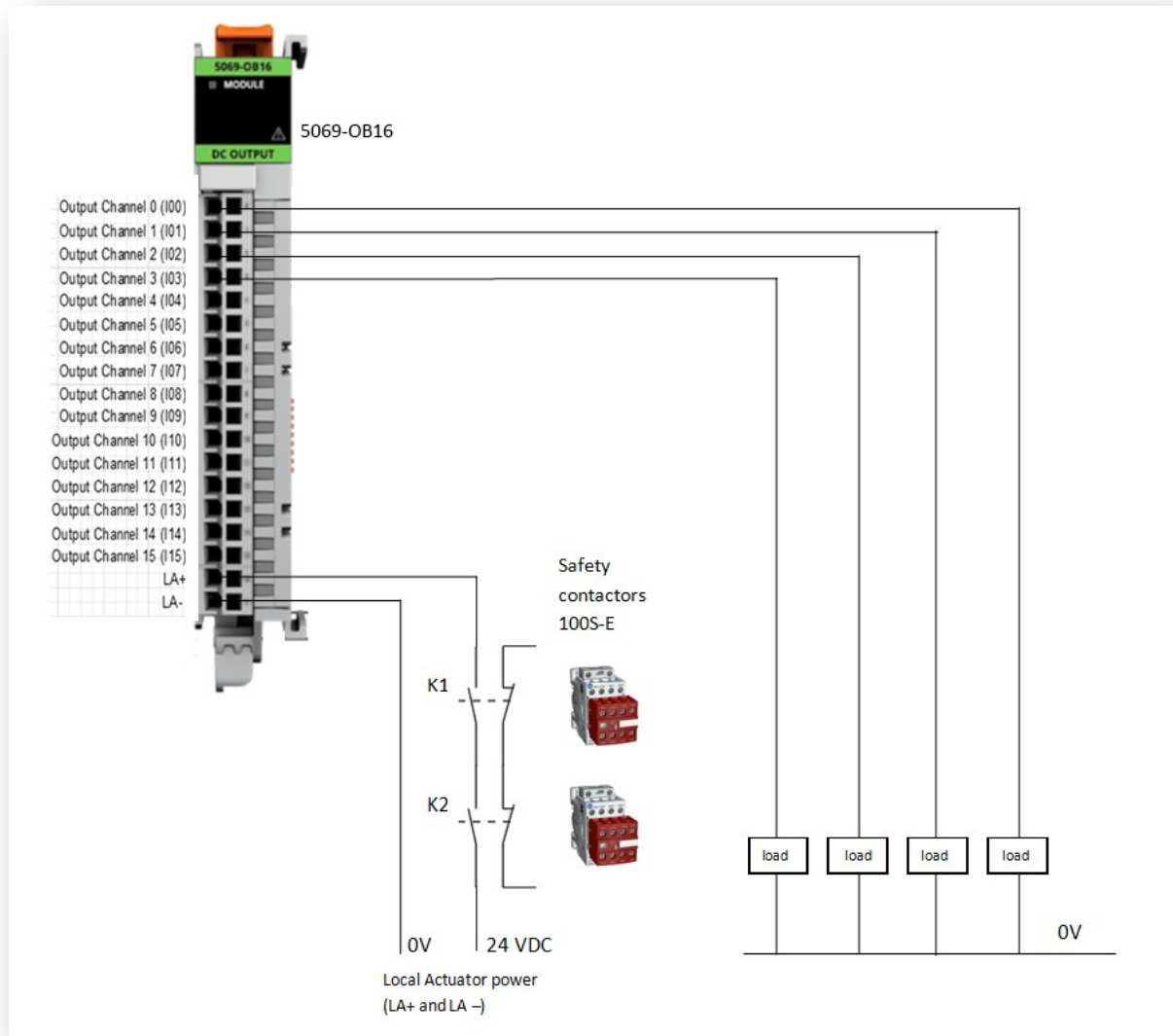


Figure 9

1734 POINT I/O modules

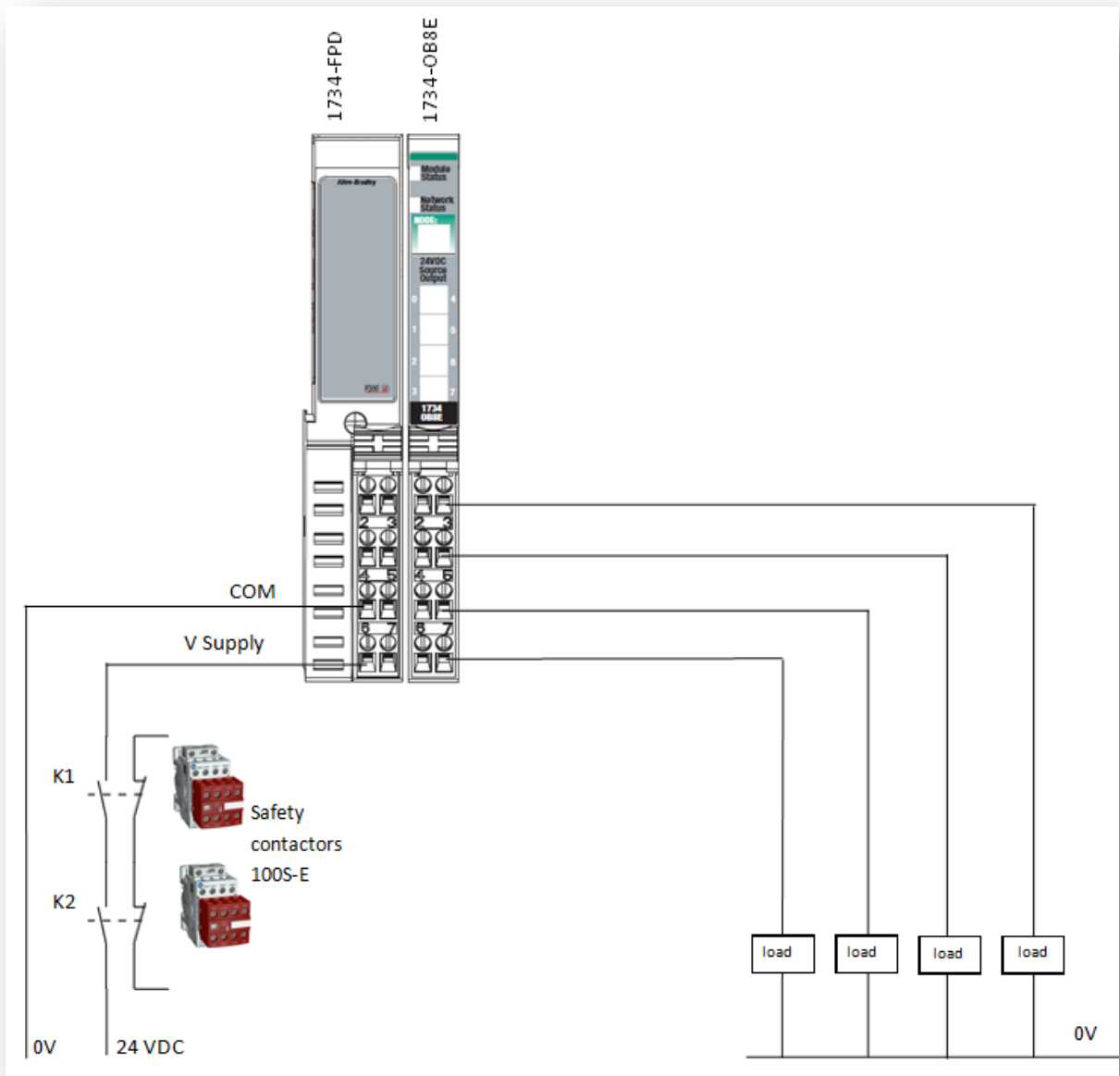


Figure 10

5094 FLEX 5000 I/O modules

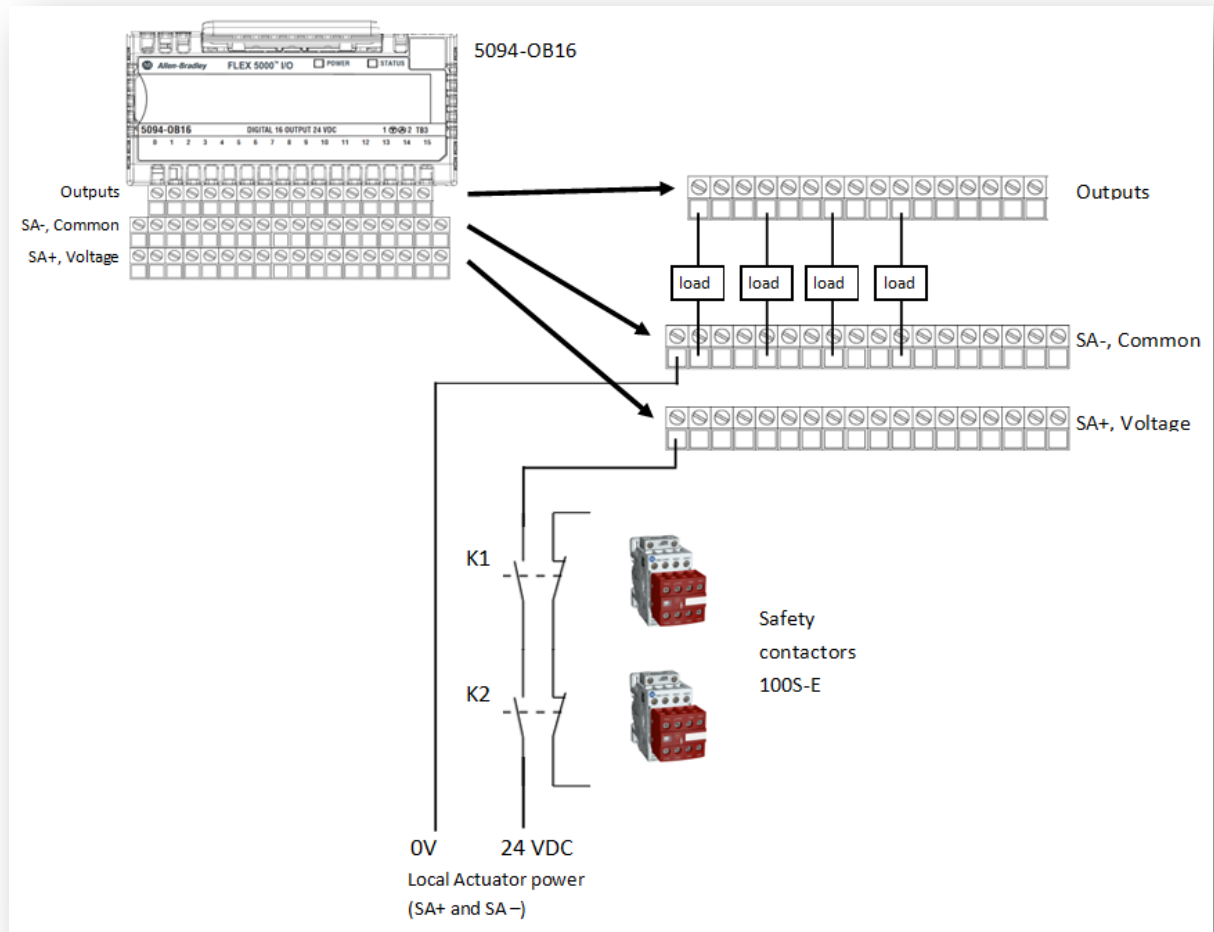


Figure 11

1756 ControlLogix® I/O modules

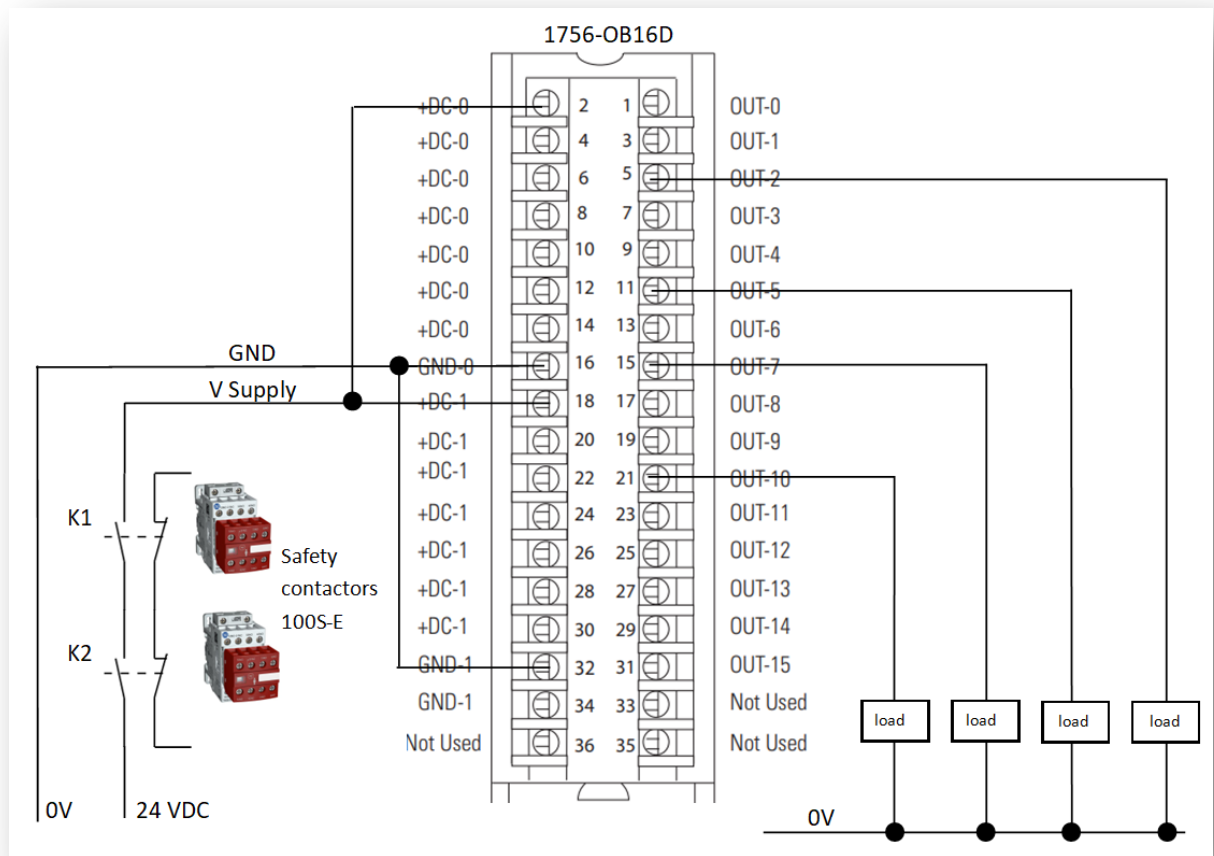


Figure 12

1732E ArmorBlock I/O modules

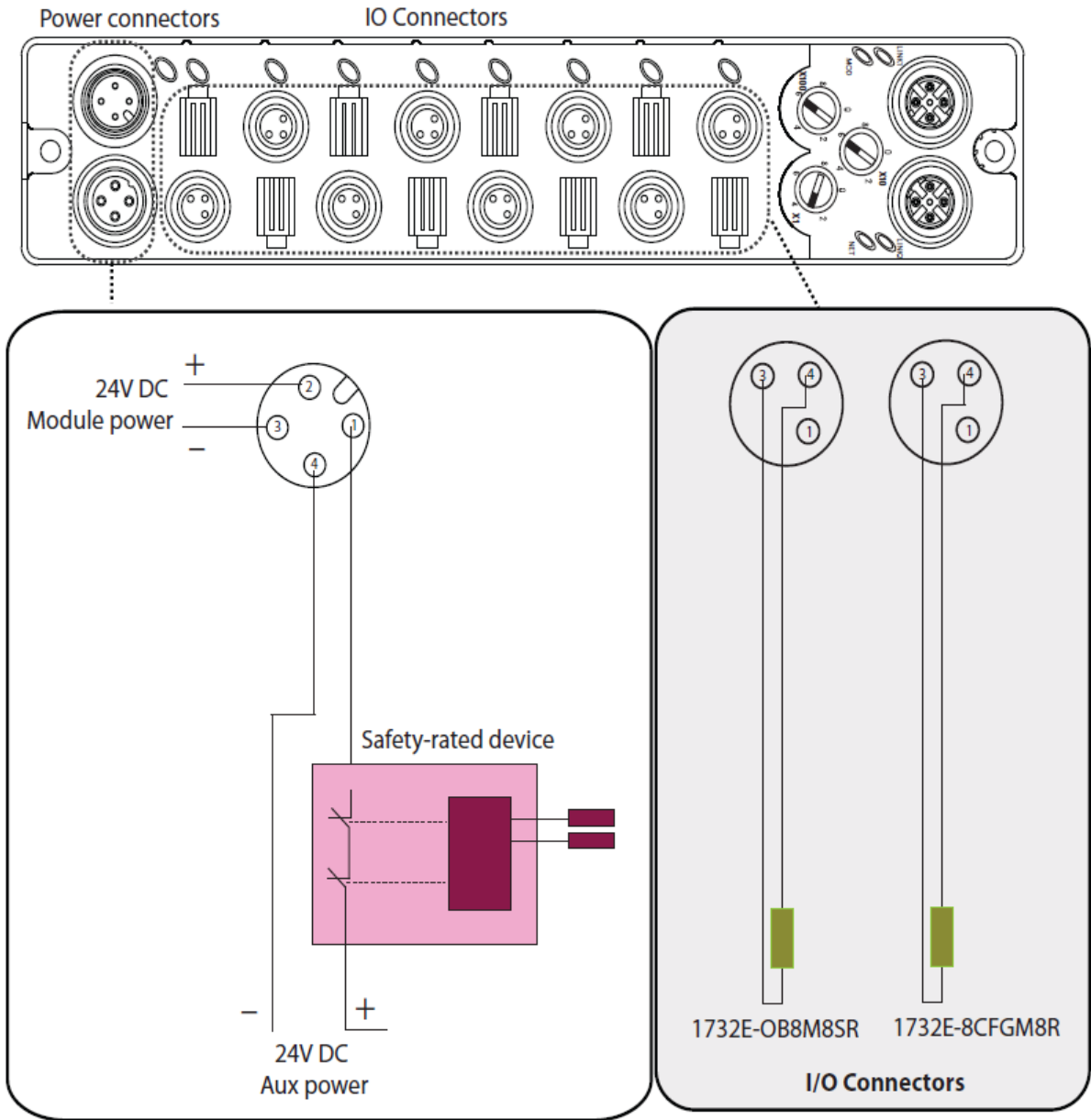


Figure 13

Connect with us.    

rockwellautomation.com — expanding **human possibility**[®]

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640

ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Allen-Bradley, ArmorBlock, Compact 5000, Compact I/O, ControlLogix, expanding human possibility, FLEX 5000, FLEX I/O, PanelBuilder, POINT I/O, Rockwell Automation and Safety Automation Builder are trademarks of Rockwell Automation, Inc.

Publication 5069-WP001A-EN-P — March 2022

Copyright© 2022 Rockwell Automation, Inc. All rights reserved. Printed in USA.