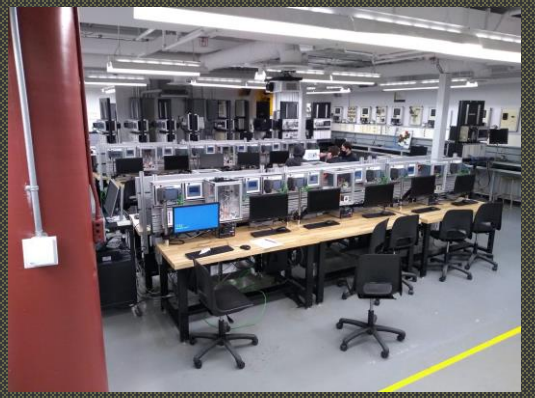


PROGRAMMABLE LOGIC CONTROLLERS
MENG 3500

HUMBER

PLC Enclosures

- PLC Protection Requirements:
  - Temperature extremes, humidity, dust, shock, vibration, and corrosive environments.
- Mounting of PLCs:
  - Typically, within a machine or in a separate enclosure for protection.

- NEMA Enclosure Types:
  - Defined by National Electrical Manufacturers Association (NEMA).
  - Recommended Enclosure for Solid-State Control Devices:
    - NEMA 12, enclosure suitable for general purpose areas and designed to be dust-tight.
- Material of Enclosures:
  - Typically metal for electromagnetic radiation shielding.

Figure 13-1 Typical PLC control panel enclosure.
Source: Courtesy Aaron Associates.

PLC Enclosures

- Heat Dissipation in PLC Installation:
  - Heat generated from power supplies, local I/O racks, and processor.
- Temperature Control:
  - Internal enclosure temperature shouldn't exceed controller's maximum operating temperature (usually 60°C max).
- Cooling Provisions:
  - Fans or blowers may be necessary for high internal or ambient temperatures.
- Mounting Orientation:
  - PLCs mounted horizontally for thermal considerations.
  - Manufacturer's name facing outward and left side up.

Frank D. Petruzella Programmable Logic Controllers 5th edition

HUMBER

PLC Enclosures

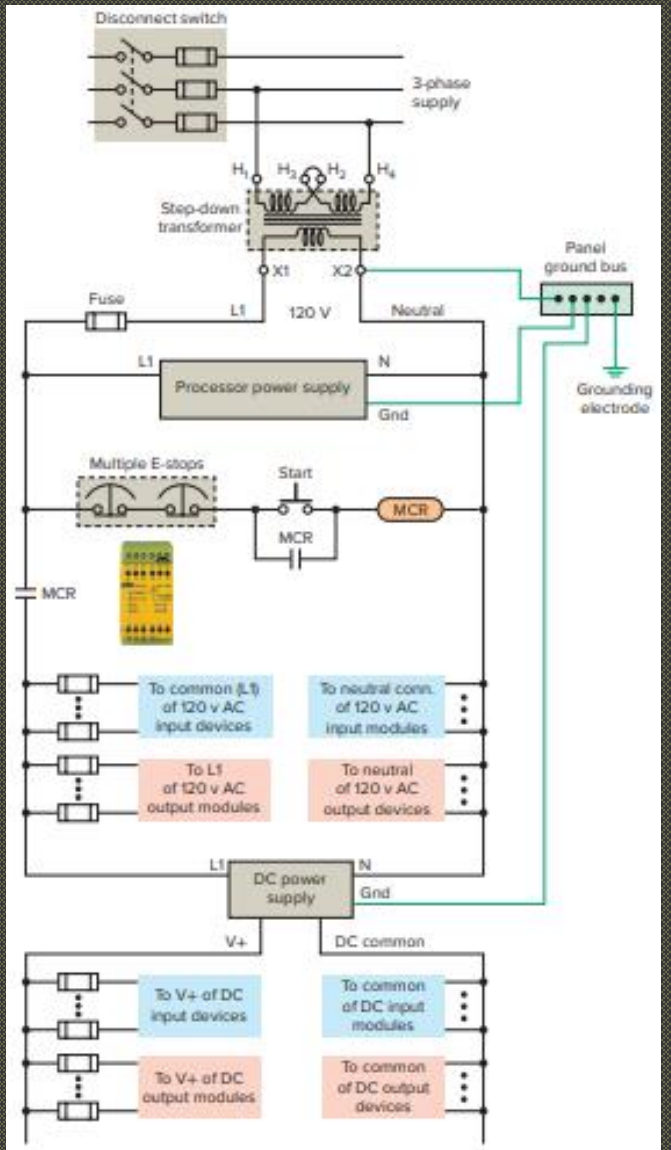


Figure 13-3 Typical wiring for an AC power distribution with a master control relay.
Source: Courtesy Pilz GmbH & Co. KG.

- Hardwired Electromechanical Master Control Relay (MCR):
  - Integral part of PLC system wiring.
  - De-energizes entire circuit that does not depend on software.
- Function of MCR:
  - Interrupts power to I/O rack during emergencies.
  - Maintains power to processor for diagnostics.
- Power Disconnect Switch:
  - Enables servicing PLC with power off when needed.
- Step-Down Transformer:
  - Provides isolation from main power.
  - Decreases voltage to 120V for controller and DC power supplies.

PLC Enclosures

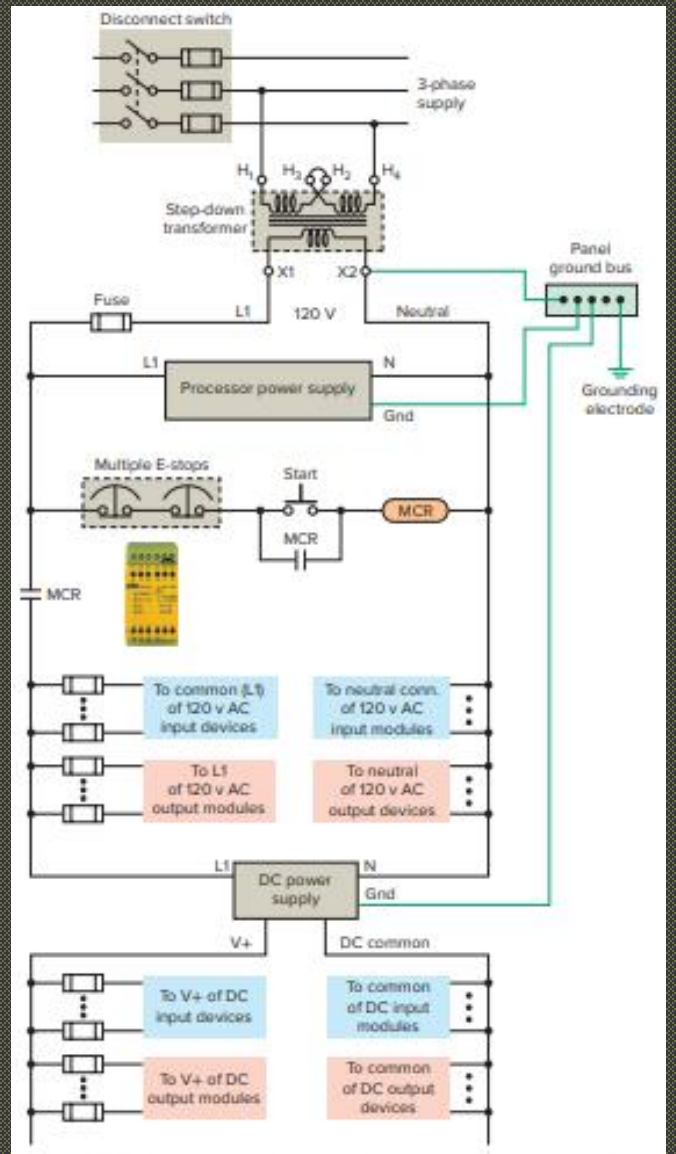
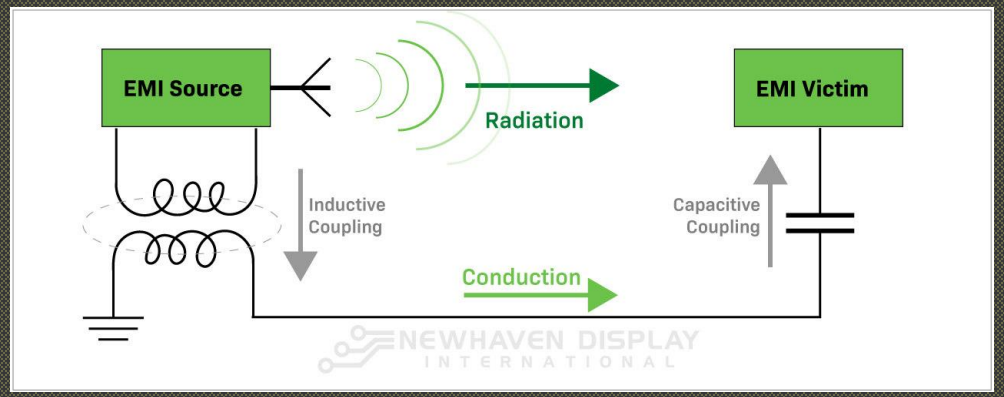


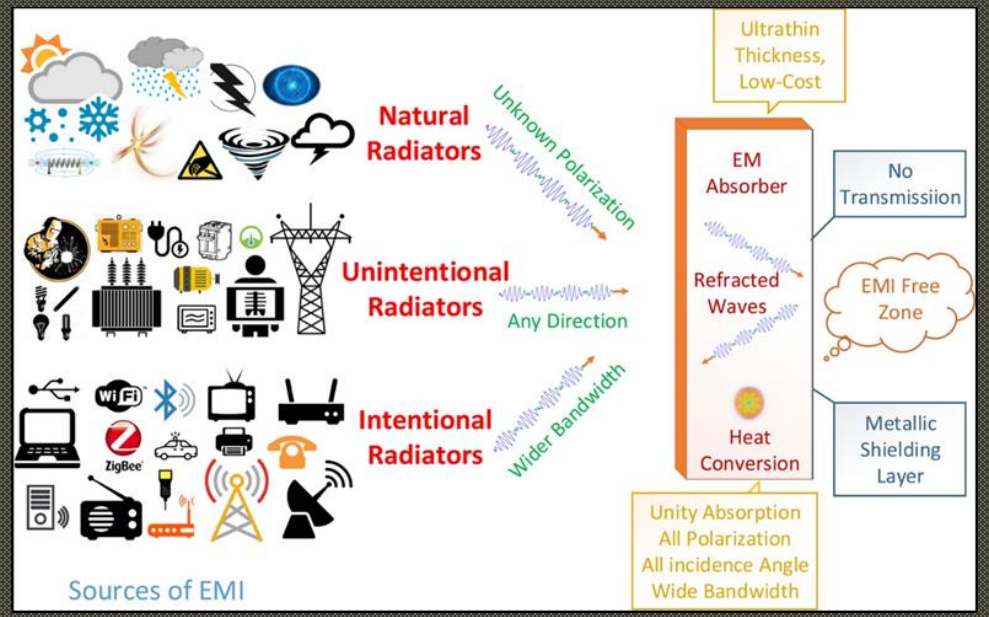
Figure 13-3 Typical wiring for an AC power distribution with a master control relay.
Source: Courtesy Pilz GmbH & Co. KG.

- Power Disconnect Switch:
  - Easily accessible for operators and maintenance.
  - Mount outside PLC enclosure for quick access.
- Machine Safety Precautions:
  - Disconnect all power sources (electrical, pneumatic, hydraulic).
  - Lock out to ensure safety before work.
- Limit Switches/Emergency Stop Buttons:
  - Connected in series with MCR.
  - Activation cuts power to master control.
- MCR and Safety:
  - Doesn't replace disconnect switch.
  - Always use disconnect switch, lock, and tag out during maintenance.

Electrical Noise

- Electrical noise, EMI, is unwanted electrical signals that produce undesirable effects and disrupt the electrical circuits.
- EMI may be either radiated or conducted.
  - Radiated noise originates from a source and travels through the air, such an antenna
  - Conducted noise travels on an actual conductor, such as a power line.
- Noise usually enters through input, output, and power supply lines.





HUMBER

Frank D. Petruzella Programmable Logic Controllers 5th edition

https://copperpod.medium.com/electromagnetic-wave-absorbers-a-solution-to-wave-pollution-5ca189f3d37b

Electrical Noise

To reduce the effect of EMI:

- Locate the controller away from noise-generating devices such as large AC motors and high-frequency welders
- Ground properly the equipment
- Route properly the wires
- Add suppression to noise-generating devices

Lack of surge suppression on inductive loads may contribute to processor faults and sporadic operation as they can cause an electrical pulse to be back-fed into the PLC system.

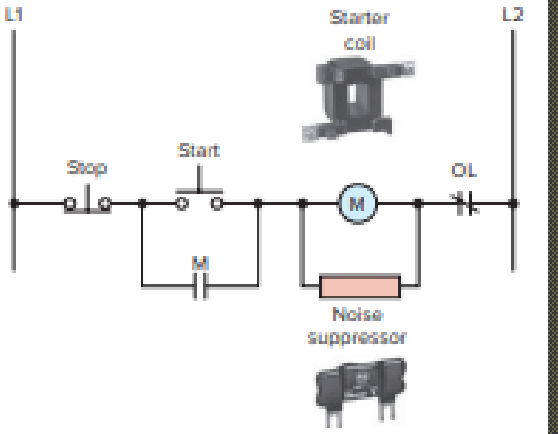


Figure 13-4 Motor starter noise suppression.
Source: Images Courtesy of Rockwell Automation, Inc.

Electrical Noise

- Routing field power and signal wiring properly, both outside and inside the PLC enclosure, reduces electrical noise (cross-talk interference).
- Guidelines for PLC Wire Routing:
  - Use shortest wire runs for I/O signals.
  - Use metal conduit for conductors from PLC enclosure to other locations.
  - Separate signal wiring from power wiring.
  - Keep AC and DC I/O signal wires in separate wireways.
  - Route low-level signal conductors (e.g., thermocouples, serial communications) as shielded twisted pair and separately.
  - Consider fiber optic system for signal wiring.

Figure 13-5 Heat-shrinkable wire identification sleeves.
Source: Courtesy Tyco Electronics Ltd.

Leaky Inputs and Outputs

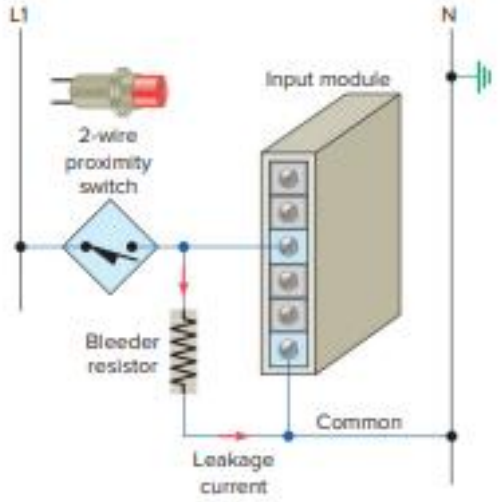


Figure 13-6 Bleeder resistor connection for input sensors.

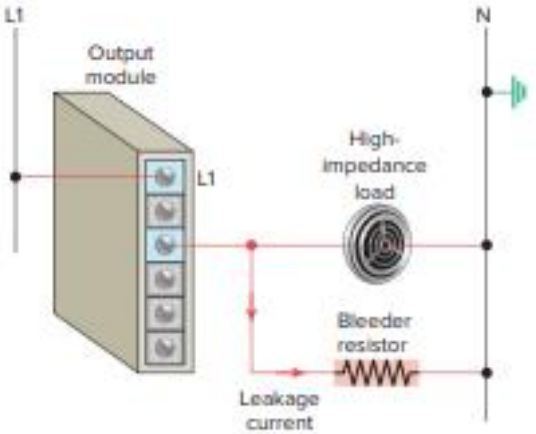


Figure 13-7 Bleeder resistor connection for a high-impedance output.

Input field devices with transistor or triac outputs may have leakage current when in the OFF state.

- Adding a bleeder resistor (10 to 20 kΩ) in parallel with the input provides a lower resistance path for the leakage current to flow.

Leakage current can happen with solid-state switches in output modules.

- Adding a resistor in parallel with the load helps bleed off this current.
- Alternatively, an isolation relay can solve this issue.

Grounding

- Grounding Information:
  - Electrical code and manufacturers provide guidance on conductors, color codes, and connections for safe grounding.
- Requirements for Grounding Path:
  - Permanent, continuous, solder-free.
  - Able to safely conduct ground-fault current with minimal impedance.
- PLC Installation Grounding:
  - Entire installation, including enclosures, CPU, I/O chassis, and power supplies, connected to single low-impedance ground.
- Preventing Nonconductive Coating:
  - Remove paint or nonconductive material where chassis contacts enclosure.
- Ground Loop Issues:
  - Ground loops can affect input signal devices by adding or subtracting current or voltage.
  - Varying magnetic fields through ground loops can produce voltage and induce current flow.
- Shielded Cable Grounding:
  - Ground shields of cables at one end only to prevent ground loops.

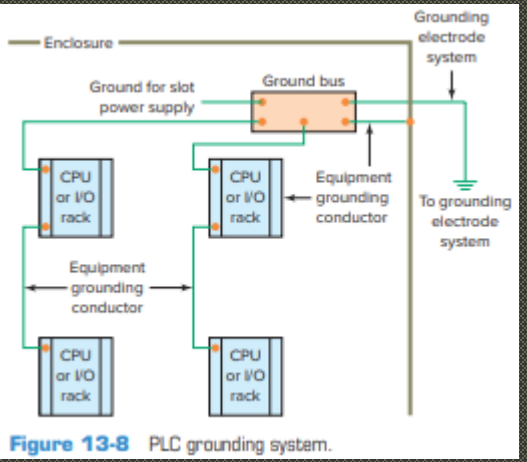


Figure 13-8 PLC grounding system.

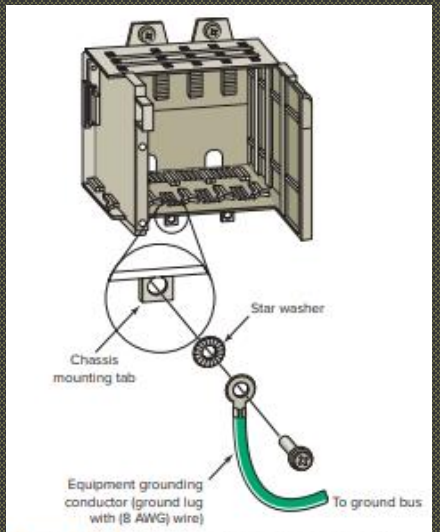


Figure 13-9 Make ground connections using a star washer.

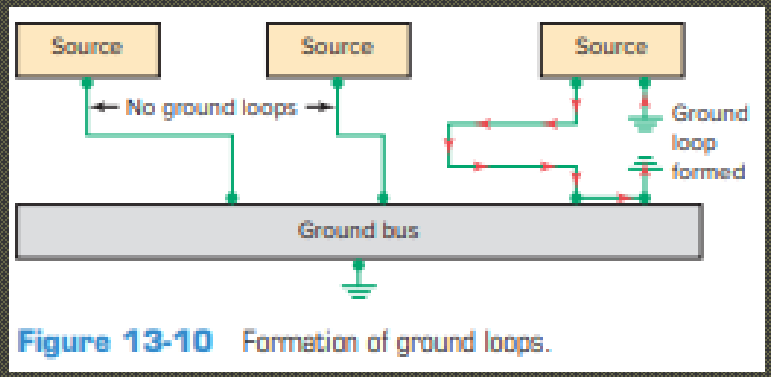


Figure 13-10 Formation of ground loops.

Surge Voltages

- Inductive Load Voltage Spike:
  - Turning off current in an inductive load generates high voltage spike.
- Suppression Techniques:
  - Absorb inductive induced voltage to reduce or eliminate high voltage.
- Built-in Suppression Networks:
  - Output modules for inductive loads typically include suppression networks.
- Recommendation for External Suppression Device:
  - Use additional external suppression device if output module controls relays, solenoids, motor starters, or motors.
- Appropriate Suppression Component Rating:
  - Suppression components must be rated to suppress switching transient characteristic of specific inductive device.

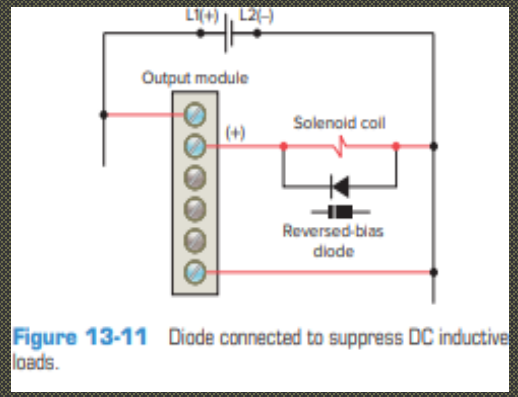


Figure 13-11 Diode connected to suppress DC inductive loads.

When voltage to the solenoid is switched off, a voltage spike with opposite polarity is generated due to the collapsing magnetic field. This induced voltage creates a current flow through the diode, reducing the high-voltage spike.

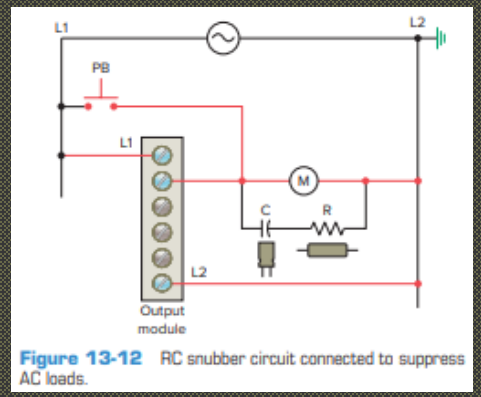


Figure 13-12 RC snubber circuit connected to suppress AC loads.

The resistor and capacitor connected in series slows the rate of rise of the transient voltage, which occurs at the instant the current path to the coil is opened.

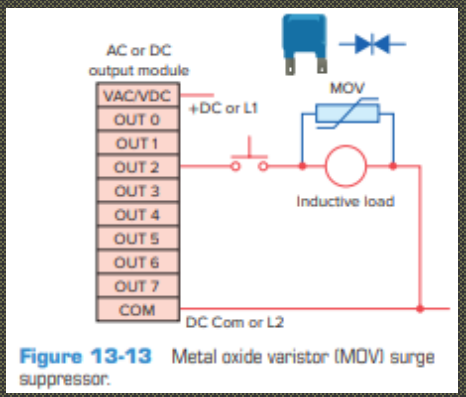


Figure 13-13 Metal oxide varistor (MOV) surge suppressor.

The device acts as an open circuit until the voltage across it in either direction exceeds its rated value. Any greater voltage peak instantly makes the device act like a short circuit.

Preventive Maintenance

Preventive Maintenance Tasks During Short Shutdown Periods:

- Clean or replace filters in enclosures for clear air circulation.
- Clean dust or dirt accumulated on PLC circuit boards to prevent heat dissipation obstruction or short circuits.
- Check tightness of connections to I/O modules, ensuring all plugs, sockets, terminal strips, and module connections are secure.
- Inspect field I/O devices to ensure proper adjustment; calibrate analog devices every 6 months and service sensors monthly.
- Avoid placing heavy-noise or heat-generating equipment too close to the PLC.
- Check condition of battery backing up RAM memory in CPU; most CPUs have a battery status indicator.
- Stock commonly needed spare parts, especially input and output modules.
- Keep a master copy of operating programs used.

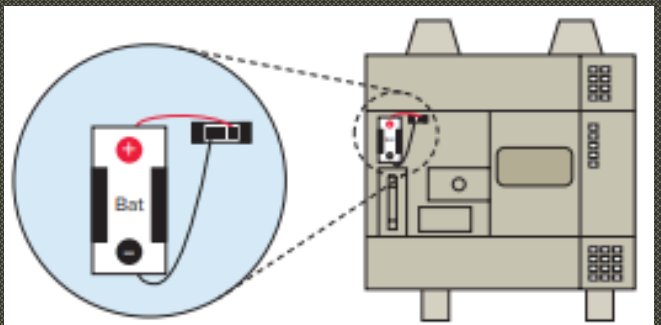


Figure 13-17 CPU backup memory battery.

Preventive Maintenance

- Check connections with power removed to avoid injury and equipment damage.
- De-energize all power sources (electrical, pneumatic, hydraulic) before working on machine controlled by PLC.
- Implement lockout and tagout procedures to prevent equipment operation during maintenance and repairs.

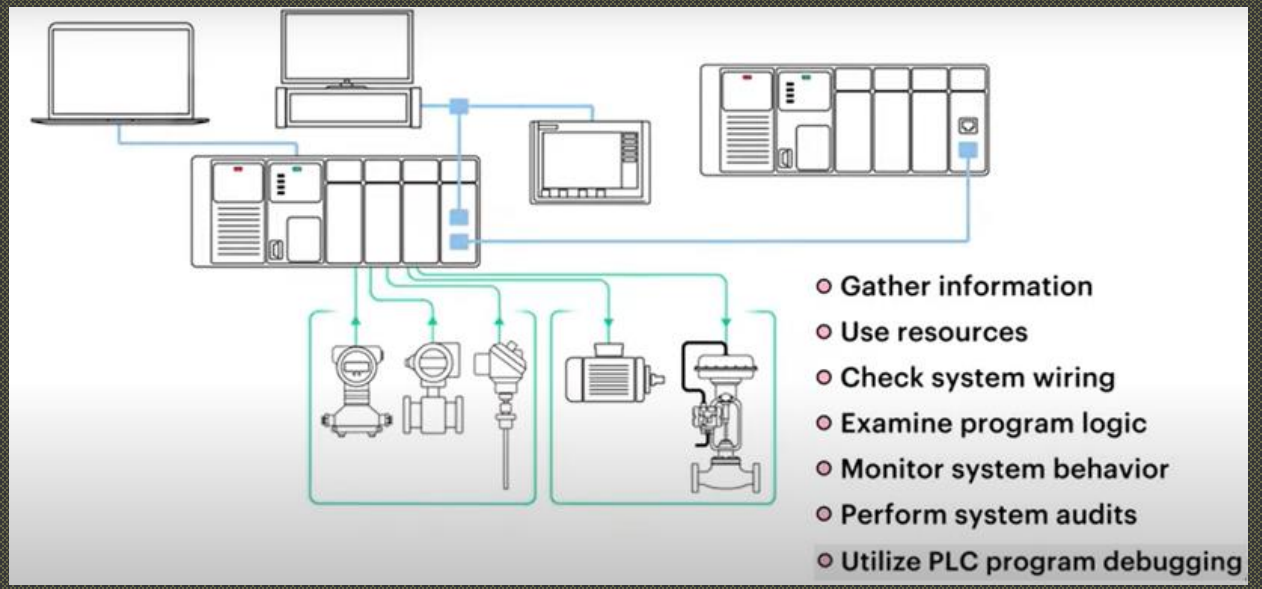
Figure 13-18 Lockout/tagout devices.
Source: Photo courtesy Panduit Corporation, **www.panduit.com**

HUMBER

Frank D. Petruzella Programmable Logic Controllers 5th edition

TROUBLESHOOTING

- PLC Program Display:
  - Display program on monitor to watch real-time execution during fault troubleshooting.
- Confidence in Program Accuracy:
  - If control system has been operating, confidence in program logic accuracy.
- Considerations for Programming Errors:
  - Newly commissioned system may have programming errors to consider.



HUMBER

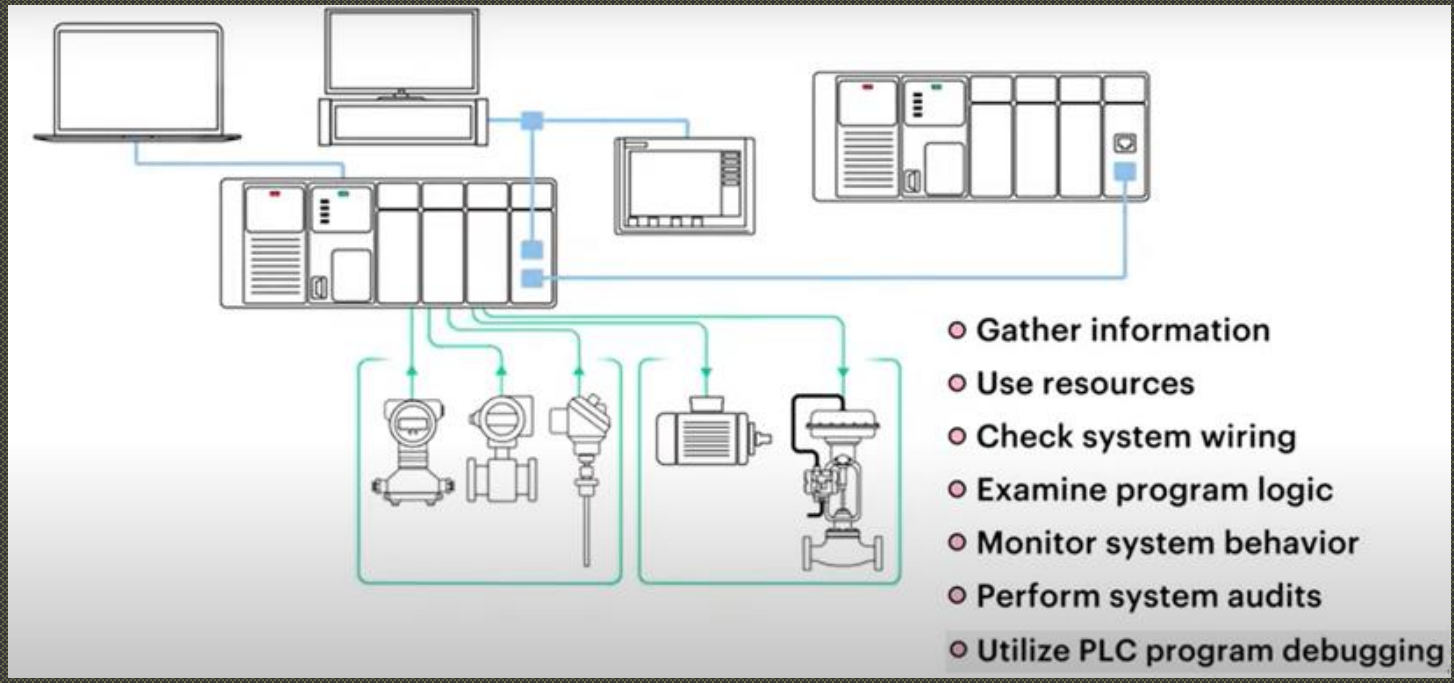
Frank D. Petruzella Programmable Logic Controllers 5th edition

https://www.youtube.com/watch?v=bFvgWXkbMU0

TROUBLESHOOTING

Troubleshooting Procedure:

- Identify problem/source as first step.
  - Possible Sources of Problem:
    - Processor module.
    - I/O hardware, wiring.
    - Machine inputs or outputs.
    - Ladder logic program.



HUMBER

Frank D. Petruzella Programmable Logic Controllers 5th edition

https://www.youtube.com/watch?v=bFvgWXkbMU0

Troubleshooting

Processor

- Processor Status Indicators:
  - Processor performs error checks and sends status info to front indicators.
- Accessing Detailed Information:
  - More detailed faults/status can be obtained through programming software.
- Status Indicators:
  - RUN (Green):
    - On steady: Process is in RUN mode.
    - Flashing during operation: Transferring program from RAM to memory module.
    - Off: Processor in mode other than RUN.
  - FLT (Red):
    - Flashing at power-up: Processor not configured.
    - Flashing during operation: Major error in processor, chassis, or memory.
    - On steady: Fatal error present (no communications).
    - Off: No errors.
  - BATT (Red):
    - On steady: Battery voltage low or missing.
    - Off: Battery functional.

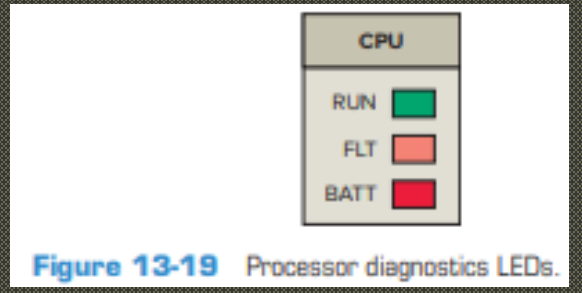


Figure 13-19 Processor diagnostics LEDs.

Troubleshooting

Processor

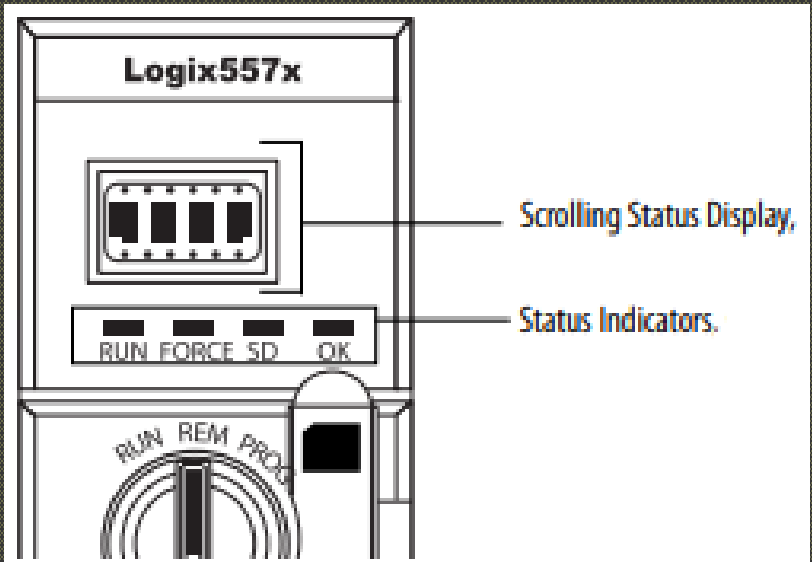


Table 60 - RUN Indicator

State	Description
Off	The controller is in Program or Test mode.
Steady green	The controller is in Run mode.

Table 61 - FORCE Indicator

State	Description
Off	No tags contain I/O force values.
Solid amber	I/O forces are active (enabled) though I/O force values and can be configured. **Use caution if you install (add) a force. If you install (add) a force, it immediately takes effect.**
Flashing amber	One or more input or output addresses have been forced to an On or Off state, but the forces have not been enabled. **Use caution if you enable I/O forces. If you enable I/O forces, all existing I/O forces also take effect.**

Table 62 - SD Indicator

State	Description
Off	No activity is occurring with the SD card.
Flashing green	The controller is reading from or writing to the SD card. Do not remove the SD card while the controller is reading or writing.
Solid green	
Flashing red	The SD card does not have a valid file system.
Solid red	The controller does not recognize the SD card.

Table 63 - OK Indicator

State	Description
Off	No power is applied to the controller.
Flashing red	Either of the following is true: • It is a new controller, out of the box, and it requires a firmware upgrade. If a firmware upgrade is required, the status display indicates Firmware Installation Required. To upgrade firmware, see Upgrade Controller Firmware on page 50. • It is a previously used or in-use controller and a major fault has occurred. For details about major recoverable and nonrecoverable faults, see the Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
Solid red	One of the following is true: • The controller is completing power-up diagnostics. • The charge of the capacitor in the ESM is being discharged upon powerdown. • The controller is powered, but is inoperable. • The controller is loading a project to nonvolatile memory.
Solid green	The controller is operating normally.

HUMBER

Rockwell Automation Publication 1756-UM001P-EN-P - May 2017

Troubleshooting

Processor

Scroller Status Display:

- Scrolls messages about firmware revision, Energy Storage Module status, project status, and major faults.
- Controller displays faults if present.
- "Major Fault TXX:CXX" message indicating major faults are displayed.

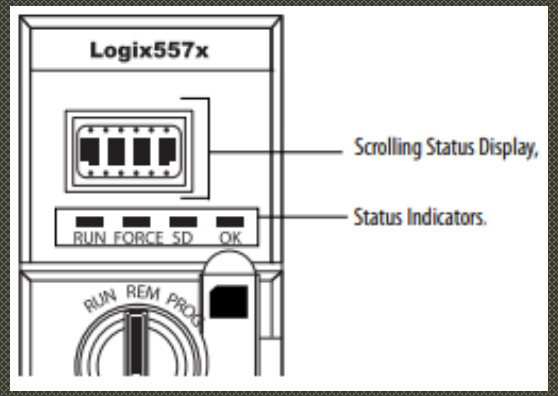


Table 57 - Fault Messages

Message	Interpretation
Major Fault T*XX*:C*XX message*	A major fault of Type *XX* and Code *XX* has been detected. For example, if the status display indicates Major Fault T04:C42 Invalid JMP Target, a JMP instruction is programmed to jump to an invalid LBL instruction. For details about major recoverable faults, see the Logix5000™ Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.
I/O Fault Local:*X* #*XXXX message*	An I/O fault has occurred on a module in the local chassis. The slot number and fault code are indicated along with a brief description. For example, I/O Fault Local:3 #0107 Connection Not Found indicates that a connection to the local I/O module in slot three is not open. Take corrective action specific to the type of fault indicated. For details about each I/O fault code, see the Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, publication 1756-PM014.

The user manual provides additional details on the ongoing count of messages in this table.

Table 56 - General Status Messages

Message	Interpretation
No message is indicated	The controller is Off. Check the OK indicator to determine if the controller is powered and determine the state of the controller.
TEST	The controller is conducting power-up tests.
PASS	Power-up tests have been successfully completed.
SAVE	A project is being saved to the SD card. You can also view the SD Indicator (see page 195) for more status information. Allow the save to complete before: • removing the SD card. • disconnecting power.

The user manual provides additional details on the ongoing count of messages in this table.

Table 58 - Major Fault Status Messages

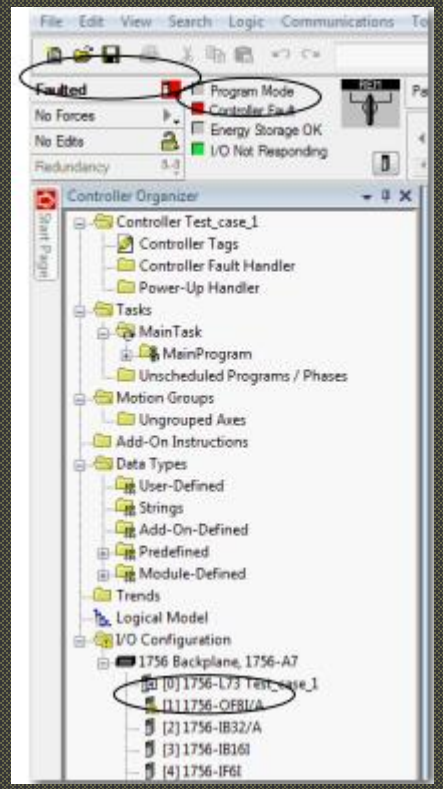
Type	Code	Message
1	1	Run Mode Powerup
1	60	Nonrecoverable
1	61	Nonrecoverable – Diagnostics Saved on CF Card
1	62	Nonrecoverable – Diagnostics and Program Saved on SD card
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	

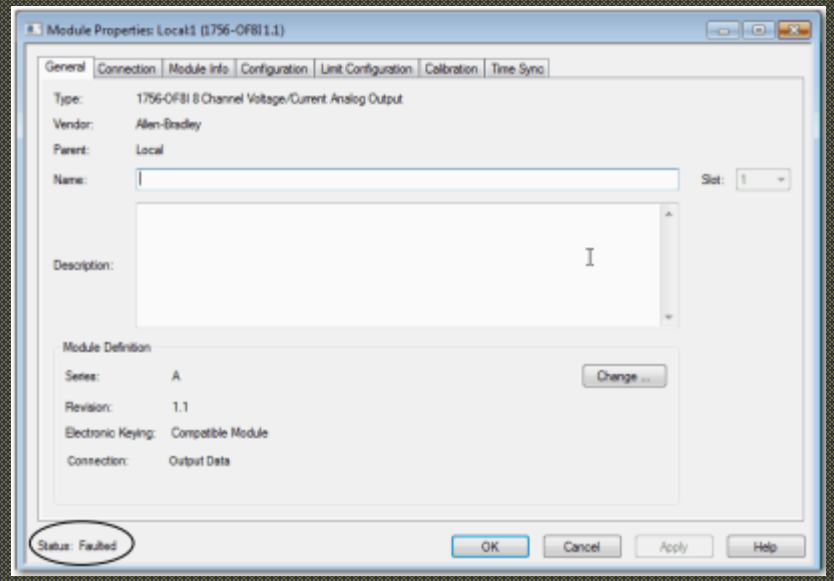
The user manual provides additional details on the ongoing count of messages in this table.

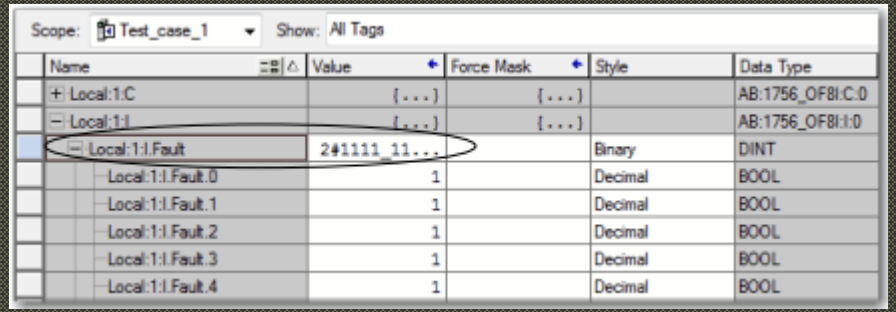
Troubleshooting - Processor

The processor constantly checks for any issues that could affect the program's execution.

1. Warning Signal for Module Disconnection:
   - Appears next to module on main screen when connection is broken.
2. Controller State and Fault Indication:
   - Controller state shows "Faulted", with Controller fault illuminated in red.
3. Status line on screen displays fault message:
   - Module Info tab lists Major and Minor Faults, along with Internal State.
4. Module Fault Reporting:
   - General module faults reported in Tag Editor.







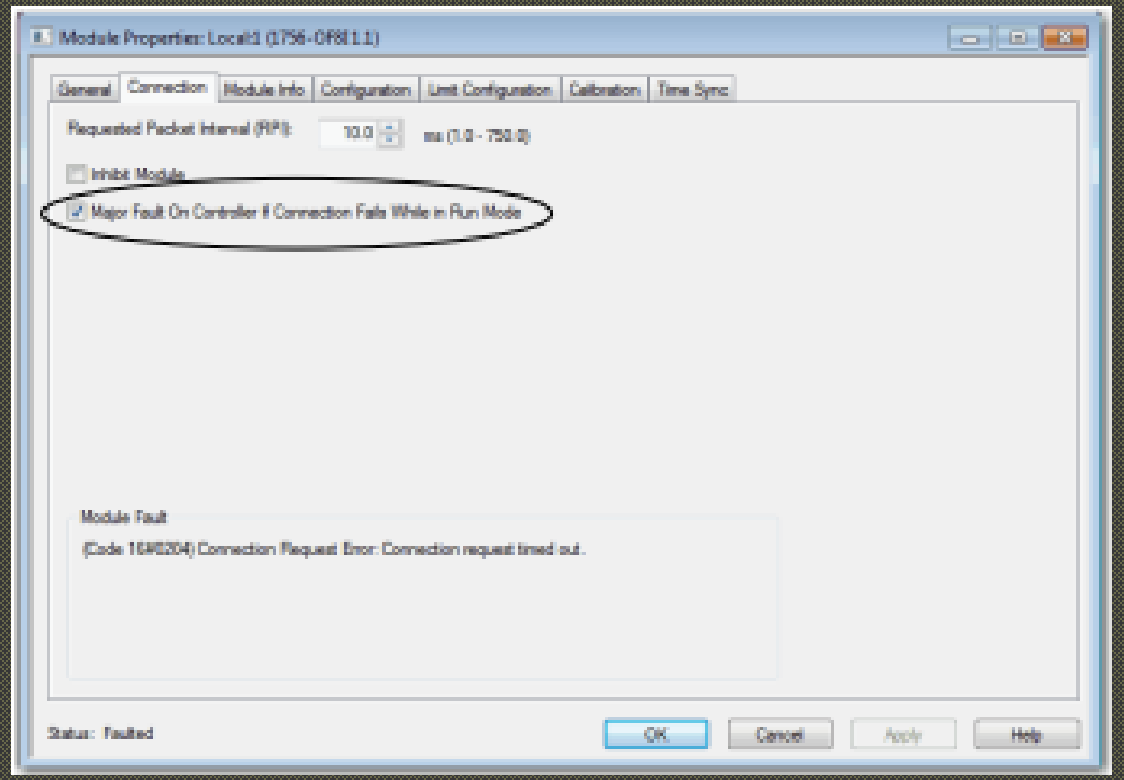
https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

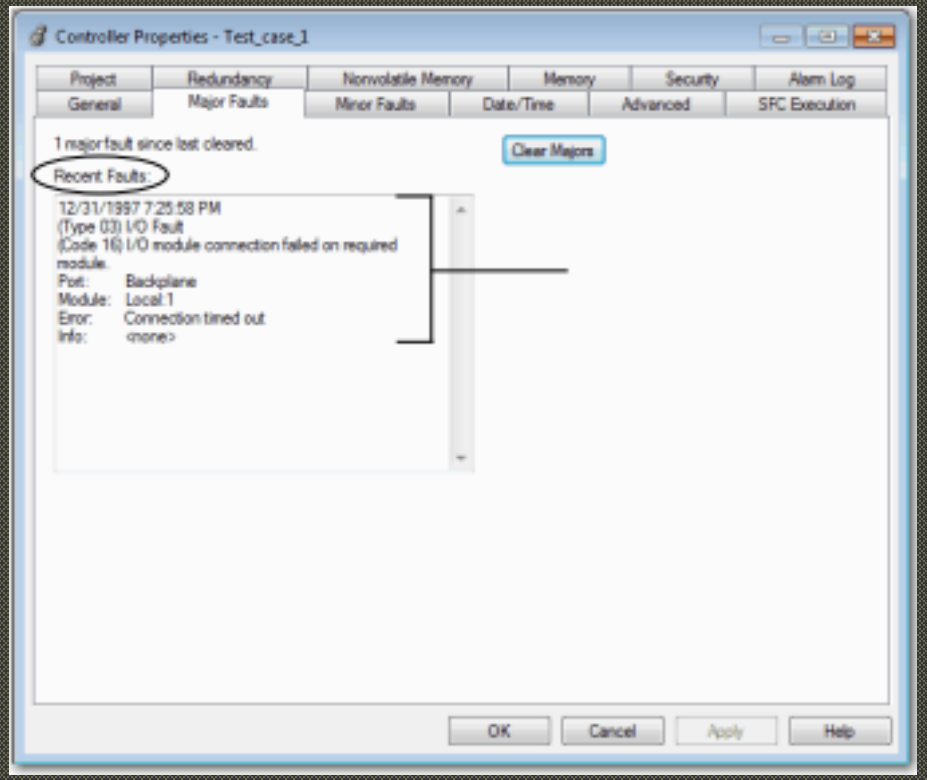
HUMBER

Troubleshooting

Processor

- Check the "Major Fault on Controller" option in the Connection tab to see recent faults in the Major Faults tab of Module Properties screen.
- In Logix Designer, when monitoring module configuration and you get a Communication fault, the Major Faults tab shows the fault type under Recent Faults.





https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

Troubleshooting

Processor

- The controller indicates I/O faults on the status display in one of these formats:
  - I/O Fault Local:X #XXXX message
  - I/O Fault ModuleName #XXXX message
- The first part of the format is used to indicate the location of the module with a fault I/O Fault
- The latter part of the format, #XXXX message, can be used to diagnose the type of I/O fault and potential corrective actions

Table 59 - I/O Fault Messages

Code	Message
#0001	Connection Failure
#0002	Insufficient Resource
#0003	Invalid Value
#0004	IOI Syntax

The user manual provides additional details on the ongoing count of messages in this table.

HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

Troubleshooting

Input/Output Malfunction

If the controller is operating in the RUN mode but output devices do not operate as programmed, the faults could be:

- Input and output wiring between field devices and modules
- Field device or module power supplies
- Input sensing devices
- Output actuators
- PLC I/O modules
- PLC processor

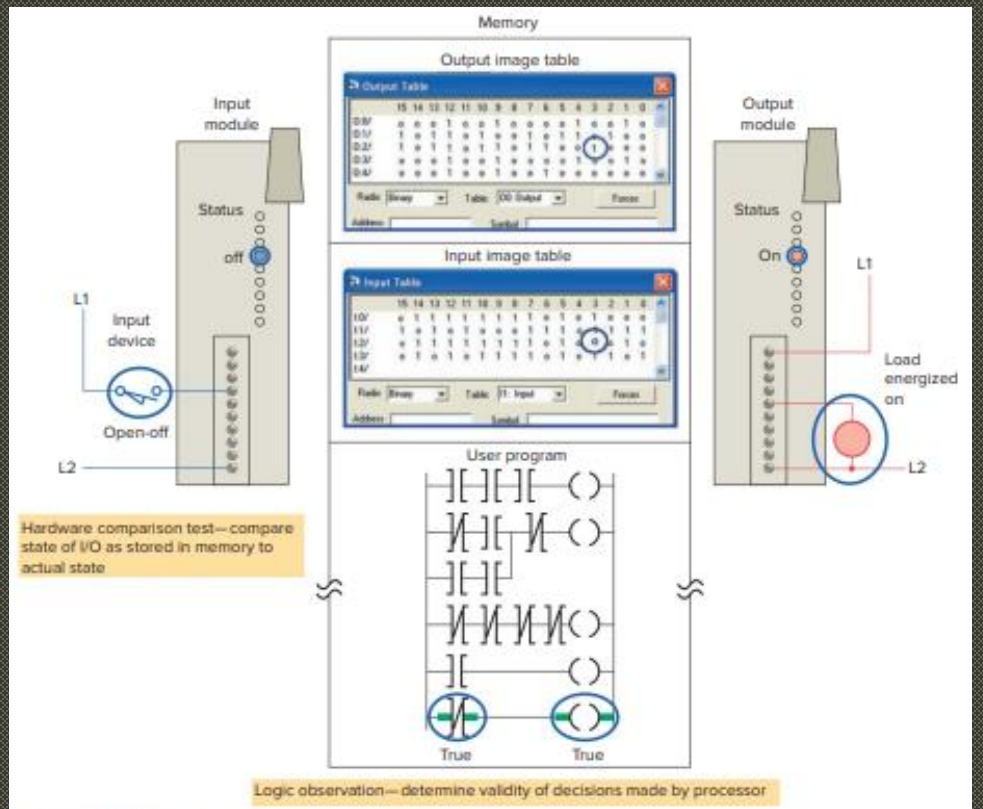


Figure 13-29 General methods of troubleshooting.
Source: Courtesy of TheLearningPit.

Troubleshooting

Input Malfunction

- Input module's status LED shows when its logic circuitry detects voltage in corresponding terminals to turn on.
- To isolate field device problems, compare suspect I/O actual status with controller indicators.
- Each device has status indicators on both the I/O module and the program device monitor.

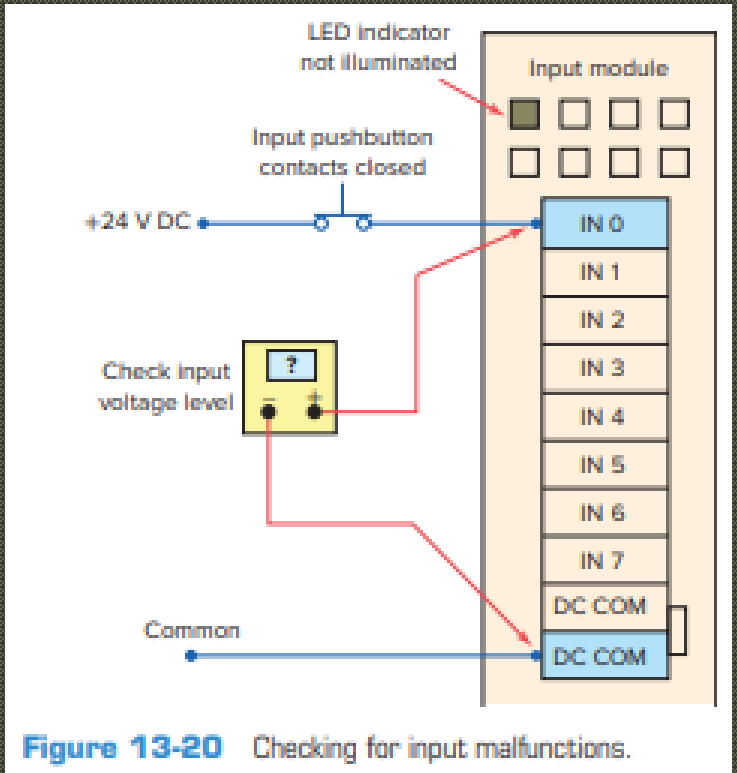


Figure 13-20 Checking for input malfunctions.

Input device troubleshooting guide

Input device condition	Input module status indicator	Monitor display status indicator		Possible fault(s)
				
 Closed — ON 24 V DC input	ON	True 	False 	None - correct indications
 Open — OFF 0 V DC input	OFF	False 	True 	None - correct indications
 Closed — ON 24 V DC input	ON	False 	True 	Sensor condition, input voltage, status indicator are correct. Ladder instructions have incorrect indications. Input module or processor fault.
 Closed — ON 0 V DC input	OFF	False 	True 	Status indicator and instructions agree but not with the sensor condition. Open field device or wiring.
 Open — OFF 0 V DC input	OFF	True 	False 	Sensor condition, input voltage, status indicator are correct. Ladder instructions have incorrect indications. Input module or processor fault.
 Open — OFF 24 V DC input	ON	True 	False 	Input voltage, status indicator, and ladder instructions agree but not with sensor condition. Short circuit in the field device or wiring.

Figure 13-21 Input troubleshooting guide.

Troubleshooting

Input Malfunction

When input hardware is suspected to be the source of a problem:

- Check if status indicator on input module lights up when it gets power from its device (e.g., pushbutton).
- If not lit, measure voltage across input terminal for correct level.
- If voltage is correct, replace input module.
- If voltage is incorrect, check power supply, wiring, or input device for faults.

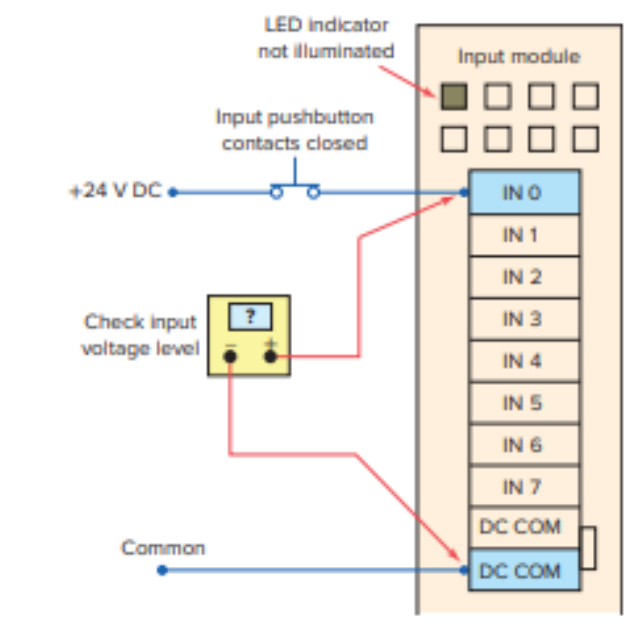


Figure 13-20 Checking for input malfunctions.

Input device troubleshooting guide

Input device condition	Input module status indicator	Monitor display status indicator		Possible fault(s)
Closed — ON 24 V DC input	ON	True	False	None - correct indications
Open — OFF 0 V DC input	OFF	False	True	None - correct indications
Closed — ON 24 V DC input	ON	False	True	Sensor condition, input voltage, status indicator are correct. Ladder instructions have incorrect indications. Input module or processor fault.
Closed — ON 0 V DC input	OFF	False	True	Status indicator and instructions agree but not with the sensor condition. Open field device or wiring.
Open — OFF 0 V DC input	OFF	True	False	Sensor condition, input voltage, status indicator are correct. Ladder instructions have incorrect indications. Input module or processor fault.
Open — OFF 24 V DC input	ON	True	False	Input voltage, status indicator, and ladder instructions agree but not with sensor condition. Short circuit in the field device or wiring.

Figure 13-21 Input troubleshooting guide.

Troubleshooting

Input Malfunction

- If programming device monitor doesn't display correct status, input module might not convert signal properly. Replace input module in this case.
- If a replacement module does not eliminate the problem and wiring is assumed to be correct, then the I/O rack, communication cable, or processor should be suspected.

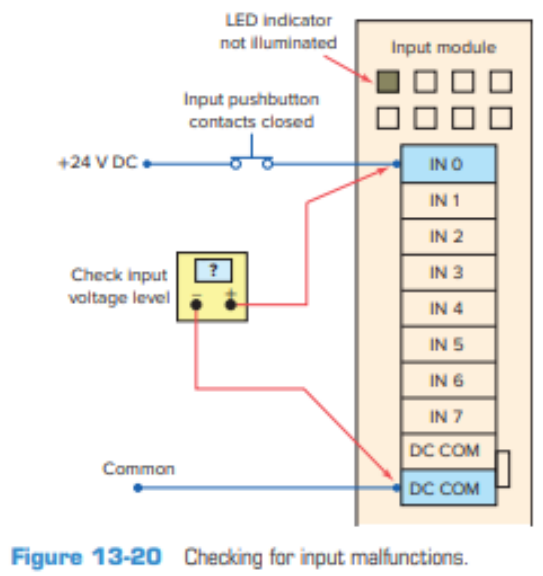


Figure 13-20 Checking for input malfunctions.

Input device troubleshooting guide

Input device condition	Input module status indicator	Monitor display status indicator		Possible fault(s)
Closed — ON 24 V DC input	ON	True	False	None - correct indications
Open — OFF 0 V DC input	OFF	False	True	None - correct indications
Closed — ON 24 V DC input	ON	False	True	Sensor condition, input voltage, status indicator are correct. Ladder instructions have incorrect indications. Input module or processor fault.
Closed — ON 0 V DC input	OFF	False	True	Status indicator and instructions agree but not with the sensor condition. Open field device or wiring.
Open — OFF 0 V DC input	OFF	True	False	Sensor condition, input voltage, status indicator are correct. Ladder instructions have incorrect indications. Input module or processor fault.
Open — OFF 24 V DC input	ON	True	False	Input voltage, status indicator, and ladder instructions agree but not with sensor condition. Short circuit in the field device or wiring.

Figure 13-21 Input troubleshooting guide.

Troubleshooting

Input Malfunction

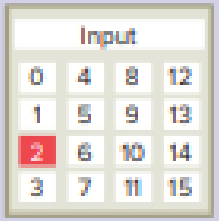
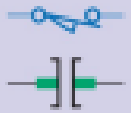
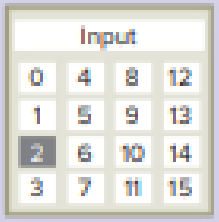
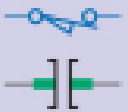
If Your Input Circuit LED Is . . .	And Your Input Device Is . . .	And	Probable Cause
ON 	On/Closed/Activated 	Your input device will not turn off.	Device is shorted or damaged.
		Your program operates as though it is off.	Input circuit wiring or module.
			Input is forced off in program.
	Off/Open/Deactivated 	Your program operates as though it is on and/or the input circuit will not turn off.	Input device off-state leakage current exceeds input circuit specification.
			Input device is shorted or damaged.
			Input circuit wiring or module.
OFF 	On/Closed/Activated 	Your program operates as though it is off and/or the input circuit will not turn on.	Input circuit is incompatible.
			Low voltage across the input.
			Input circuit wiring or module.
			Input signal turn-on time too fast for input circuit.
	Off/Open/Deactivated 	Your input device will not turn on.	Input device is shorted or damaged.
		Your program operates as though it is on.	Input is forced on in program.
			Input circuit wiring or module.

Figure 13-31 Input troubleshooting guide.

Troubleshooting

Output Malfunction

In addition to the logic indicator, some output modules incorporate a blown fuse indicator or a power indicator.

- Check output module blown fuse indicator if output doesn't energize.
- Indicator lights up when corresponding output circuit has blown fuse.
- If illuminated, fix malfunction cause and replace blown fuse in module.

Output device troubleshooting guide

Output device condition	Output module status indicator	Monitor display status indicator	Fault(s)
Energized — ON	ON	True	None - correct indication
De-energized — OFF	OFF	False	None - correct indication
De-energized — OFF	ON	True	Output instruction and status indicator agree but the field device does not. Open field device or wiring. Module circuit or fuse.
De-energized — OFF	OFF	True	Field device status and status indicator agree but the output condition does not. Module circuit or fuse.

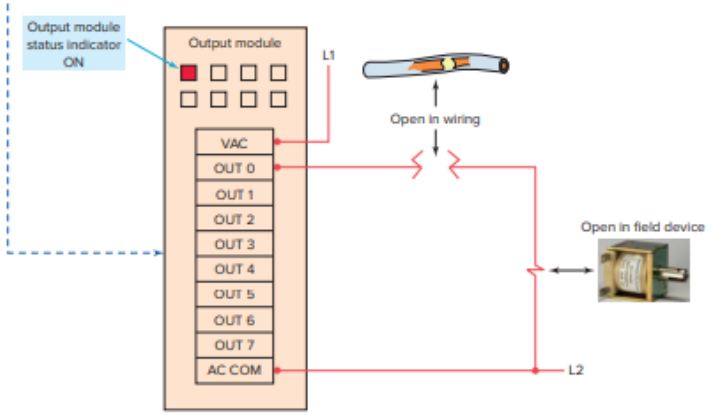


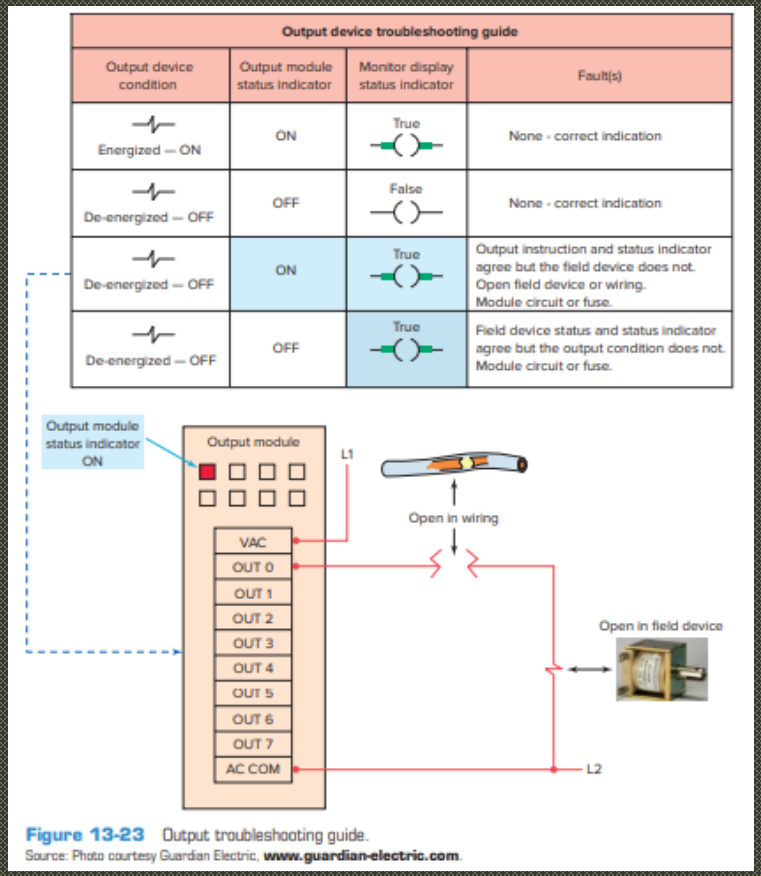
Figure 13-23 Output troubleshooting guide.
Source: Photo courtesy Guardian Electric, **www.guardian-electric.com**.

Frank D. Petruzella Programmable Logic Controllers 5th edition

Troubleshooting

Output Malfunction

- Output module's status LED indicates when its logic circuitry recognizes a command from the processor to turn on.
- If the blown fuse indicator isn't lit (fuse OK), check if the output device responds to the LED status indicator.
- If an output rung is activated, the module status indicator is on, and the output device doesn't respond, suspect either the wiring or the output device itself.
- If an output rung is activated, but the status indicator is off, then the output module or processors may be at fault.



Output device troubleshooting guide

Output device condition	Output module status indicator	Monitor display status indicator	Fault(s)
Energized — ON	ON	True	None - correct indication
De-energized — OFF	OFF	False	None - correct indication
De-energized — OFF	ON	True	Output instruction and status indicator agree but the field device does not. Open field device or wiring. Module circuit or fuse.
De-energized — OFF	OFF	True	Field device status and status indicator agree but the output condition does not. Module circuit or fuse.

Figure 13-23 Output troubleshooting guide.
Source: Photo courtesy Guardian Electric, **www.guardian-electric.com**.

HUMBER

Troubleshooting

Output Malfunction

- Some digital outputs have internal electronic fusing to prevent excess current, protecting the module from damage.
- Other modules require external fusing.
- Modules with electronic fusing protect output points from excessive current surge. If too much current flows through a point, the fuse trips, sending a point-level fault to the controller, with a corresponding tag for examination in case of a fault.

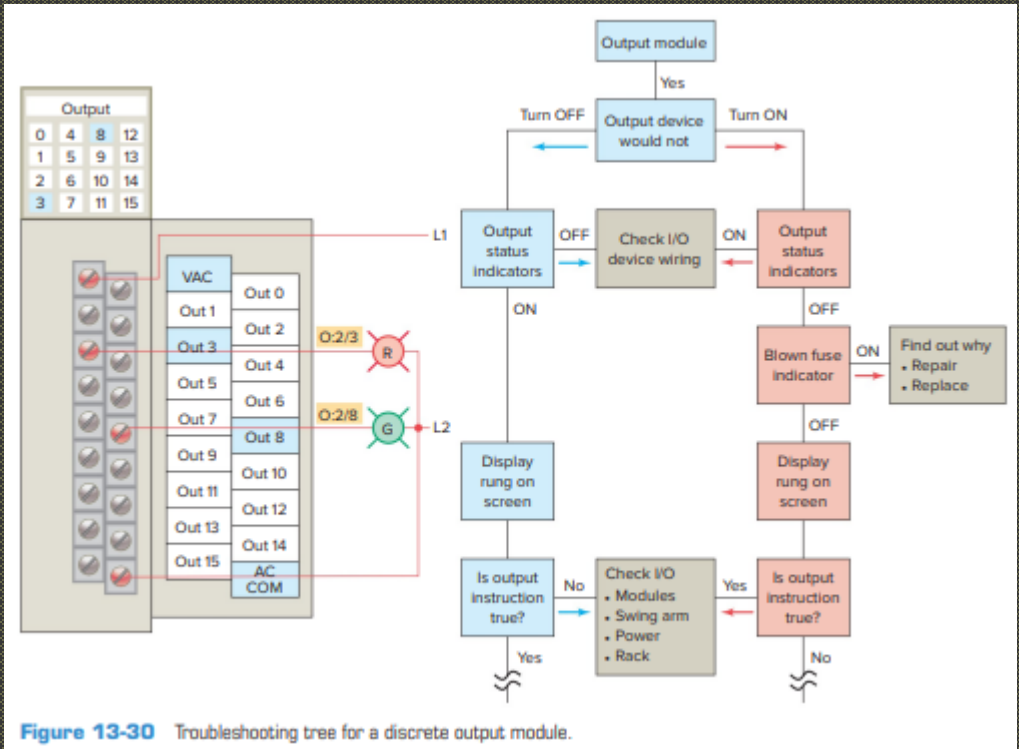


Figure 13-30 Troubleshooting tree for a discrete output module.

Frank D. Petruzella Programmable Logic Controllers 5th edition

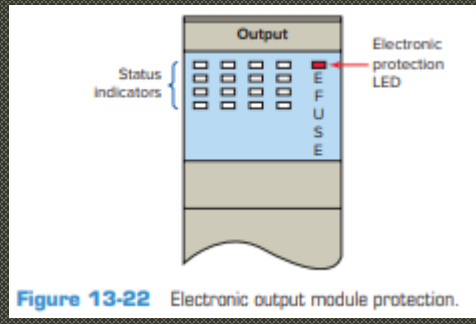


Figure 13-22 Electronic output module protection.

https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um058_-en-p.pdf

HUMBER

Troubleshooting

Output Malfunction

If Your Output Circuit LED Is . . .	And Your Output Device Is . . .	And	Probable Cause
ON Output: 0 4 8 12 / 1 5 9 13 / 2 6 10 14 / 3 7 11 15	On/Energized	Your program indicates that the output circuit is off or the output circuit will not turn off.	Programming problem: - Check for duplicate outputs and addresses. - If using subroutines, outputs are left in their last state when not executing subroutines. - Use the force function to force output off. If this does not force the output off, output circuit is damaged. If the output does force off, then check again for logic/programming problem.
			Output is forced on in program.
			Output circuit wiring or module.
	Off/De-energized	Your output device will not turn on and the program indicates that it is on.	Low or no voltage across the load.
			Output device is incompatible: check specifications and sink/source compatibility (if dc output).
			Output circuit wiring or module.
OFF Output: 0 4 8 12 / 1 5 9 13 / 2 6 10 14 / 3 7 11 15	On/Energized	Your output device will not turn off and the program indicates that it is off.	Output device is incompatible.
			Output circuit off-state leakage current may exceed output device specification.
			Output circuit wiring or module.
			Output device is shorted or damaged.
	Off/De-energized	Your program indicates that the output circuit is on or the output circuit will not turn on.	Programming problem: - Check for duplicate outputs and addresses. - If using subroutines, outputs are left in their last state when not executing subroutines. - Use the force function to force output on. If this does not force the output on, output circuit is damaged. If the output does force on, then check again for logic/programming problem.
			Output is forced off in program.
			Output circuit wiring or module.

Figure 13-32 Output troubleshooting guide.

INPUT AND OUTPUT FORCING

- Ability to Override Inputs and Outputs:
  - Useful for testing purposes.

- Input Force:
  - Useful when PLC isn't connected to physical input devices.
  - Temporarily bypasses input device.
  - Overrides actual input status with value in force table.

- Output Force:
  - Temporarily sets output to desired state for testing.
  - Should be used temporarily until logic is corrected.
  - Overrides actual output device status with value in force table.

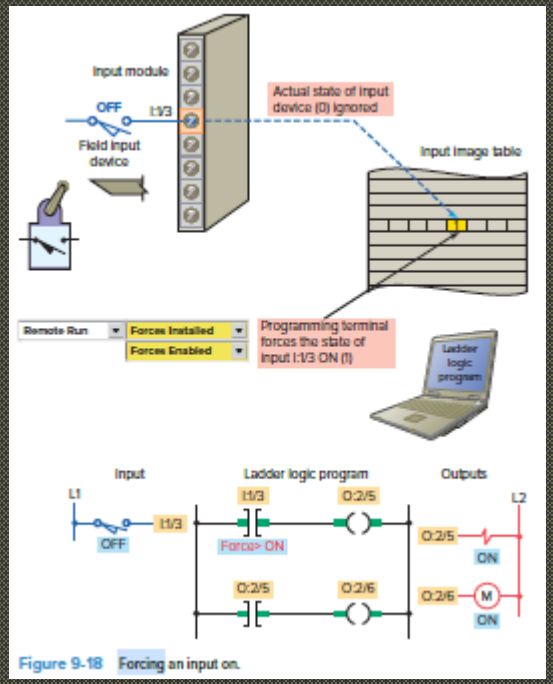


Figure 9-18 Forcing an input on.

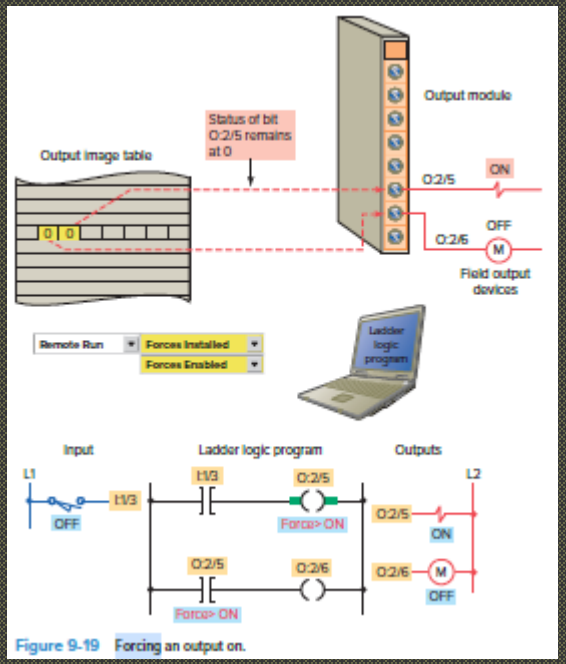


Figure 9-19 Forcing an output on.

Troubleshooting

Analog Modules

Troubleshooting analog modules is usually more difficult than for discrete modules because they do not have indication to analog channel voltage or current.

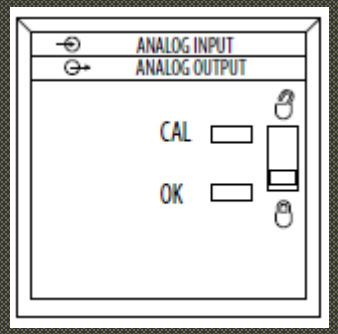


Table 13 - Status Indicators for Input Modules

Indicator	Status	Description
OK	Steady green	The inputs are being multicast and in normal operating state. The outputs are in Run mode.
OK	Flashing green	The module has passed internal diagnostics but is not currently performing connected communication or is in Program mode. Inputs are in a normal operating state. Outputs are in the configured state for Program mode.
OK	Flashing red	Previously established communication has timed out. Check controller and chassis communication.
OK	Steady red	The module must be replaced. Replace the module.
CAL	Flashing green	The module is in Calibration mode.

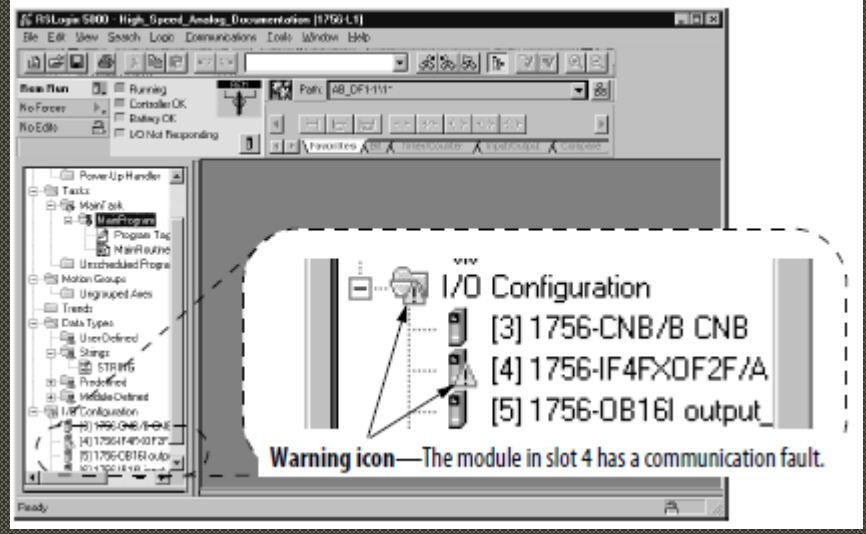
Troubleshooting

Analog Modules

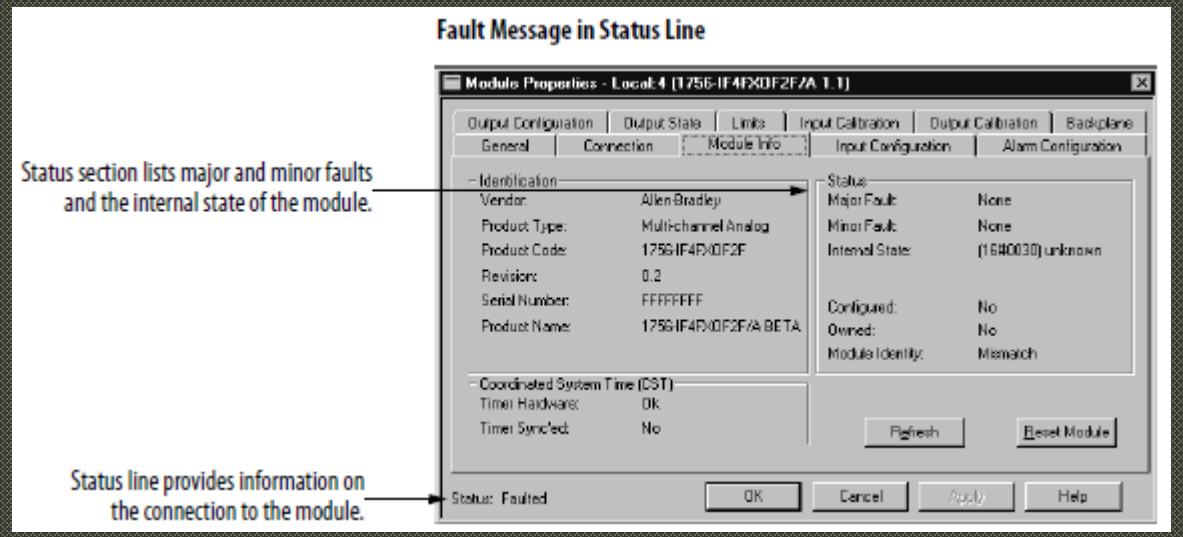
In addition to module status indicators, the application alerts about the fault conditions in the ways below:

- Warning icon next to module in I/O Configuration tree
- Status on Module Info page
- Fault message in status line
- Notification in tag editor

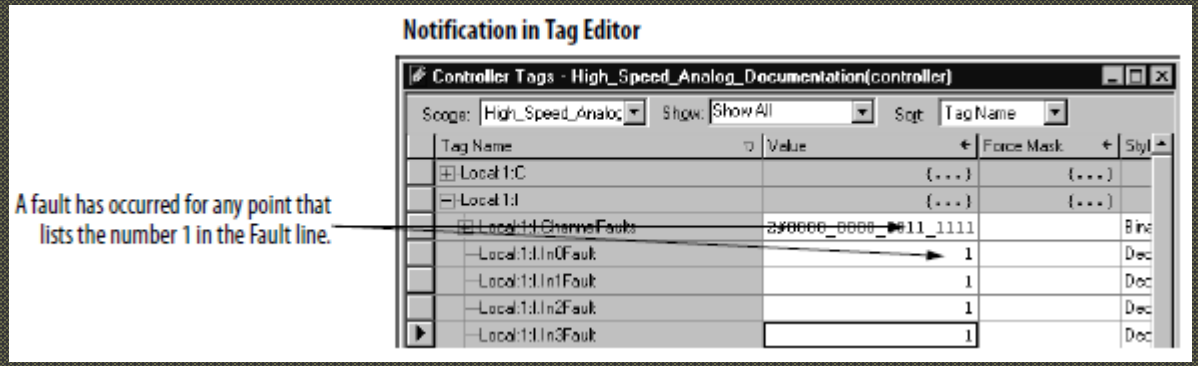
Warning Signal in I/O Configuraton Tree



Fault Message in Status Line



Notification in Tag Editor



HUMBER

COMMUNICATION PROBLEMS

Communication problems between personal computer and a PLC.

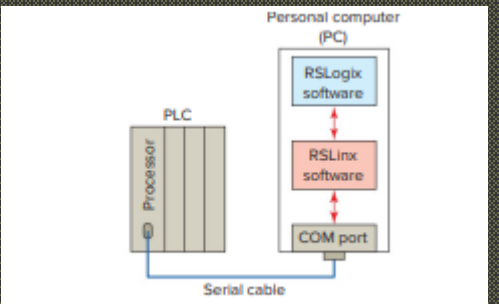


Figure 13-35 Direct PC-to-PLC software connection.

A PC is connected to the PLC with a USB or serial (RS-232) cable or through a communication network (Ethernet, Data Highway+, Modbus+, Profibus etc.).

Depending on the vender, the software connection between the programming software to the USB/serial port may be:

- Direct or Through a communication server (RSLinx – Rockwell Automation).
- USB connection problems are related to the PC USB driver.
- Serial cable problems involve either the cable or the configuration of PC serial port (Baud rate, Parity, Number of stop bits, etc).
- To check for a disabled port, try communication to the PLC through another communication port, say Ethernet.

Programming Safety considerations

Safety considerations should be developed as part of the PLC program.

- Motor Starter Auxiliary Seal-In Contact:
  - Substitute for programmed contact in PLCs.
  - Provides positive feedback to processor about motor status.
- Field-Generated Starter Auxiliary Contact:
  - More expensive in terms of wiring and hardware.
  - Safer due to accurate motor status feedback.
- Example Scenario:
  - If OL contact of starter opens due to overload:
    - Motor stops due to lost power to starter coil.
    - If program uses examine-on contact instruction:
      - Processor doesn't detect power loss to motor.
      - Motor may restart instantly upon OL reset, creating unsafe condition.

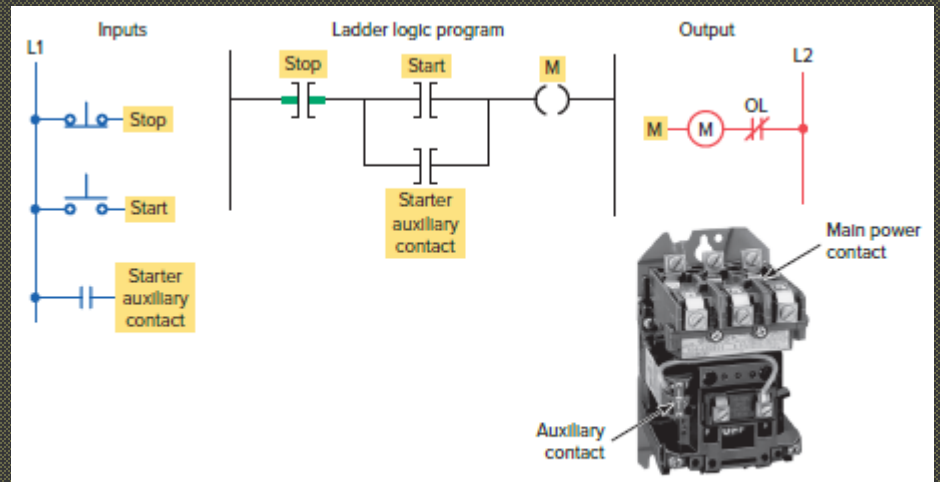


Figure 9-22 Motor starter programmed using the starter auxiliary seal-in contact.
Source: Image Courtesy of Rockwell Automation, Inc.

Programming Safety considerations

Safety considerations should be developed as part of the PLC program.

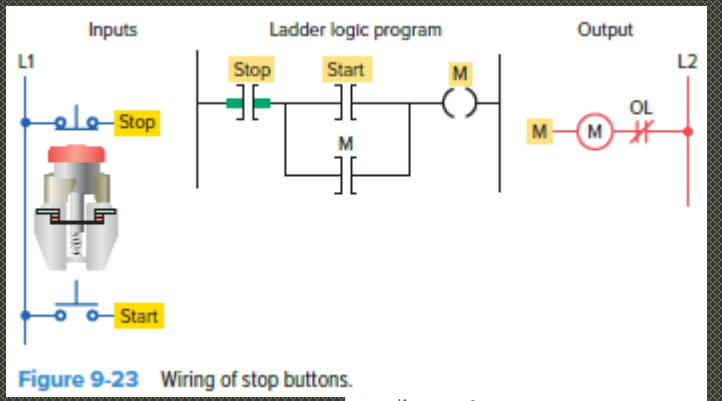


Figure 9-23 Wiring of stop buttons.

- Wiring of Stop Buttons:
  - Stop buttons serve both safety and operational functions.
  - Wired using normally closed contact programmed to examine for an on condition.
  - Using normally open contact programmed to examine for an off condition is less safe.

- Concern with Normally Open Contact:
  - If circuit between button and input point breaks:
    - Stop button can be depressed indefinitely, but the PLC logic can't react to stop command.

- Effect of Power Loss on Stop Button in Control Circuit:
  - Normally closed wiring keeps input point powered unless stop function activated.
  - Loss of power to stop button control circuit or faults in wiring simulate intentional stop.

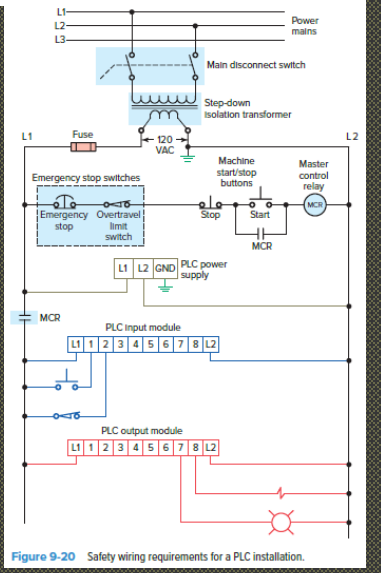


Figure 9-20 Safety wiring requirements for a PLC installation.

Programming Safety considerations

Safety considerations should be developed as part of the PLC program.

- Fault Routines in PLCs:
  - Used to handle errors and execute subroutines in response to faults.
  - PLC's fault handling capability assessed by how it informs users and available alternatives.

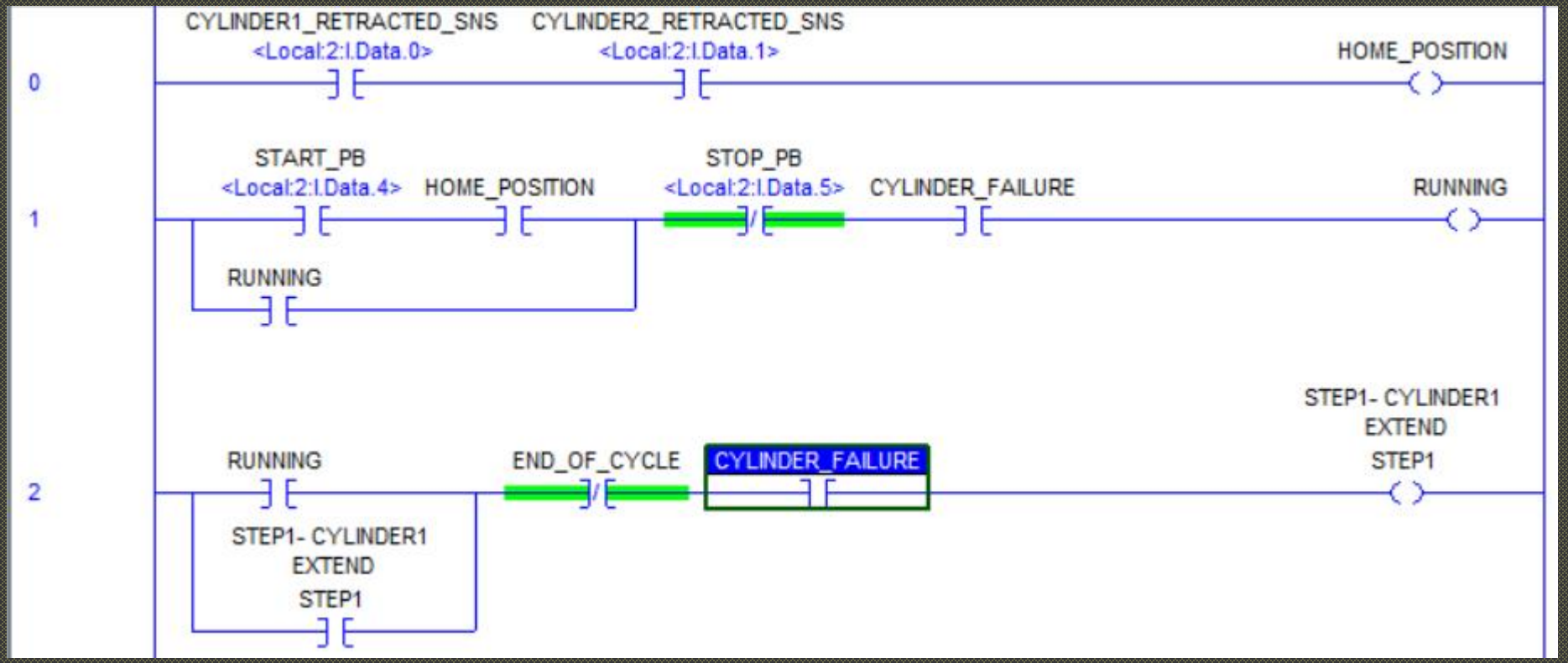
- Processor Response to Major Faults (recoverable and non-recoverable faults):
  - Processor checks for fault routine.
  - If routine exists, executes it; if not, shuts down.

- Handling of Recoverable Faults:
  - If fault routine exists, executes it.
- Handling of Non-recoverable Faults:
  - Fault routine scanned once then shuts down.

- Role of Fault Routine:
  Allows orderly shutdown in case of faults.

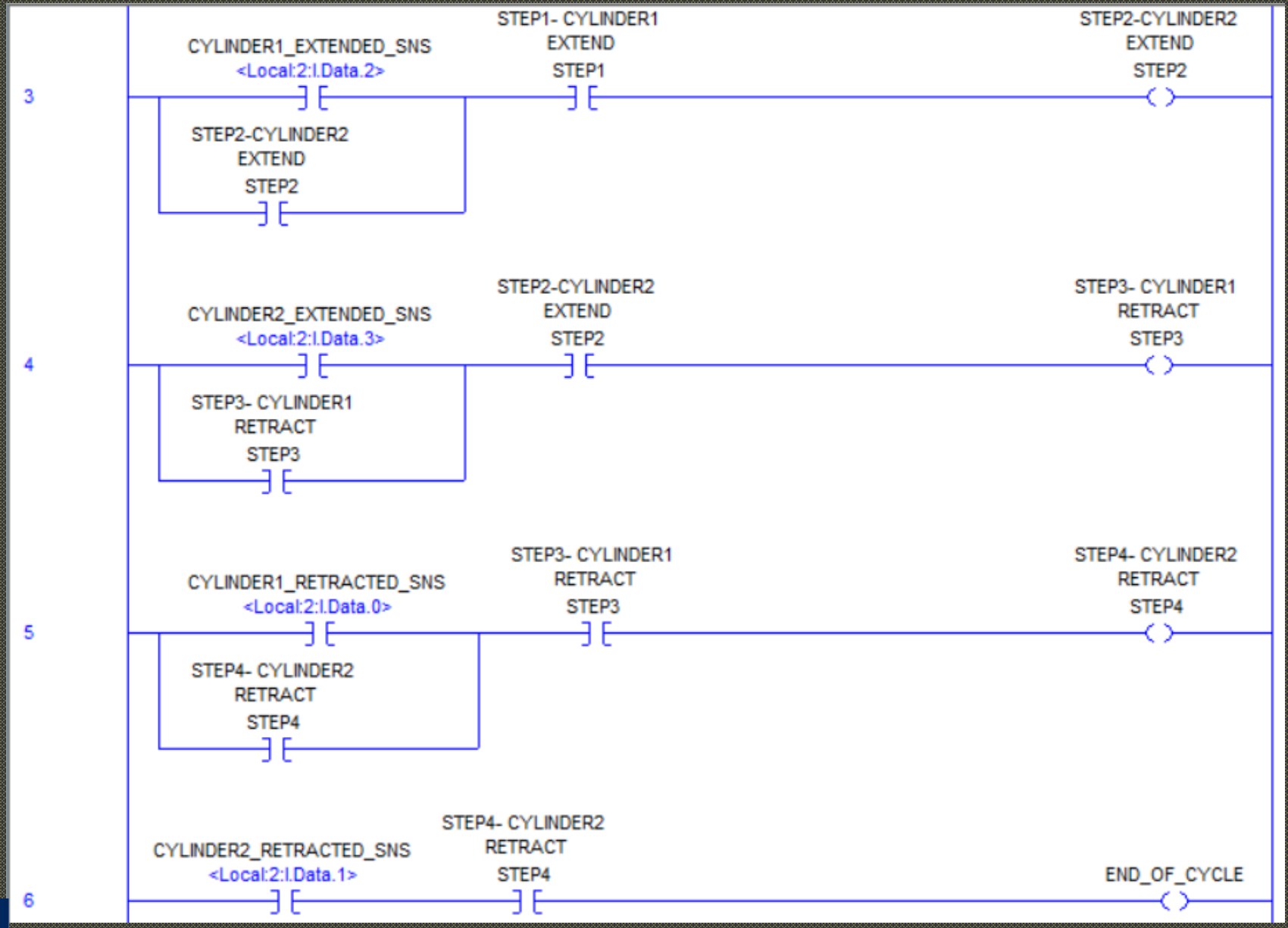
EQUIPMENT FAULT DIAGNOSTICS

Case study: Two cylinders, both controlled by double solenoids, cycle in the following sequence: cylinder1 extend, cylinder 2 extend, cylinder1 retract, cylinder 2retract.
Each motion takes 1 second.
Write the diagnostics for all 4 motions.



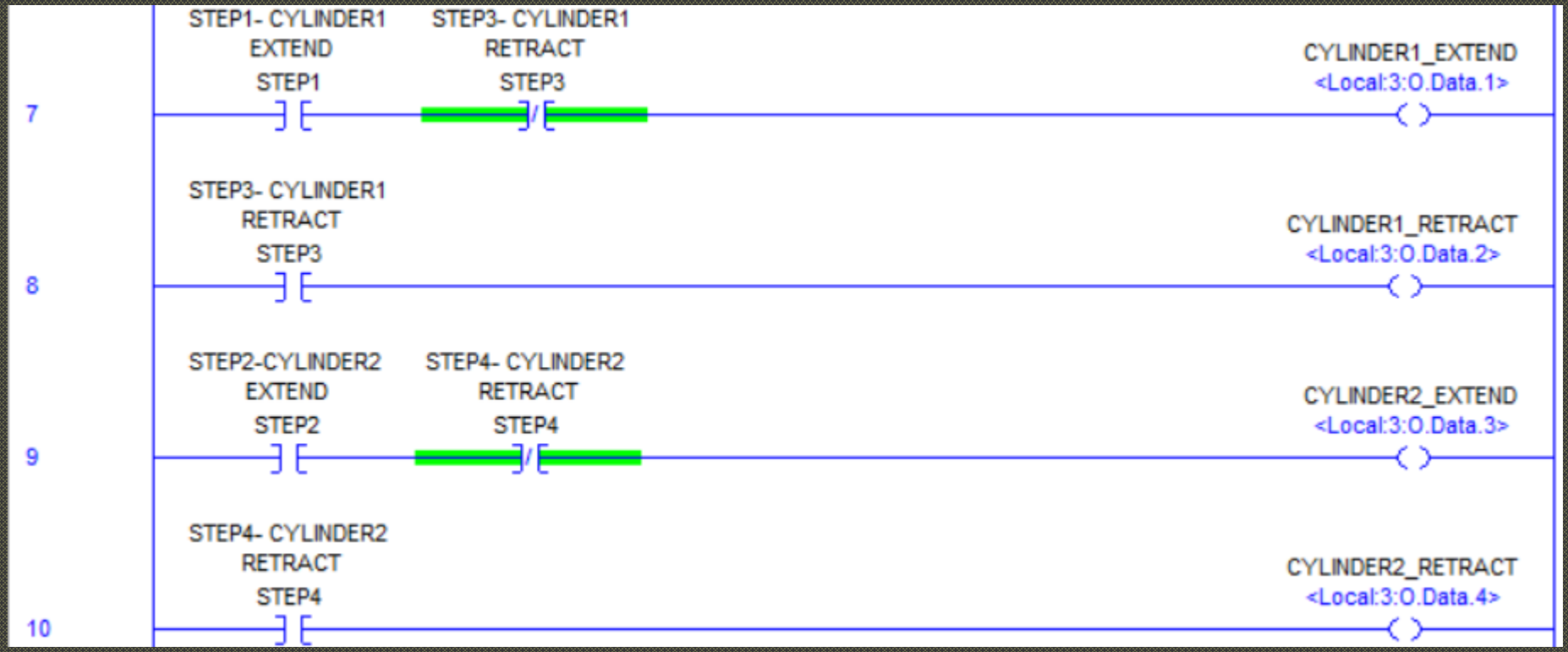
HUMBER

EQUIPMENT FAULT DIAGNOSTICS



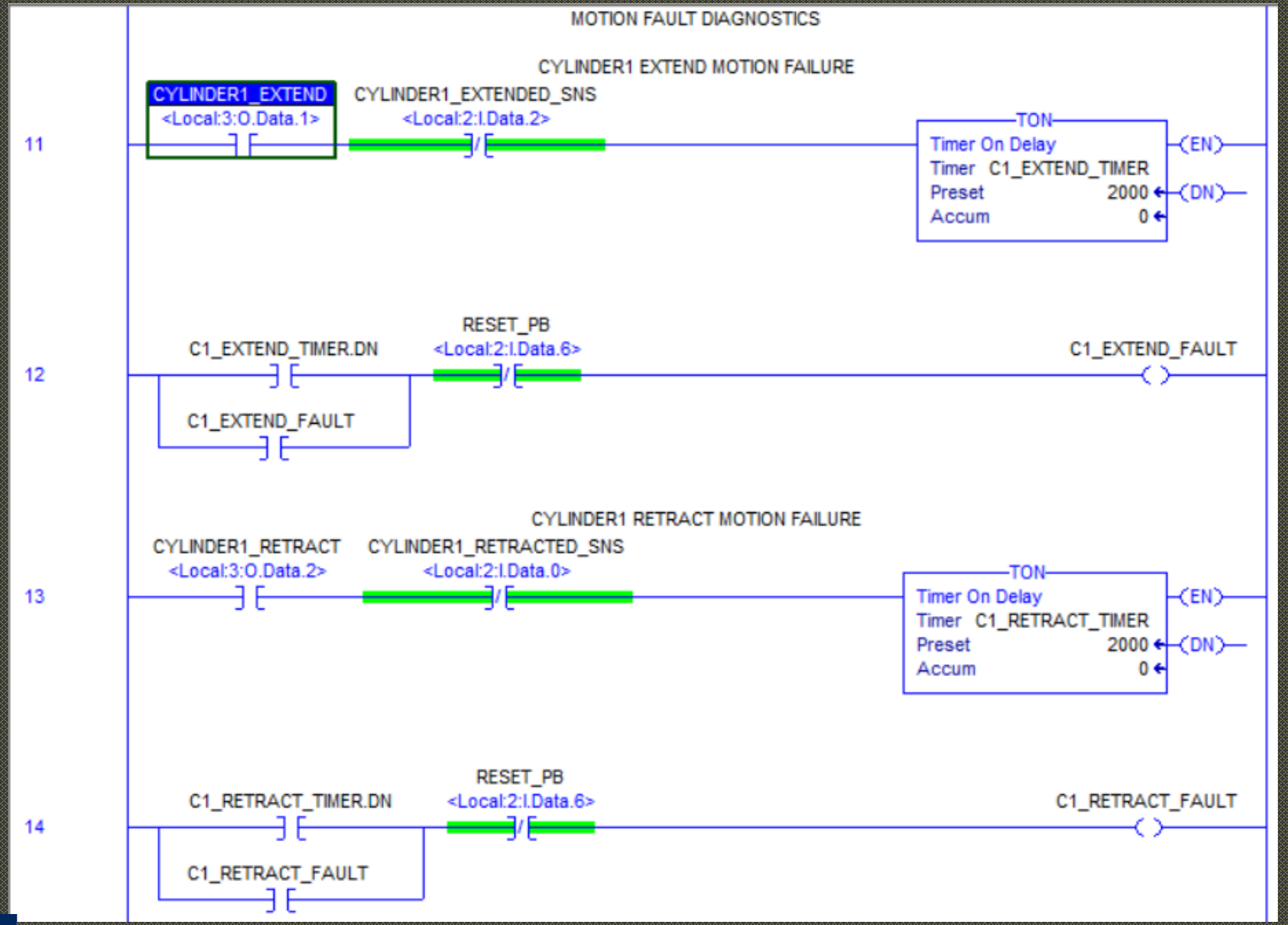
HUMBER

EQUIPMENT FAULT DIAGNOSTICS



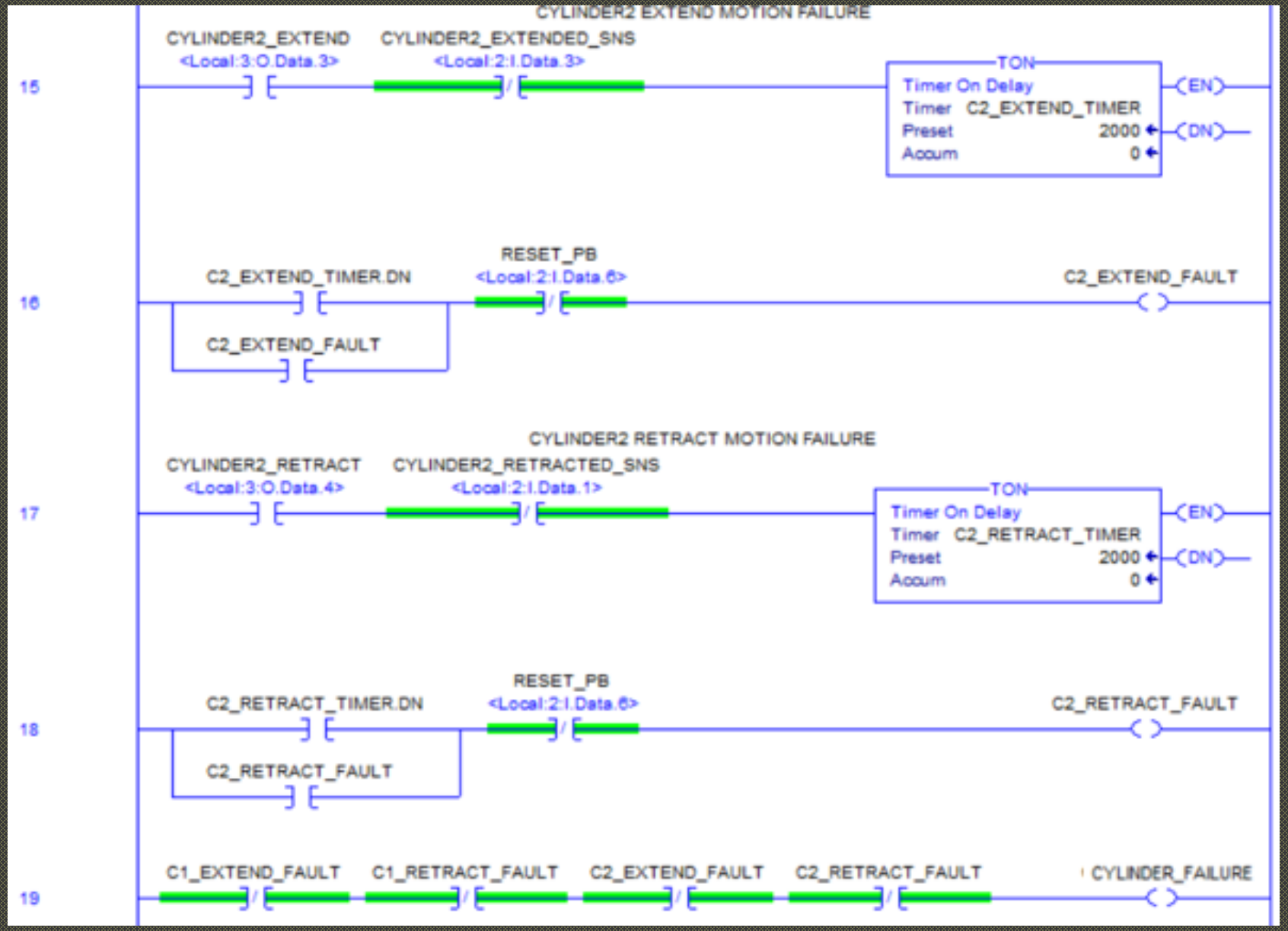
HUMBER

EQUIPMENT FAULT DIAGNOSTICS



HUMBER

EQUIPMENT FAULT DIAGNOSTICS



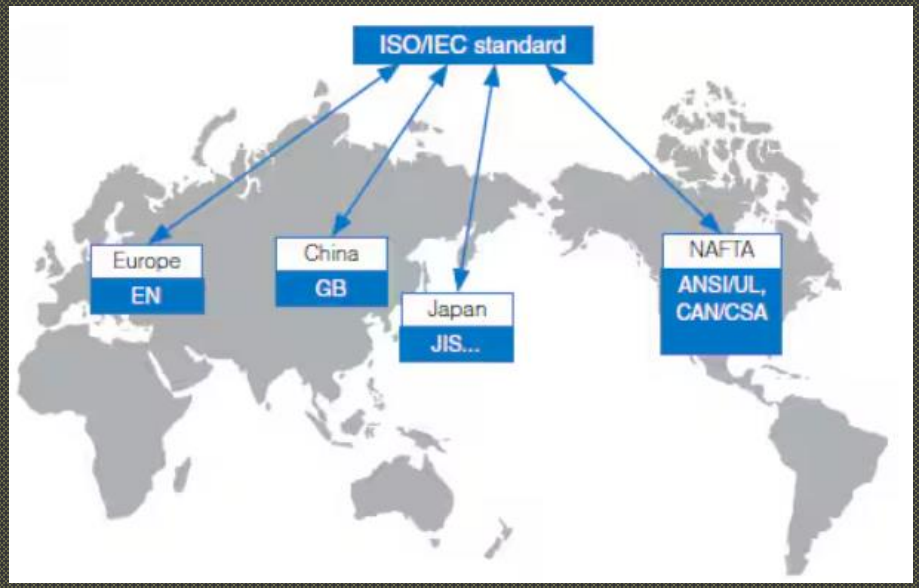
HUMBER

SAFETY STANDARDS

ISO 13849-1:2006

- Standard for Safety-Related Machinery Control Systems
  - One of two international standards for safety in control systems.
- Transition from Hardwired to Software-Based Safety
  - Shift from mechanical devices (relays) to electronic components (transistors, MOS-FETs).
- Focus on System Architecture
  - Earlier, safety was based on system design rather than individual component reliability.
- Regulatory Shift Around 2000
  - Emphasis on both functionality and reliability in safety standards.
- Integration with IEC Standards
  - Builds on ISO 13849-1:1999.
  - Incorporates functional safety principles from IEC 61508 and IEC 62061.

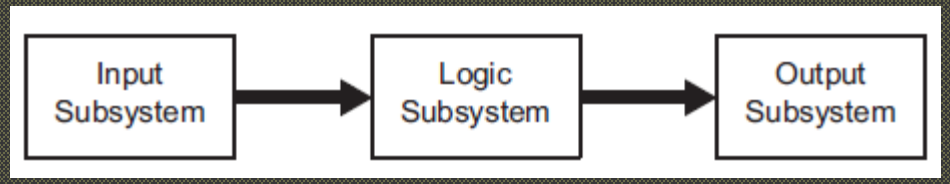
- ISO - International Organization for Standardization
  - Standards for a wide range of industries.
- IEC - International Electrotechnical Commission
  - Standards for electrical and electronic related technologies.

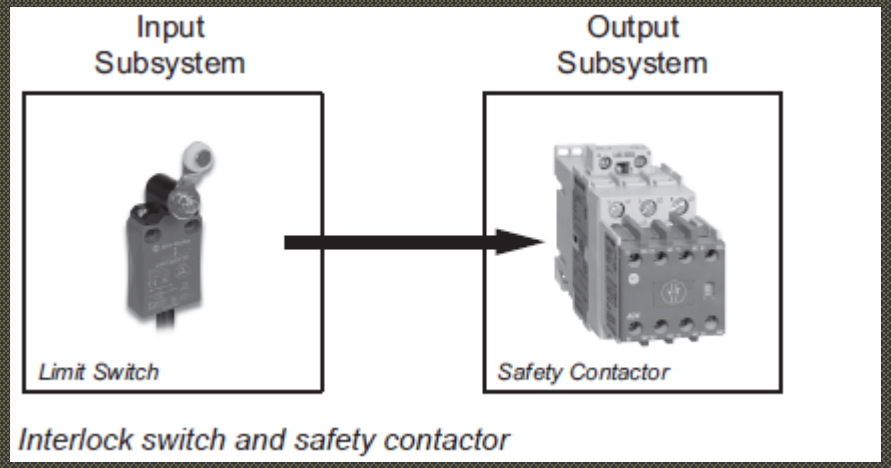


https://www.keyence.ca/ss/products/safetyknowledge/introduction/

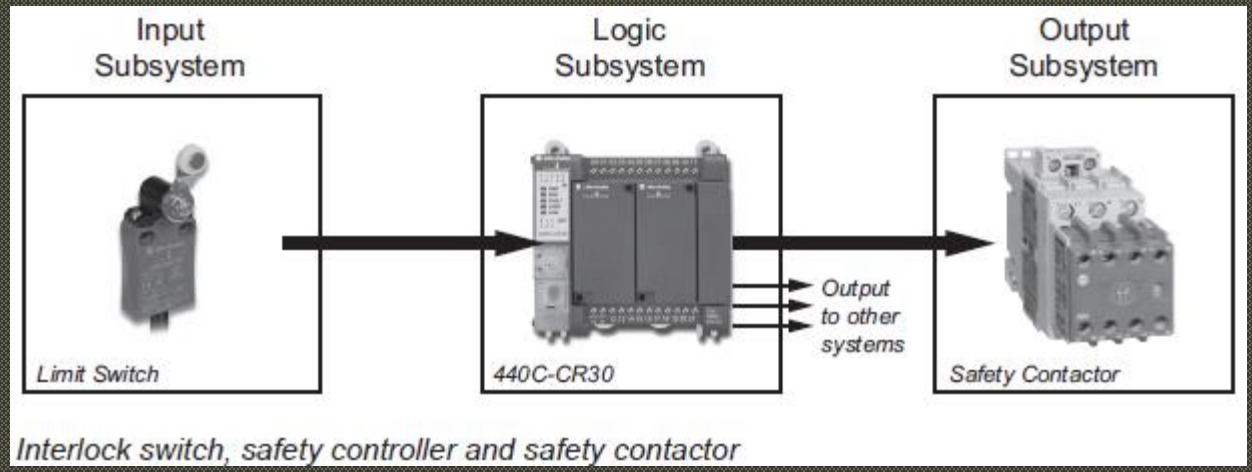
SYSTEMS STRUCTURE

- Any system can be split into basic system components or “subsystems.”
- Most systems can be split into three basic functions; input, logic solving and output
- Some simple systems may not have logic solving.





Interlock switch and safety contactor

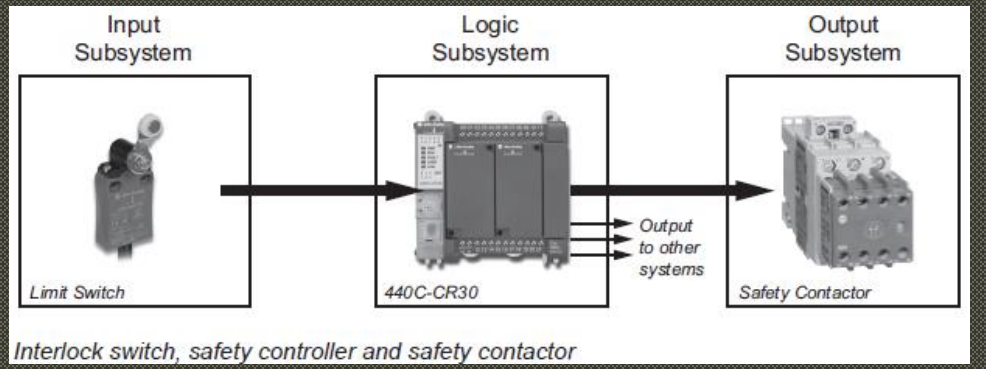


Interlock switch, safety controller and safety contactor

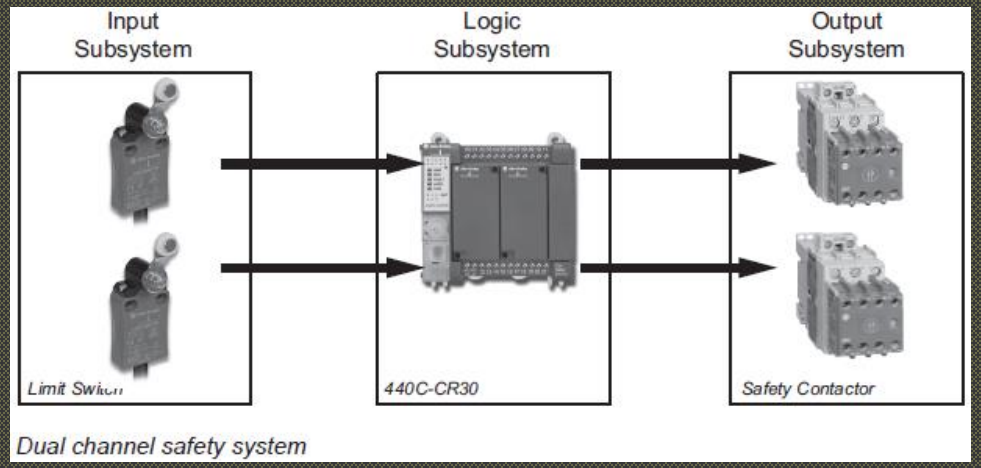
A simple single channel electrical system comprises only input and output subsystems.

SYSTEMS STRUCTURE

- The Single Channel System requires some logic.
- The safety controller itself will be fault tolerant (dual channel) internally.
- The overall system is still limited to single channel status due to:
  - single limit switch and single contactor subsystems
- A single channel system will fail if one of its single channel subsystems fails; it is not “fault tolerant”.



Interlock switch, safety controller and safety contactor



Dual channel safety system

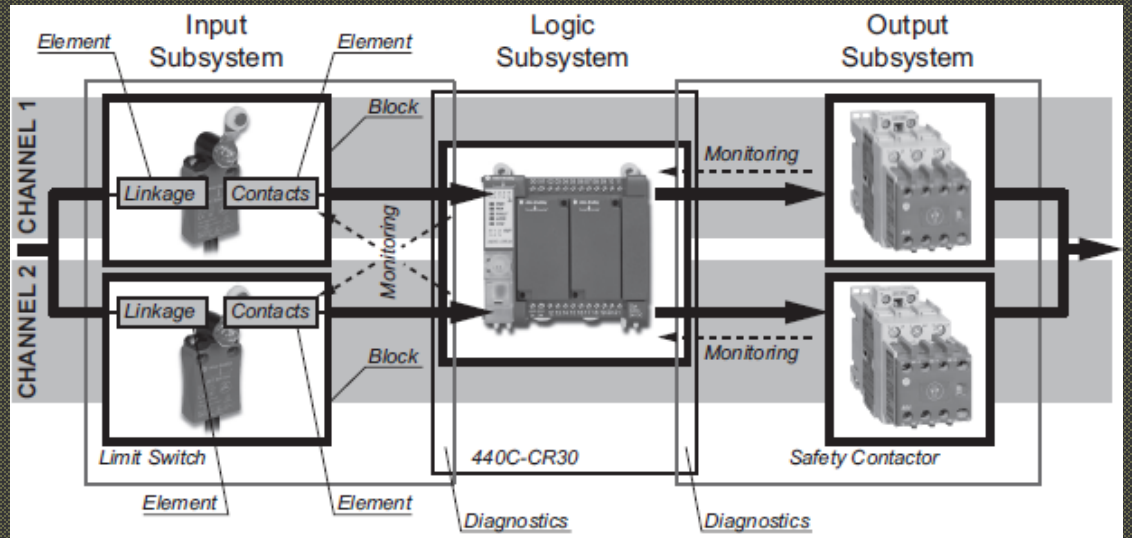
A dual channel "fault-tolerant" system provides:

- Two independent channels ensure fault tolerance.
- Continues functioning after a single fault in one channel.
- System failure occurs only if both channels fail.
- Safer than a single-channel system, reducing the risk of dangerous failures.

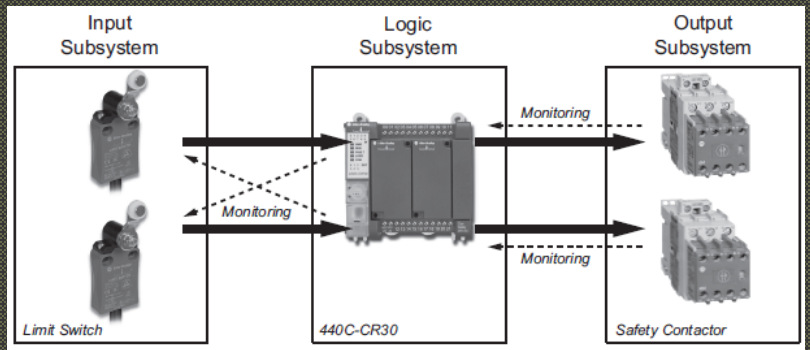
Fault tolerance is the ability of a system to maintain its functionality despite failures or malfunctions

SYSTEMS STRUCTURE

- The following diagram shows the inclusion of diagnostic measures achieved by monitoring techniques.
- Diagnostic measures improve fault detection, making the system more reliable in terms of safety function.
- Detecting a fault will require taking corrective action to restore the system to a safe state.



Subdivided system with diagnostics with a dual channel safety system

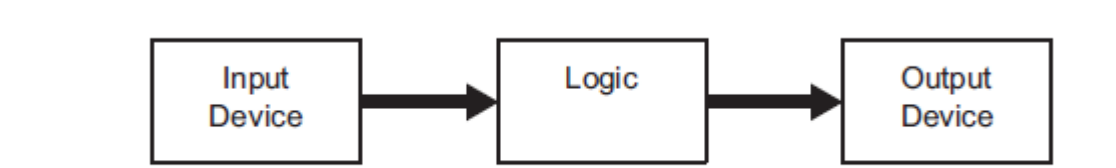


Diagnostics with a dual channel safety system

Systems typically consist of two channels in each subsystem, referred to as "blocks" in the standard.

DESIGNATED ARCHITECTURE CATEGORIES – CAT 1

Basic safety measures, usually with single-channel systems, suitable for low-risk situations.



Designated Architecture Category 1

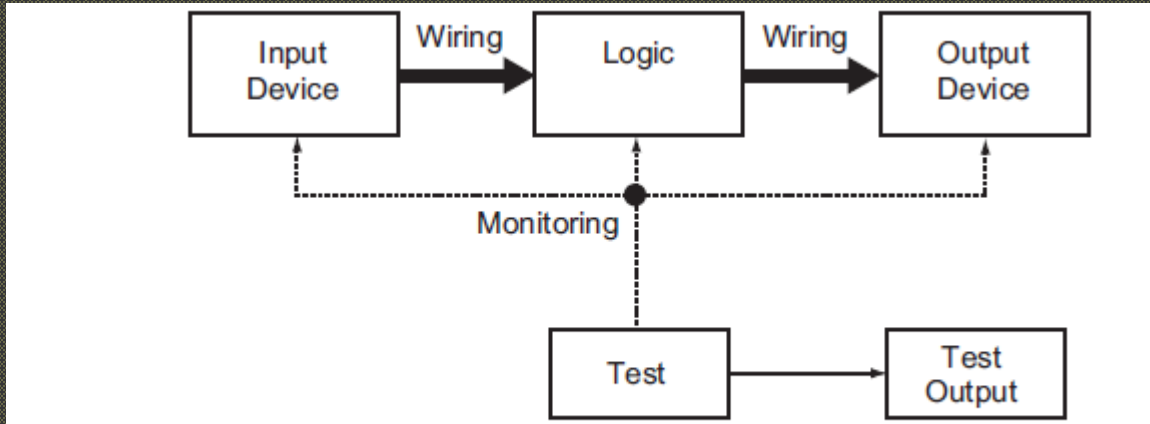
A graphical representation of conceptual requirements consists of:

- Input Device: Emergency Stops, safety mats, safety gates, two hand control
- Logic: Safety relays or safety PLCs
- Output device: Motor contactors, valves

Designated Architecture Category 1 must use basic safety principles (annexes of ISO 13849-2). The system or subsystem can fail in the event of a single fault.

DESIGNATED ARCHITECTURE CATEGORIES – CAT 2

May include some basic fault detection mechanisms but still considered a relatively low level of safety.

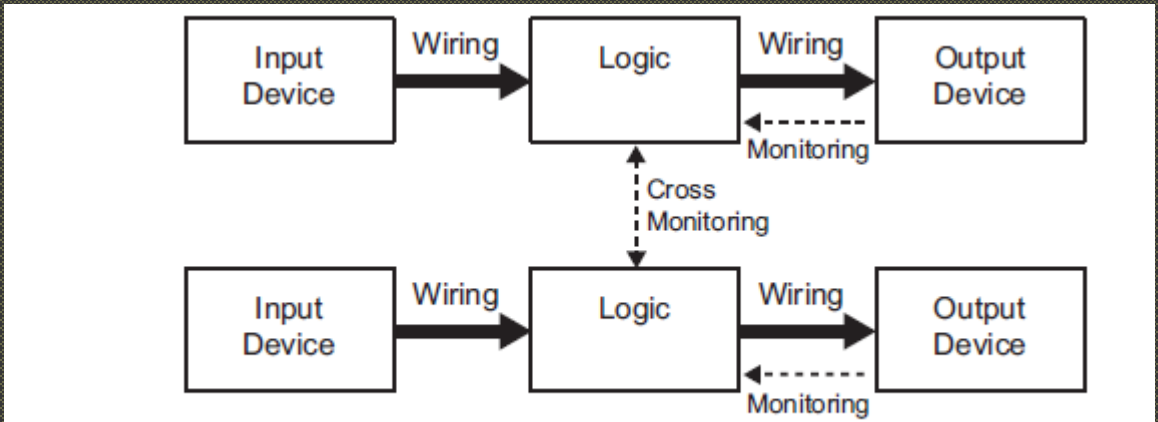


Designated Architecture Category 2

- Requires basic safety principles and diagnostic monitoring through functional tests.
- Tests occur at startup and periodically to detect faults.
- A single fault can still cause failure, but the risk is lower than in Category 1.

DESIGNATED ARCHITECTURE CATEGORIES – CAT 3

Typically uses redundant circuits or monitoring systems to detect faults, providing greater safety than Category 2.



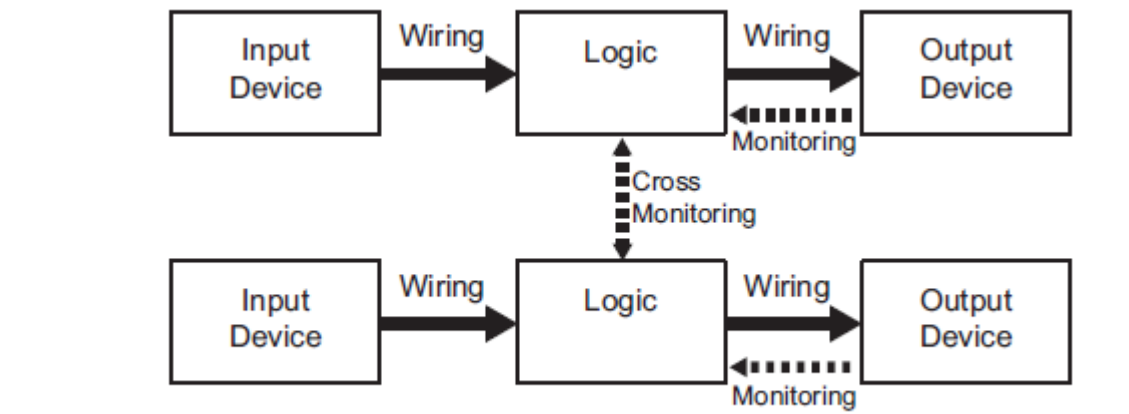
Designated Architecture Category 3

- Must follow basic safety principles to ensure the system/subsystem does not fail from a single fault.
- Requires single fault tolerance, usually through dual-channel architecture.
- Single faults should be detected whenever possible.

DESIGNATED ARCHITECTURE CATEGORIES – CAT 4

The Category 4 is the Highest Level of Safety:

- Ensures maximum fault tolerance and system reliability.
- Incorporates highly reliable redundant systems.
- Uses advanced fault detection and diagnostics.
- Follows Category 3 requirements with higher diagnostic coverage.
- Detects all single dangerous faults and their combinations.
- Prevents fault accumulation through enhanced monitoring and diagnostics.

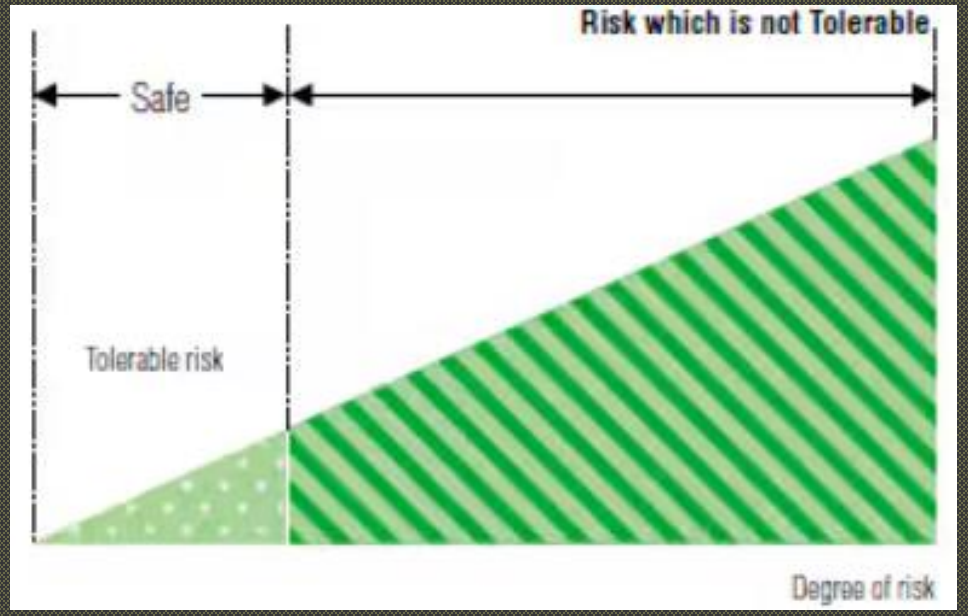


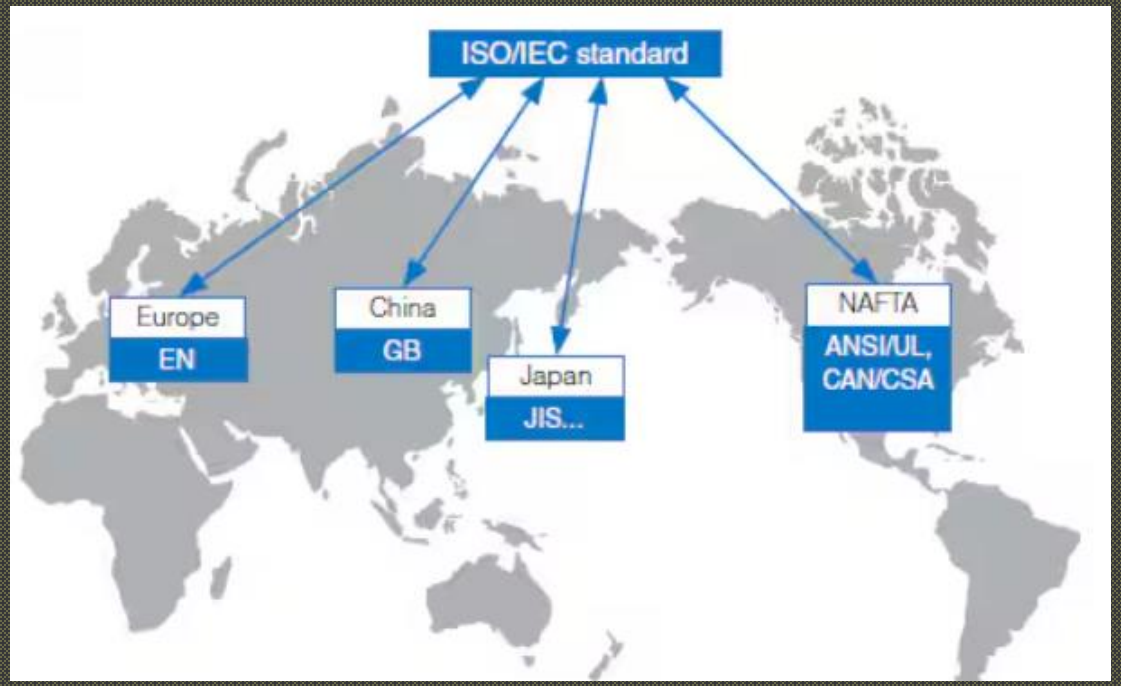
Designated Architecture Category 4

SAFETY STANDARDS

ISO/IEC Guide 51 Overview:

- Provides guidelines for incorporating safety aspects into standards.
- Applies to safety concerns related to people, property, and the environment.
- Defines safety as "freedom from risk which is not tolerable."
- Emphasizes achieving safety through risk reduction to a tolerable level.



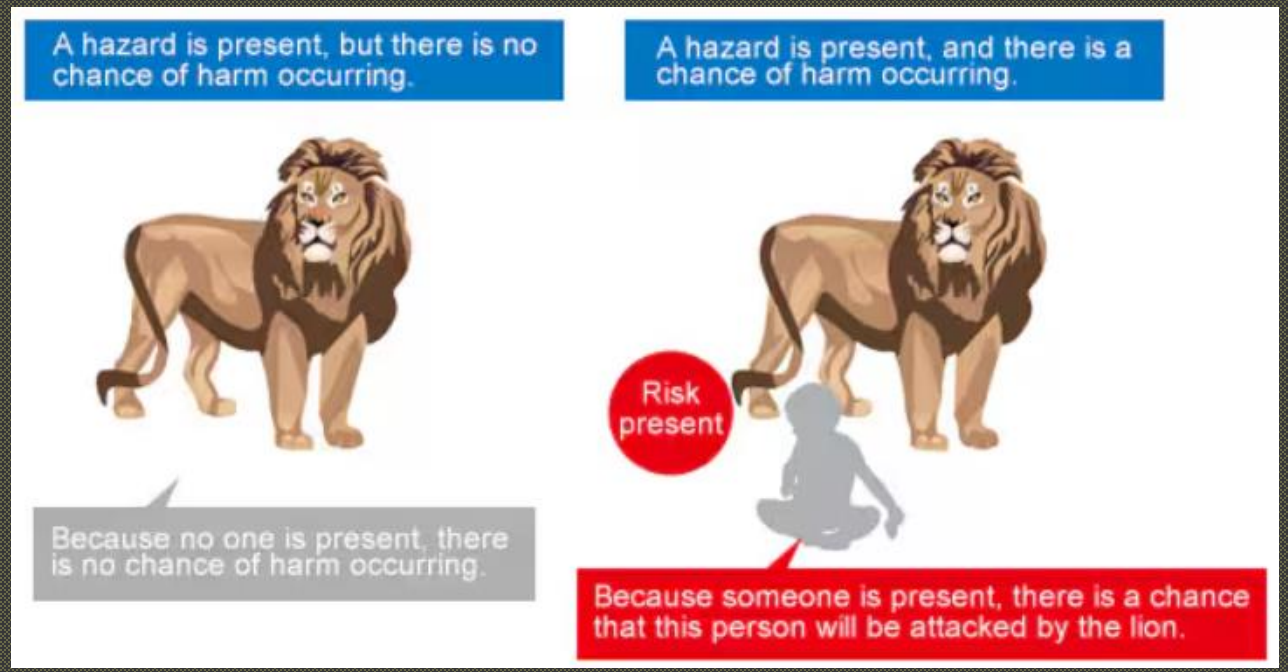


https://www.keyence.ca/ss/products/safetyknowledge/introduction/

SAFETY STANDARDS

- Risk is defined as the “combination of the probability of occurrence of harm and the severity of that harm.”
  - Risk = Severity of harm × the probability of the occurrence of harm

- Safety is defined as “freedom from risk which is not tolerable“.
  - In other words, tolerable risk is still present even when considered “safe”



“risk” exists vs “hazard” exists

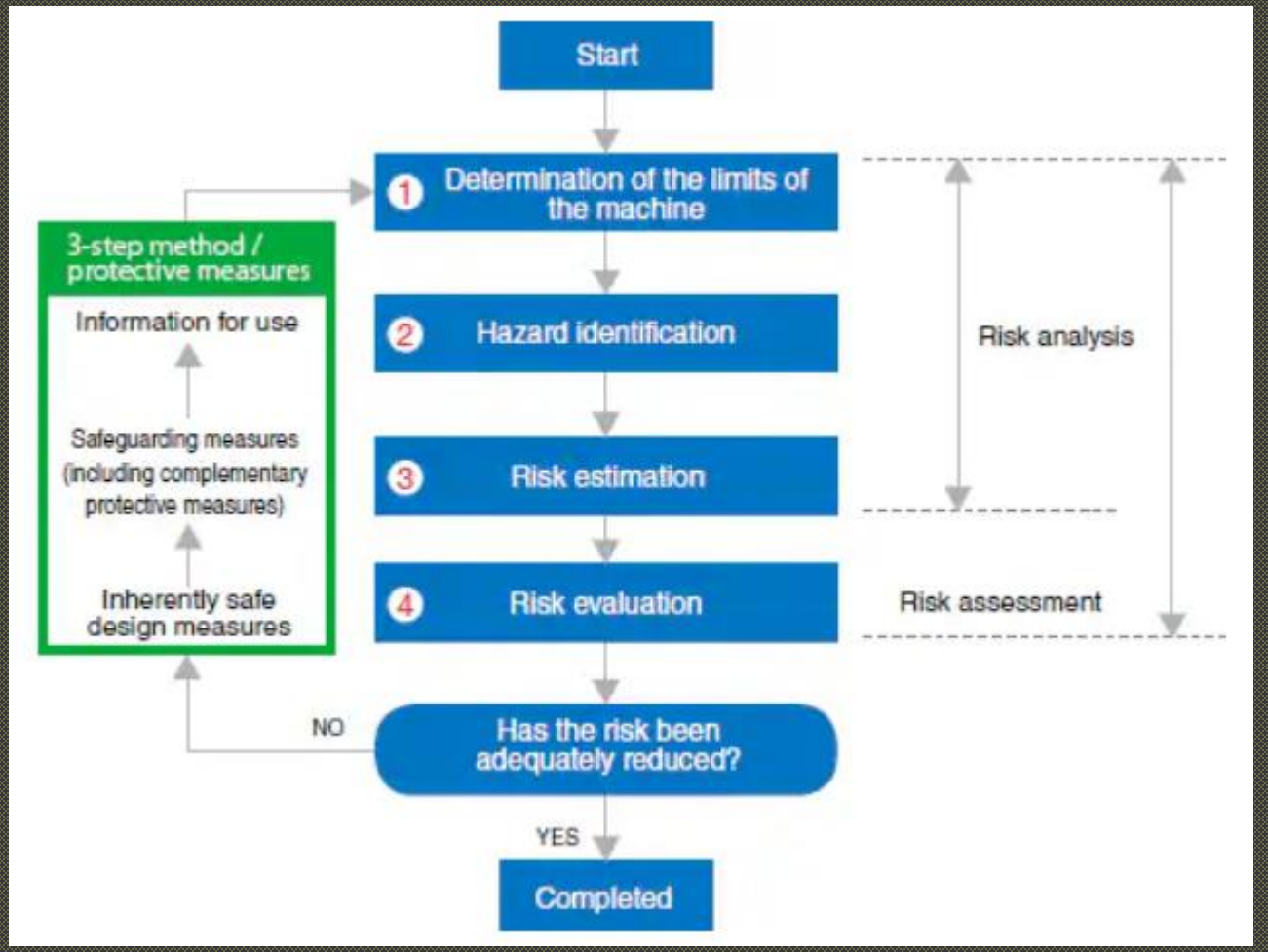
https://www.keyence.ca/ss/products/safetyknowledge/introduction/

HUMBER

SAFETY STANDARDS

- Risk Assessment:
  - Based on understanding machine limits, functions, and required tasks.
  - Evaluates both severity of harm and probability of occurrence to estimate risk.

- Risk Reduction:
  If necessary, safety measures are implemented using three methods:
  - Design Improvements – Eliminate or minimize risks through design.
  - Safeguarding Measures – Use protective devices for remaining risks.
  - Safe Use Information – Provide warnings, signals, training, and PPE.

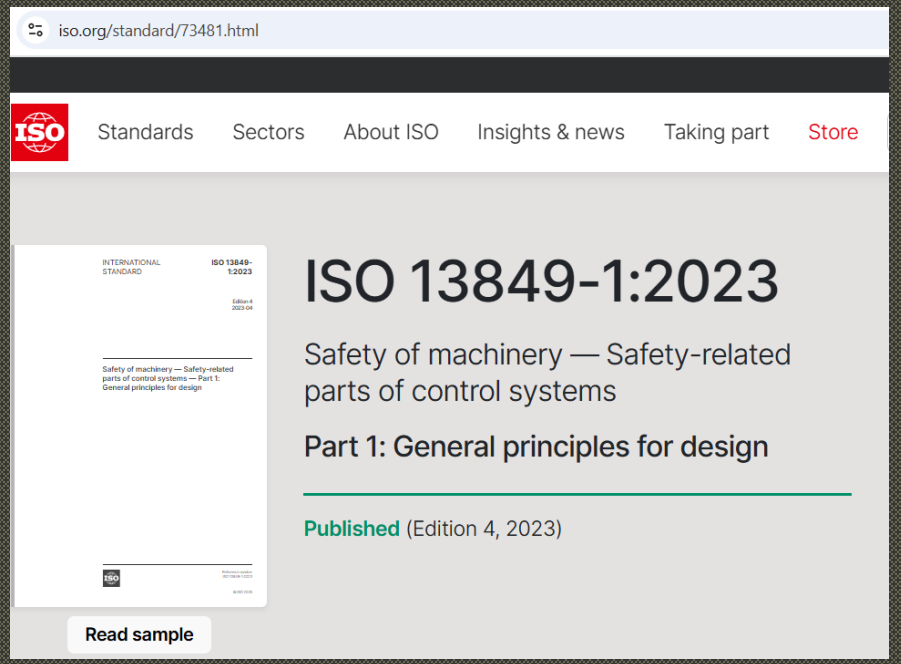


HUMBER

Safety related control systems for machinery – AB Safety related control systems for machinery – 5th Edition

SAFETY AND HARDWARE OVERVIEW

- Functional safety is the use of an automation system to guarantee the safety of people and equipment.
- Standards for functional and machine safety: IEC 62021 and ISO 13849
- ISO standards cover diverse industries, while IEC standards focus on electrical and electronic technologies.



https://www.youtube.com/user/ESECOTV

HUMBER

SAFETY INTEGRITY LEVEL - SIL

For each risk that requires a safety-related control system, the risk must be assessed, and the necessary risk reduction (SIL) determined according to IEC 62061, based on specific parameters:

- Severity of injury (Se)
- Frequency and duration of exposure (Fr)
- Probability of occurrence of a hazardous event (Pr)
- Probability of avoiding or limiting harm (Av)

Consequences	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

Frequency of exposure	Duration (Fr) <= 10 min	Duration (Fr) > 10 min
≥ 1 per h	5	5
< 1 per h up to ≥ 1 per day	4	5
< 1 per day up to ≥ 1 every 2 weeks	3	4
< 1 every 2 weeks up to ≥ 1 per year	2	3
< 1 per year	1	2

Probability of occurrence	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

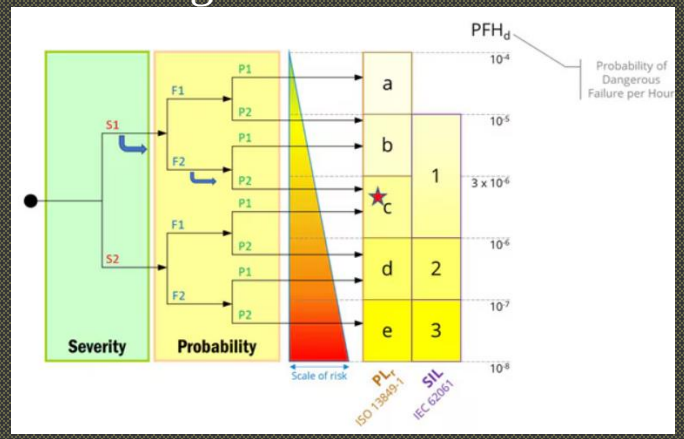
Probability of avoiding or limiting	Avoiding and limiting (Av)
Impossible	5
Rarely	3
Probable	1

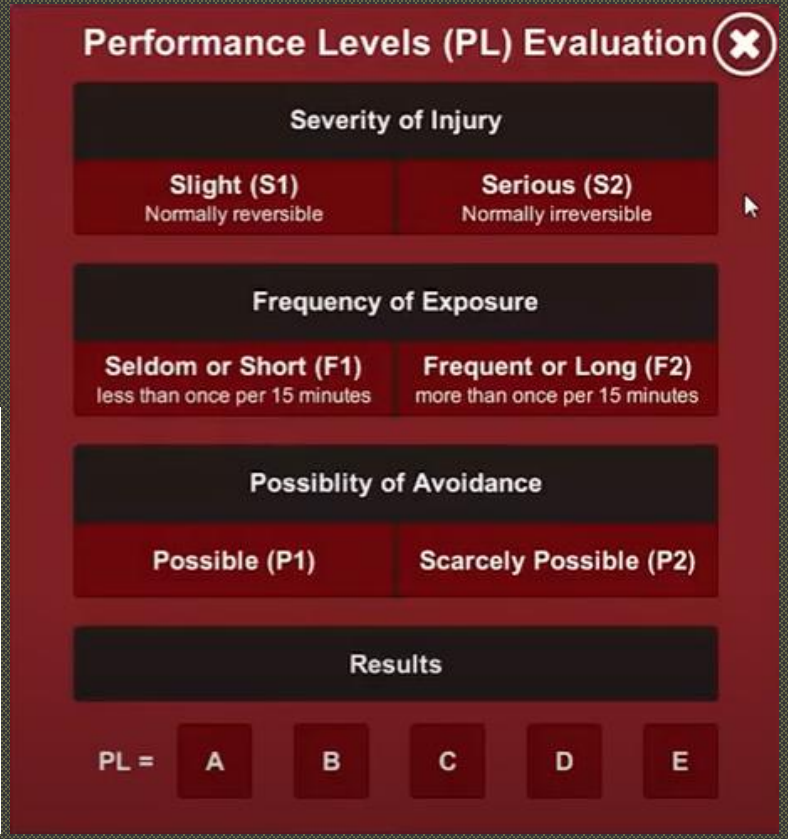
https://www.pilz.com/en-US/support/law-standards-norms/functional-safety/en-iec-62061

PERFORMANCE LEVEL - PL

The required performance level (PLr) for each safety function in a control system must be determined based on three parameters defined in ISO 13849-1:

- 1. Severity of injury:
  - S1: Slight (normally reversible injury)
  - S2: Serious (normally irreversible injury or death)
- 2. Frequency and/or exposure to hazard
  - F1: Seldom-to-less-often and/or exposure time is short
  - F2: Frequent-to-continuous and/or exposure time is long
- 3. Possibility to avoiding hazard or limiting harm
  - P1: Possible under specific conditions
  - P2: Scarcely possible

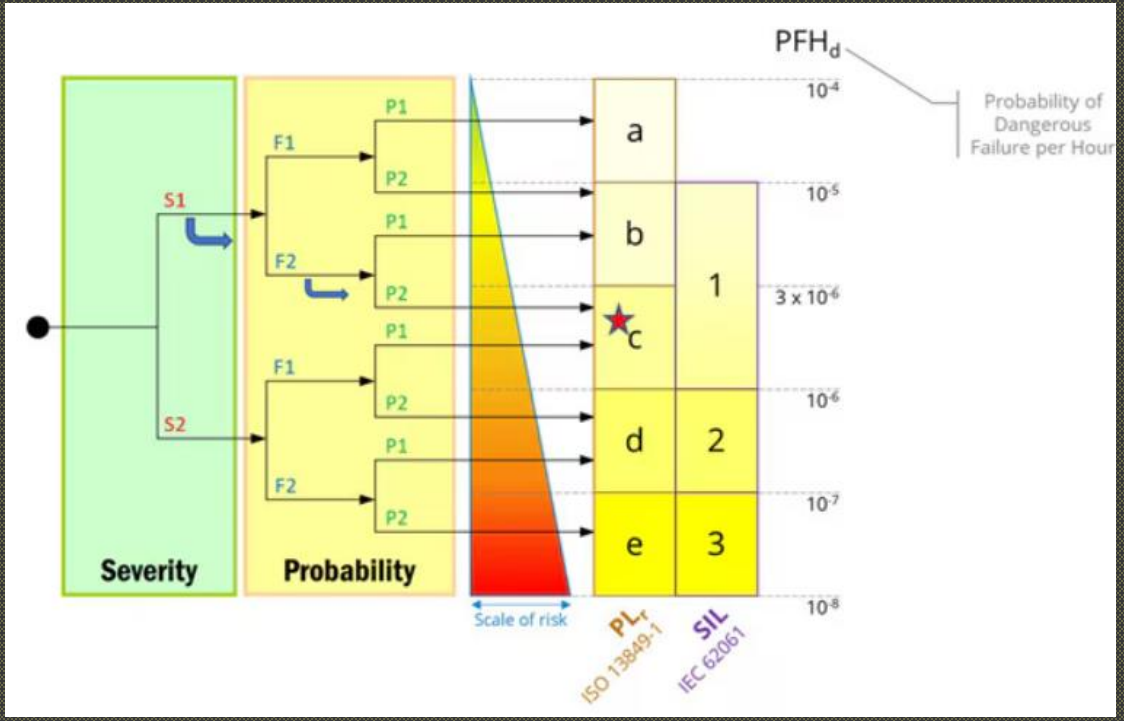




https://www.sick.com/us/en/what-are-performance-levels/w/blog-safety-standard-performance-levels/

PERFORMANCE LEVEL - PL

- Performance levels (PL) indicate the ability of a safety-related control system to function under foreseeable conditions.
- The required PL (PLr) is the minimum level needed to reduce risk. PL must meet or exceed PLr.
- Higher-risk machines need higher PLs, ranging from PLa (lowest) to PLe (highest). Small, slow robots may need PLa, while large, fast robots require PLe.

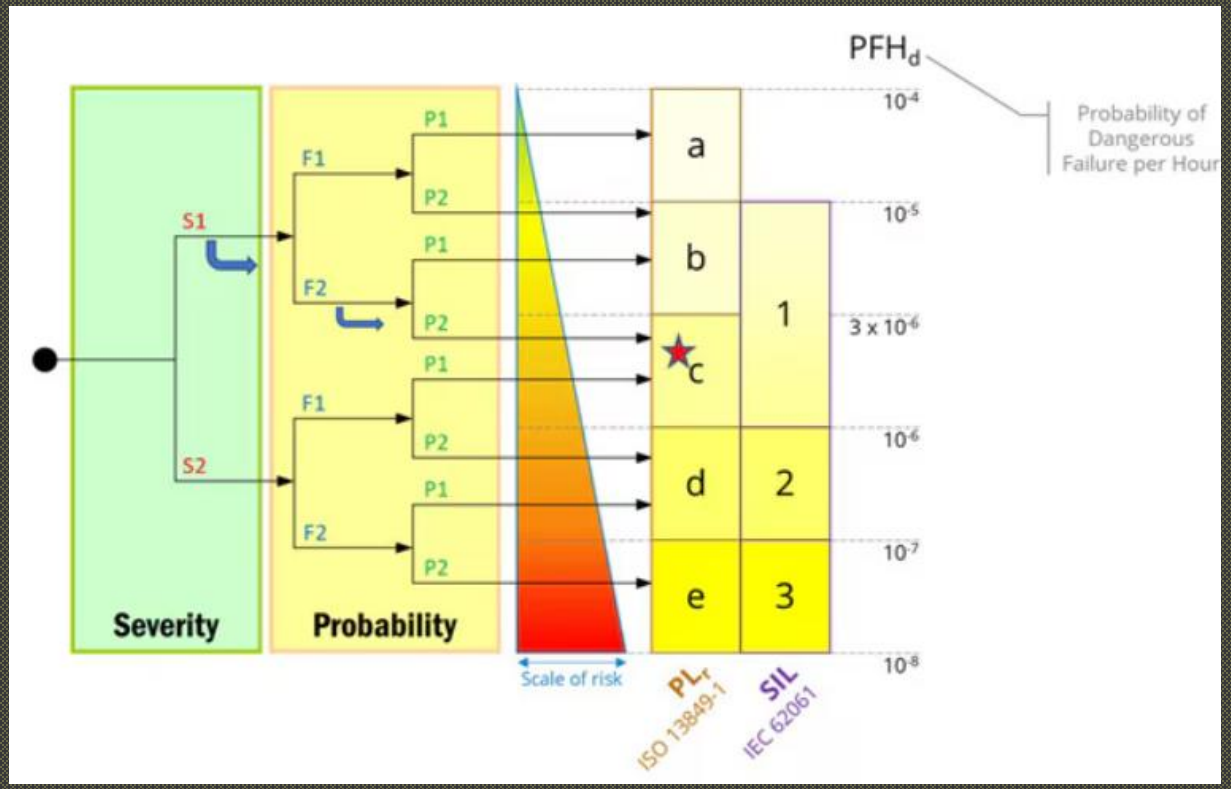


https://www.sick.com/us/en/what-are-performance-levels/w/blog-safety-standard-performance-levels/

HUMBER

SIL & PL

The chart compares Performance Level (PL) and Safety Integrity Level (SIL), which use similar risk-based thresholds but differ in labeling - PL per ISO 13849-1 and SIL per IEC 62061.



Performance Level (PL)	Probability of Dangerous Failure per Hour (PFHd) 1/h
a	≥10^{-5} and <10^{-4} ⟨0.001% to 0.01%⟩
b	≥3 × 10^{-6} and <10^{-5} ⟨0.0003% to 0.001%⟩
c	≥10^{-6} and <3 × 10^{-6} ⟨0.0001% to 0.0003%⟩
d	≥10^{-7} and <10^{-6} ⟨0.00001% to 0.0001%⟩
e	≥10^{-8} and <10^{-7} ⟨0.000001% to 0.00001%⟩

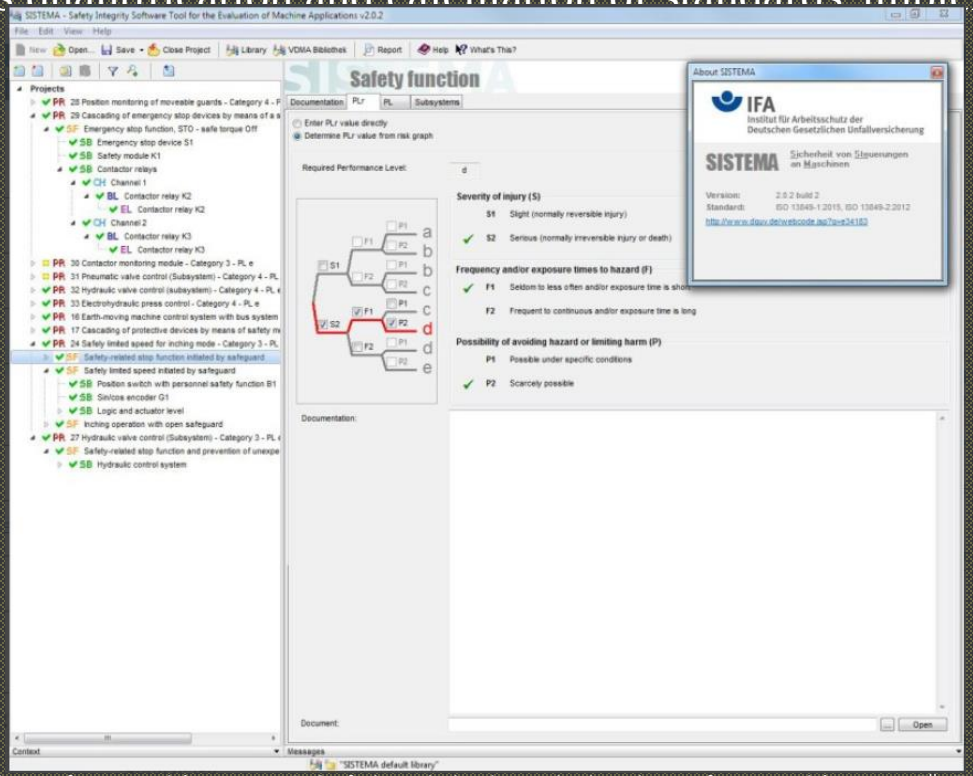
A failure per hour of 10^{-7} means a probability of 1 dangerous failure to every 10 million hours. If the robots were running 24 hours a day, 365 days a year, it indicates to run for 1,141 years of continuous operation without a fatal accident.

https://www.sick.com/us/en/what-are-performance-levels/w/blog-safety-standard-performance-levels/

HUMBER

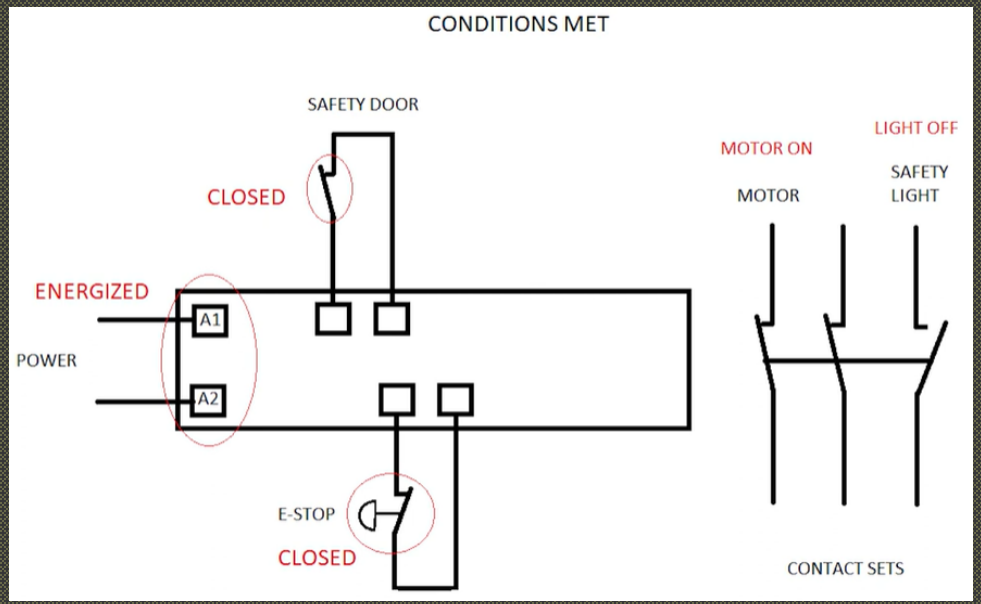
SYSTEM DESIGN

- Study Requirement:
  - ISO 13849-1 and IEC 62061 require detailed study before application.
- Design and Integration:
  - Provide requirements for design and integration of safety-related control system parts, including software aspects.
- Scope:
  - Apply to entire safety-related systems or individual components.
- Example Tool:
  - SISTEMA software by IFA simplifies quantification and calculation of standards' implementation.



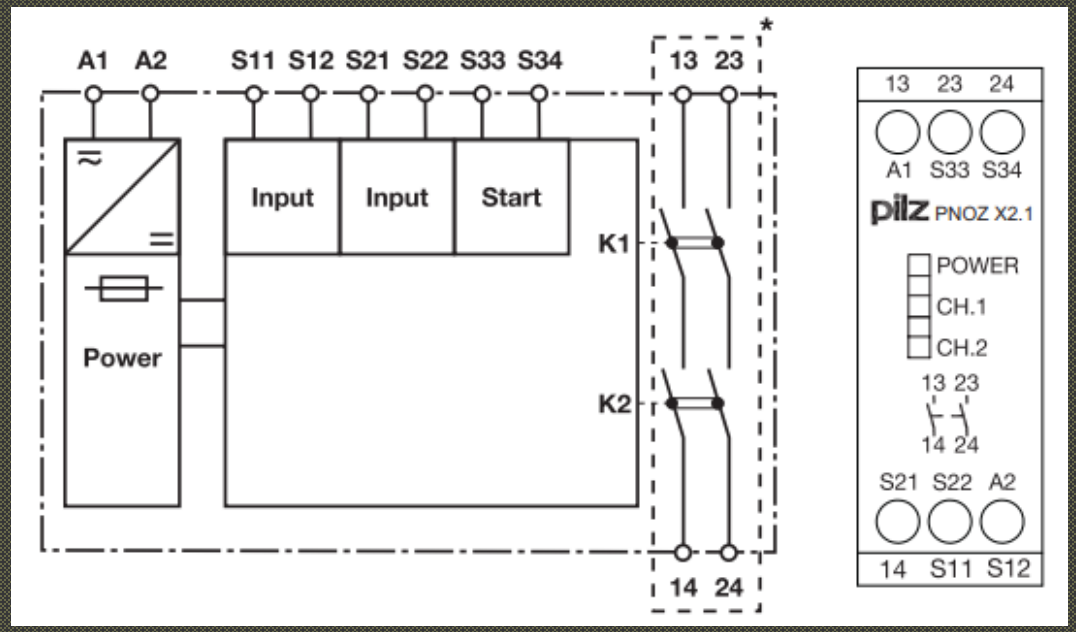
Safety Relays

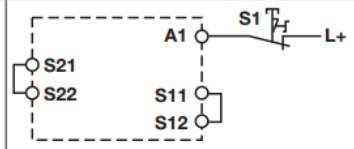
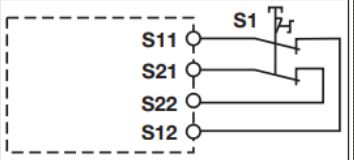
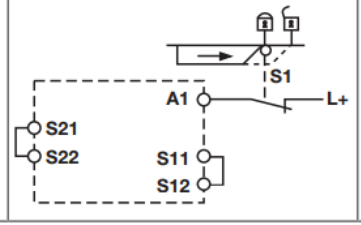
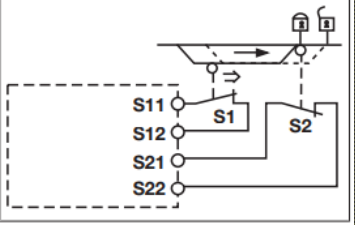
- Safety relays undergo rigorous testing and have a lower failure rate than normal relays.
- Contacts fully disconnect both sides of the power connection, unlike normal relays.
- Built-in fail-safe features and redundancies ensure maximum safety.
- Force-guided contacts (NO and NC) move together, preventing simultaneous closure and enabling fault detection.
- Multiple conditions must be met for operation, enhancing safety.

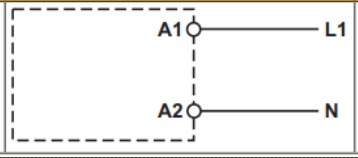
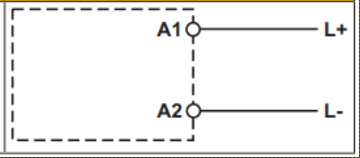


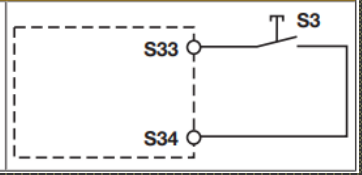
RSP Supply - https://www.youtube.com/watch?v=pGDKVLVNwtw

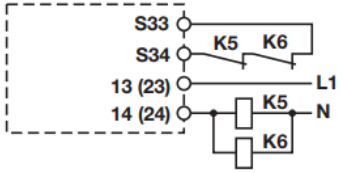
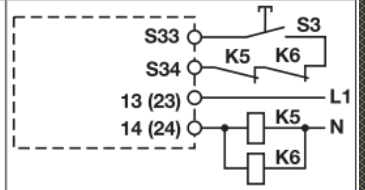
Safety Relays



Input circuit	Single-channel	Dual-channel (with detection of shorts across contacts)
E-STOP		
Safety gate		

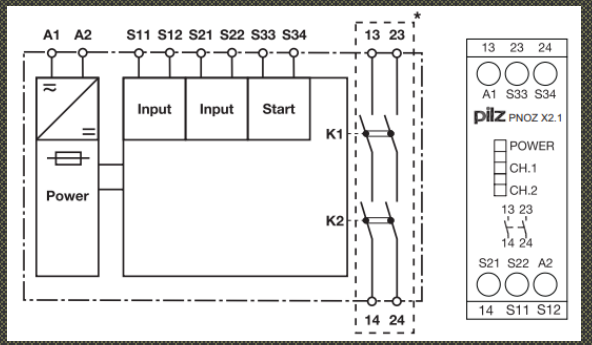
Supply voltage	AC	DC
		

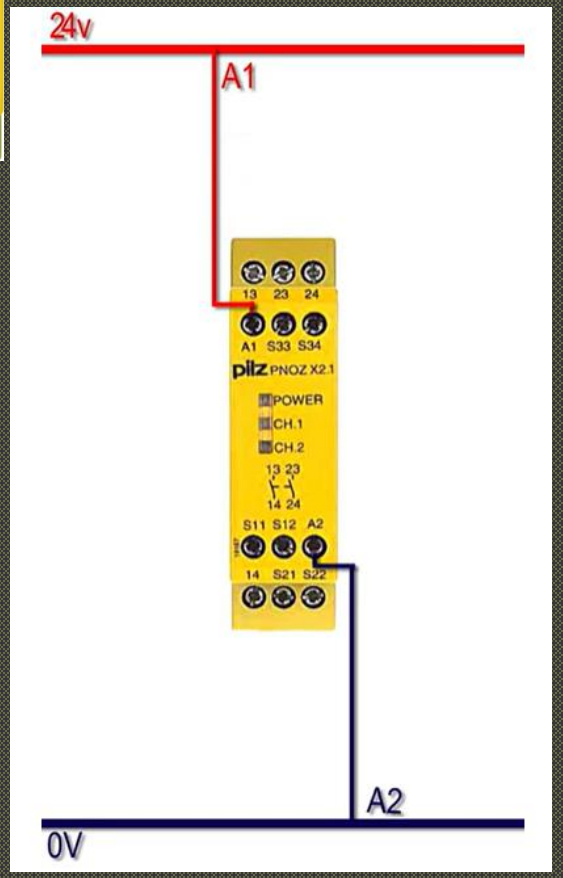
Start circuit	Automatic start	Manual start
Automatic start		

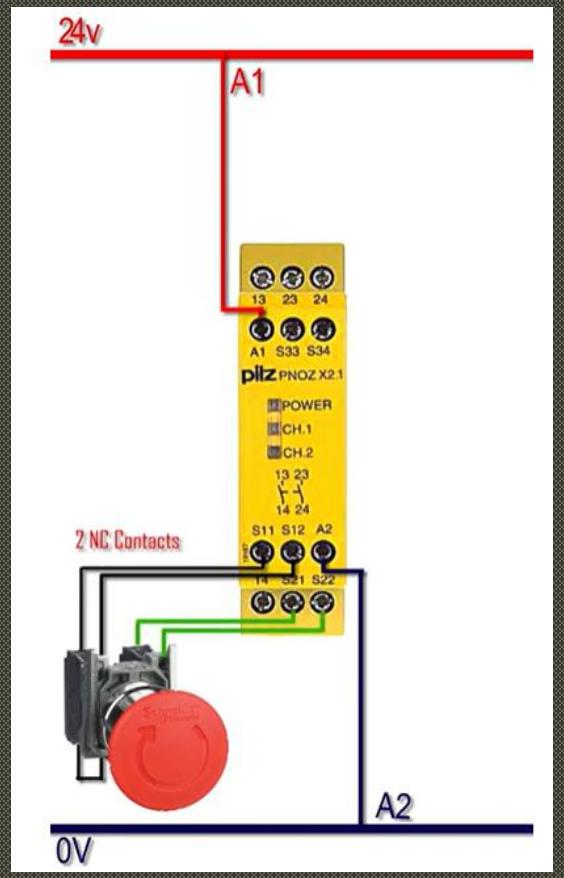
Feedback loop	Automatic start	Manual start
Contacts from external contactors		

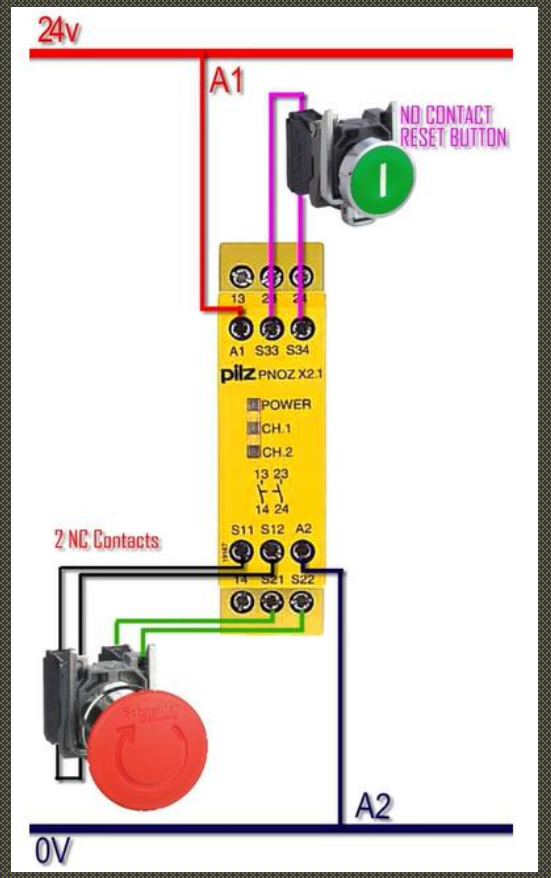
https://www.pilz.com/download/open/PNOZ_X2_1_Operat_Man_1003354-EN-10.pdf

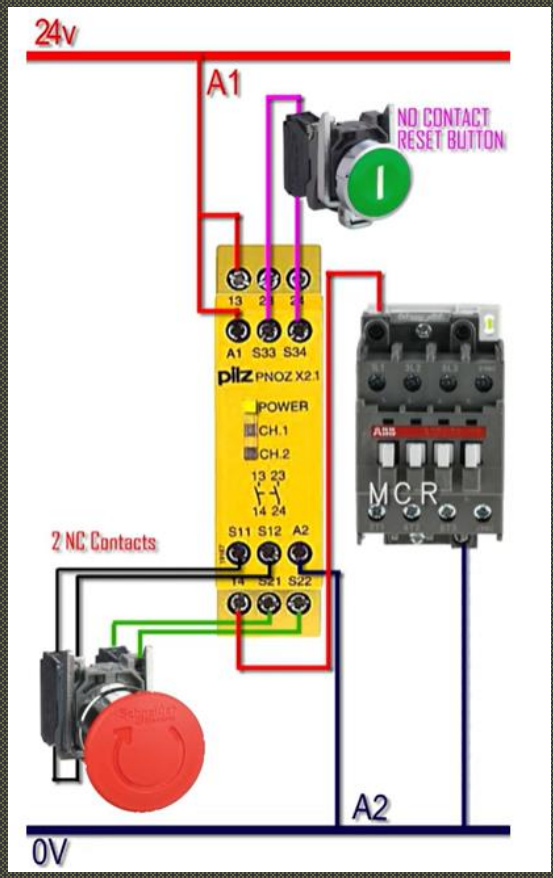
Safety Relays







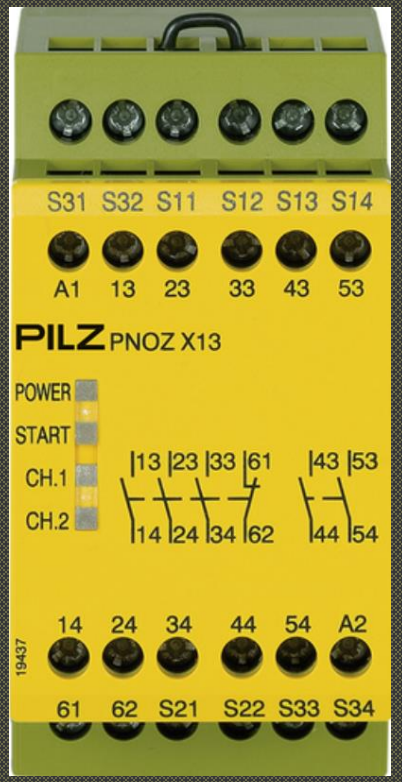


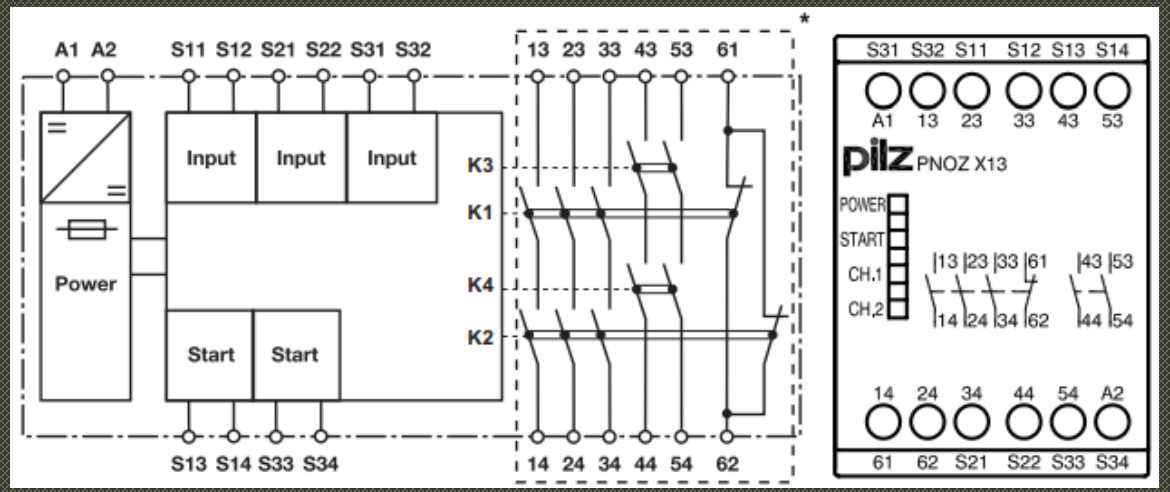


HUMBER

https://www.youtube.com/watch?v=SJwrVZEBWJA

Safety Relays



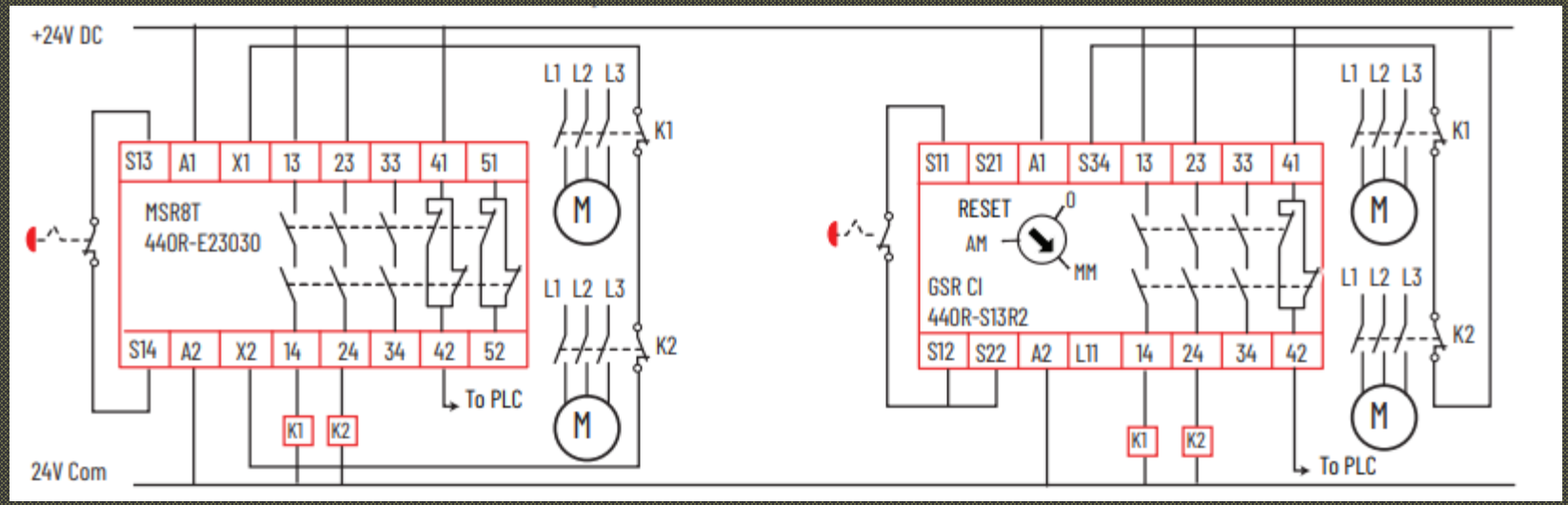


Supply voltage	AC	DC
		A1 L+ A2 L-
Input circuit	**Single-channel**	**Dual-channel**
E-STOP **without** detection of shorts across contacts	S1 S12 S11 S21 S22 S32 S31	
E-STOP **with** detection of shorts across contacts		S1 S22 S32 S11 S12 S31 S21
Safety gate **without** detection of shorts across contacts	S1 S12 S11 S21 S22 S32 S31	
Safety gate **with** detection of shorts across contacts		S31 S1 S2 S11 S32 S12 S21 S22
Start circuit	**E-STOP wiring Safety gate without start-up test**	**Safety gate with start-up test**
Automatic start	S33 S34 S13 S14	S33 S34 S1 S2 S13 S14
Monitored start	S3 S33 S34 S13 S14	
Feedback loop	**Automatic start**	**Monitored start**
Contacts from external contactors	S13 S14 K5 K6 13 (23 ... 53) 14 (24 ... 54) L1 K5 N K6	S3 S33 S34 K5 K6 13 (23 ... 53) 14 (24 ... 54) L1 K5 N K6

https://www.pilz.com/download/open/PNOZ_X13_Operating_Manual_20187-EN-09.pdf

HUMBER

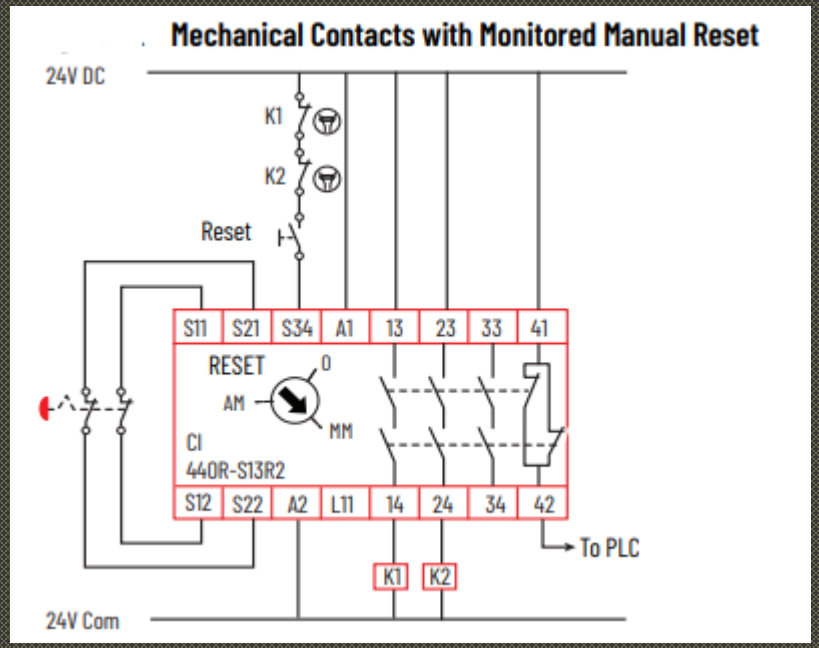
SAFETY RELAYS: LEGACY TO MODERN

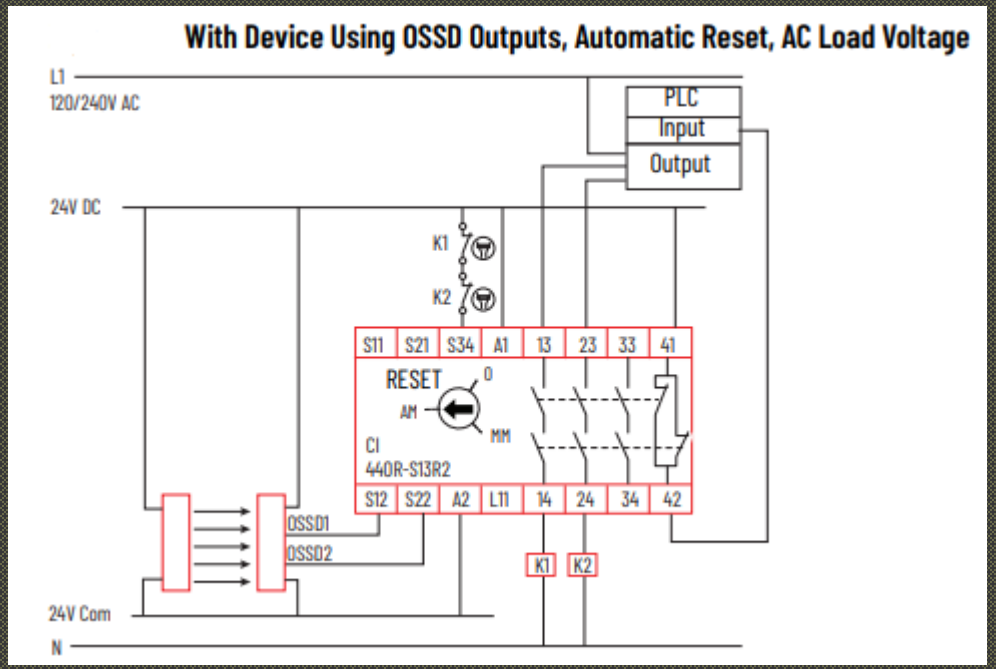


https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/440r-rm004_-en-p.pdf

SAFETY RELAYS – GUARDMASTER

GSR Relays meet the latest safety standards including ISO 13849-1 and IEC 62061





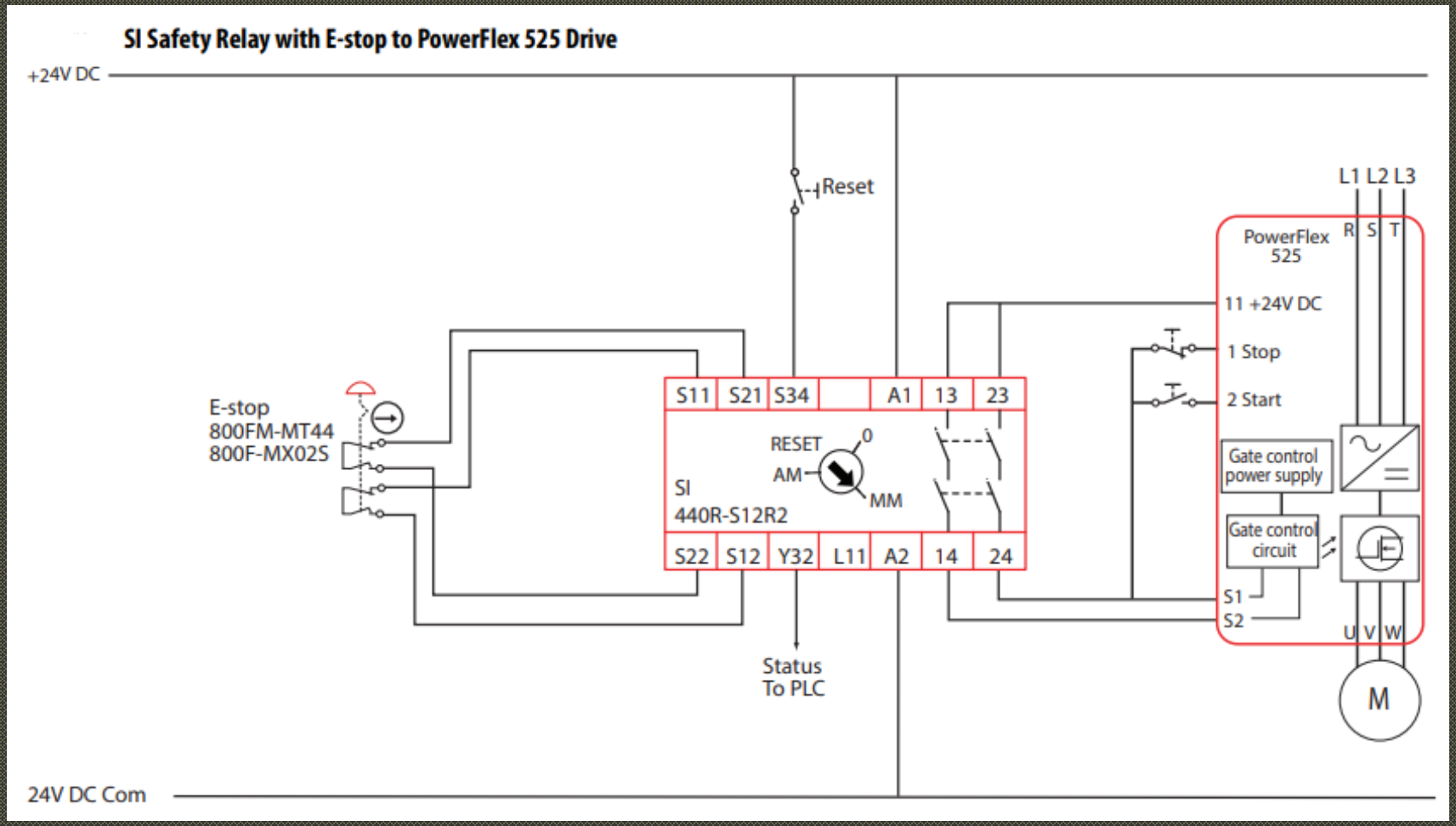
- Compatible Input (CI) safety relay monitors an E-stop push button with mechanical contacts.
- Configured for Monitored Manual (MM) reset.
- Output activates if E-stop is released and Reset button is pressed/released.
- Monitors contactors K1 and K2; does not reset if either fails to close N.C. contacts.
- Sends an auxiliary signal (terminals 41/42) to the PLC when E-stop is pressed.

- CI safety relay monitors a safety light curtain with two Output Signal Switching Device (OSSD) outputs.
- Configured for automatic/manual reset (AM).
- Auxiliary signal (terminals 41/41) informs PLC of safety system status (on/off).
- Outputs connect to AC voltage loads.
- When the CI safety relay is on, the PLC can activate contactors K1 and K2.

HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/440r-rm004_-en-p.pdf

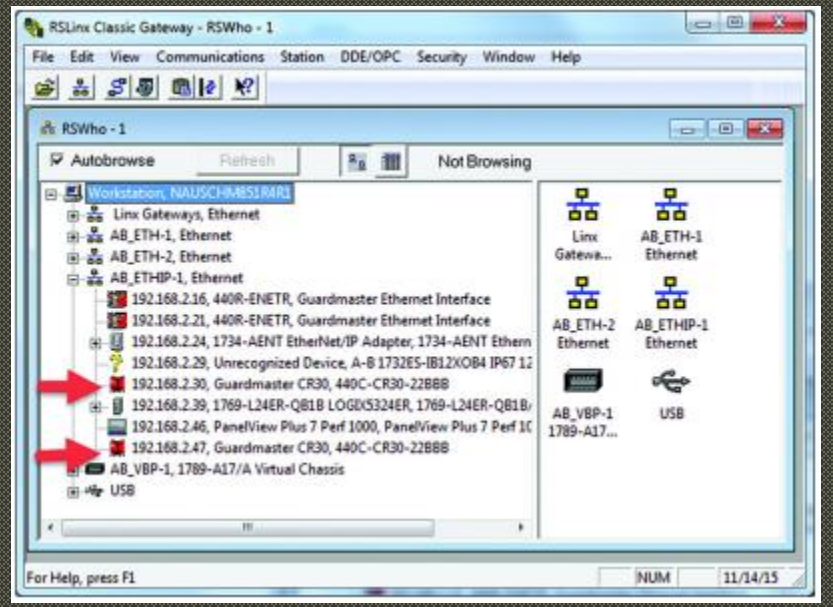
SAFETY RELAYS - GUARDMASTER



SI – Single Input

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/440r-rm004_-en-p.pdf

CONFIGURABLE SAFETY RELAYS - GUARDMASTER

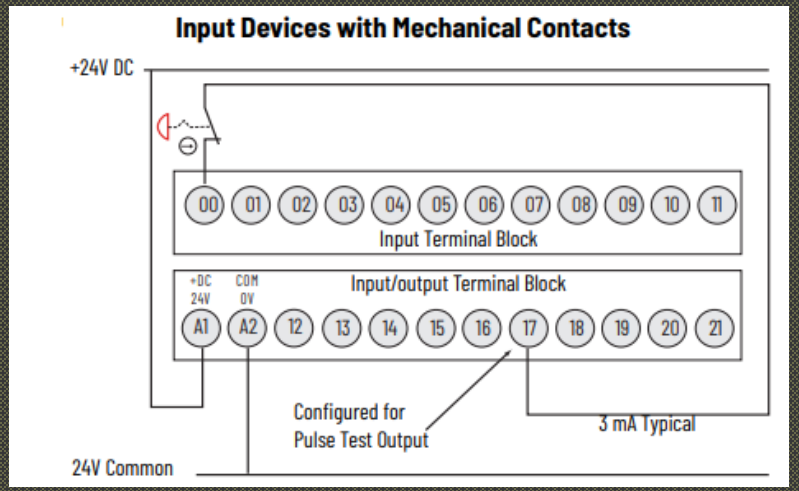


- The CR30 safety relay has 22 embedded safety rated inputs and outputs and accepts up to two plug-in modules, each of which has four standard inputs and four standard outputs.
- The CR30 safety relay is configurable with the Connected Components Workbench free software.

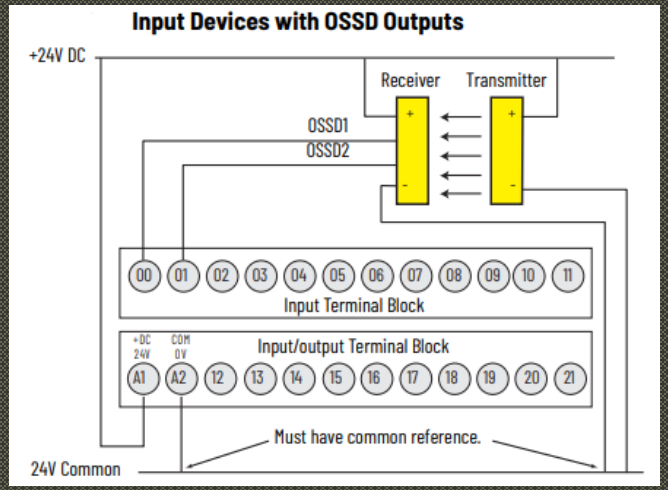
HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/440r-rm004_-en-p.pdf

CONFIGURABLE SAFETY RELAYS - GUARDMASTER



Input devices with mechanical contact outputs, such as Emergency Stop (E-stop) buttons and safety limit switches, use both a safety input terminal and a test output terminal. This setup enables the circuit to achieve a PLe or SIL3 rating.



Devices, such as safety light curtains, laser scanners, and solid-state interlocks, having current-sourcing PNP semiconductor outputs (OSSD) have built-in test pulses (or other method of fault detection). These devices connect directly to the inputs of the CR30 safety relay and do not use a test output

HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/440r-rm004_-en-p.pdf

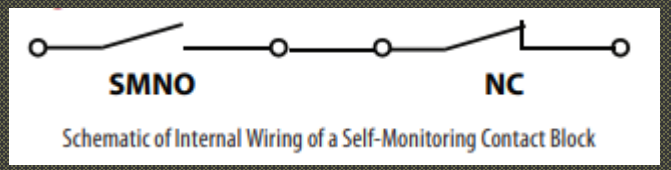
SELF MONITORING CONTACT BLOCKS

Actuator – Red Color

Self-Monitoring Contact Block (SMCB)

- Detects if a contact block separates from its actuator (e.g., emergency stop button).
- Contains a normally open (NO) contact, held closed when properly installed.
- If detached, the NO contact opens, triggering an emergency stop.
- Ensures the system shuts down even if the contact block is removed, enhancing safety.

Contact Block



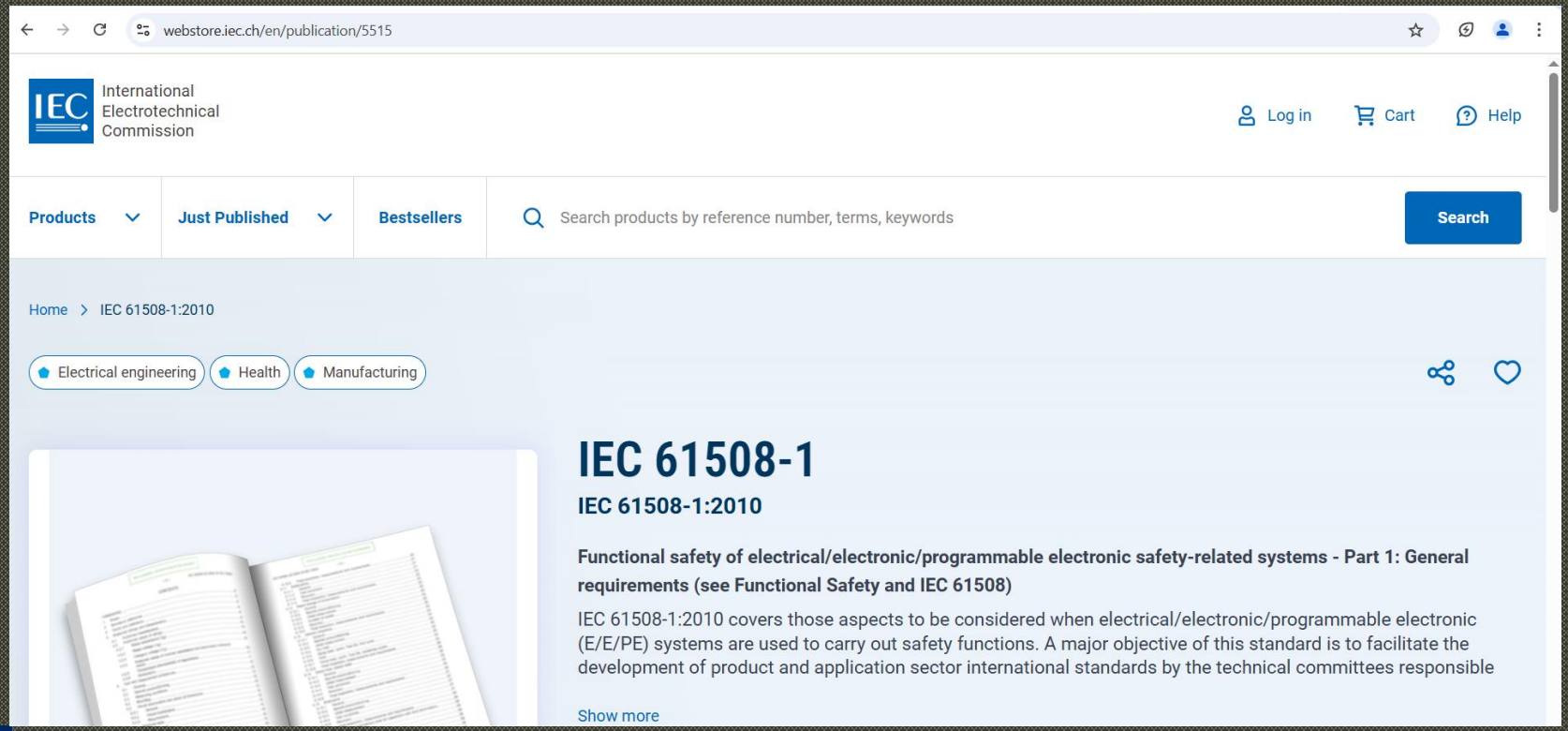
Schematic of Internal Wiring of a Self-Monitoring Contact Block

HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/440r-rm004_-en-p.pdf

SAFETY PLCS

- Designed for industrial safety, complying with IEC 61508 and ISO 13849 standards.
- Prevent accidents and ensure safe machine operation.
- Key features: dual-channel inputs, fault detection, and safety interlocks.
- Dual-input systems prevent failures from leading to unsafe conditions.

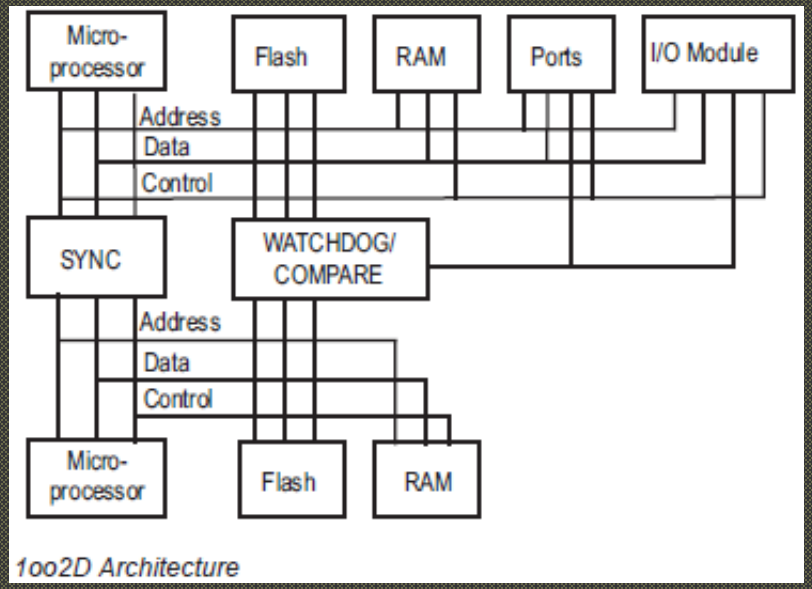


https://webstore.iec.ch/en/publication/5515

SAFETY PLCs

Advantages:

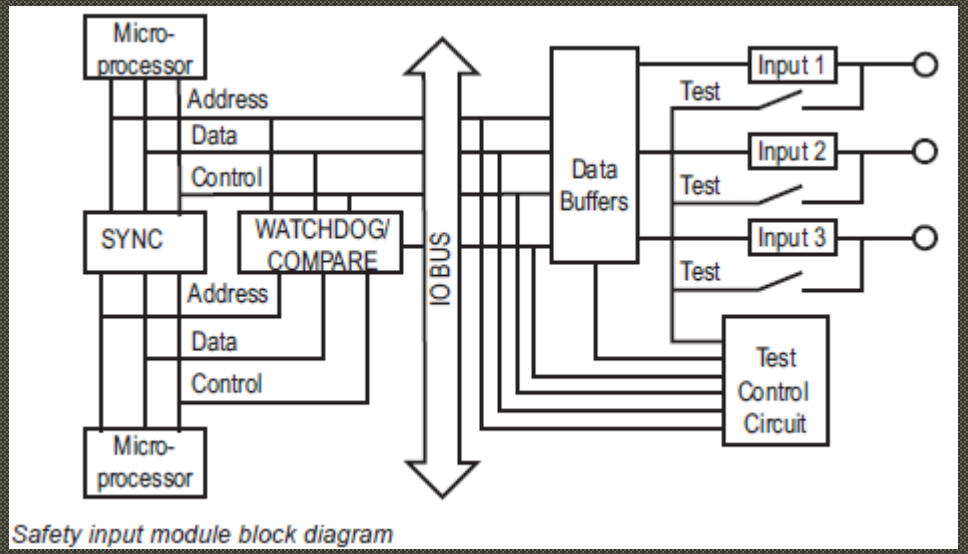
- Designed for flexible and scalable safety applications.
- Provide control flexibility similar to standard PLCs but for safety-critical tasks.
- Differ significantly from standard PLCs in architecture and fault tolerance.
- Meet scalability, functionality, and integration requirements for complex systems.



1oo2D Architecture

SAFETY PLCs

- Multiple microprocessors manage I/O, memory, and safe communications.
- Watchdog circuits perform continuous diagnostic checks (1oo2D system ensures redundancy and synchronization).
- High-frequency input testing ensures reliability by verifying each input multiple times per second.
- Pulse test signals detect cross-faults in mechanical safety devices like emergency stops and gate switches.



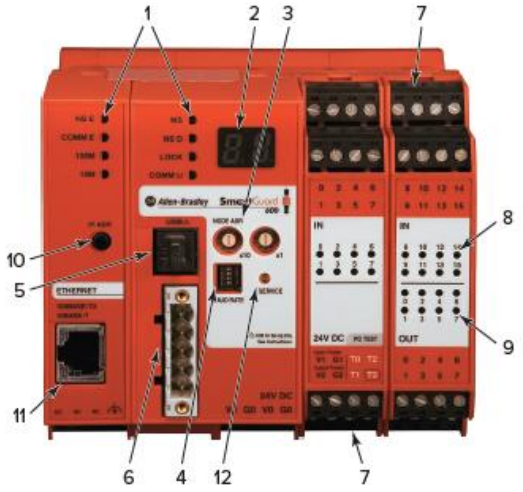
Safety input module block diagram

A 1oo2D system (one out of two with diagnostics) is a safety architecture that ensures redundancy and synchronization by using two channels.

- Redundancy: The system has two channels, and it can tolerate a single fault while still performing the safety function.
- Diagnostics: Built-in diagnostics continuously monitor both channels to detect faults.
- Synchronization: Both channels work together, ensuring that the system remains synchronized and reliable.
- Safety Function: The system requires both channels to fail before the safety function is compromised, enhancing overall safety.

SAFETY PLCs

- Safety PLCs are certified by third parties to meet strict safety standards.
- Both standard and safety PLCs perform control functions.
- Safety PLCs are designed to be fault-tolerant and fail-safe, ensuring higher reliability for safety-critical applications.



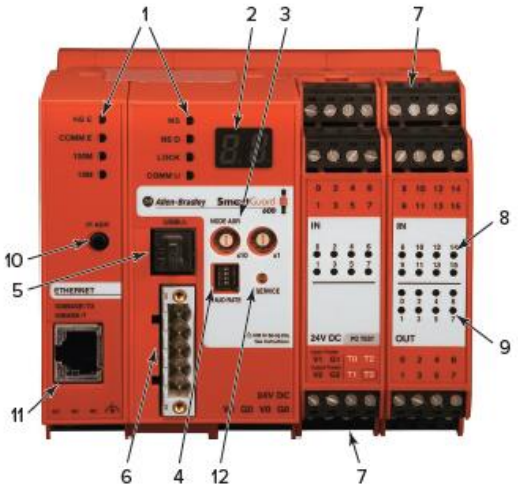
Number	Feature
1	Module status indicators
2	Alphanumeric display
3	Node address switches
4	Baud rate switches
5	USB port
6	DeviceNet communication connector
7	Terminal connectors
8	Input status indicators
9	Output status indicators
10	IP address display switch
11	Ethernet connector
12	Service switch

Figure 9-21 Safety PLC.
Source: Image Courtesy of Rockwell Automation, Inc.

A Fail-Safe System goes to a safe mode if it fails, while a Fault-Tolerant System keeps working even if a part fails. Fault tolerance often needs duplicate parts, but fail-safe systems don't always need that.

SAFETY PLCs

- Standard PLC:
  - Single microprocessor for program execution.
  - Flash memory stores program.
  - RAM for calculations.
  - Ports for communications.
  - I/O for machine detection and control.



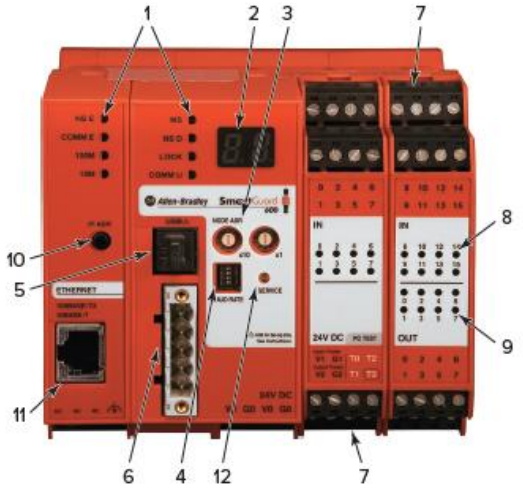
Number	Feature
1	Module status indicators
2	Alphanumeric display
3	Node address switches
4	Baud rate switches
5	USB port
6	DeviceNet communication connector
7	Terminal connectors
8	Input status indicators
9	Output status indicators
10	IP address display switch
11	Ethernet connector
12	Service switch

Figure 9-21 Safety PLC.
Source: Image Courtesy of Rockwell Automation, Inc.

- Safety PLC:
  - Redundant microprocessors.
  - Flash and RAM continuously monitored by watchdog circuit.
  - Synchronous detection circuit for increased reliability.
  - Redundancy: Minimizes hazards from electrical malfunctions by duplicating components.

SAFETY PLCs

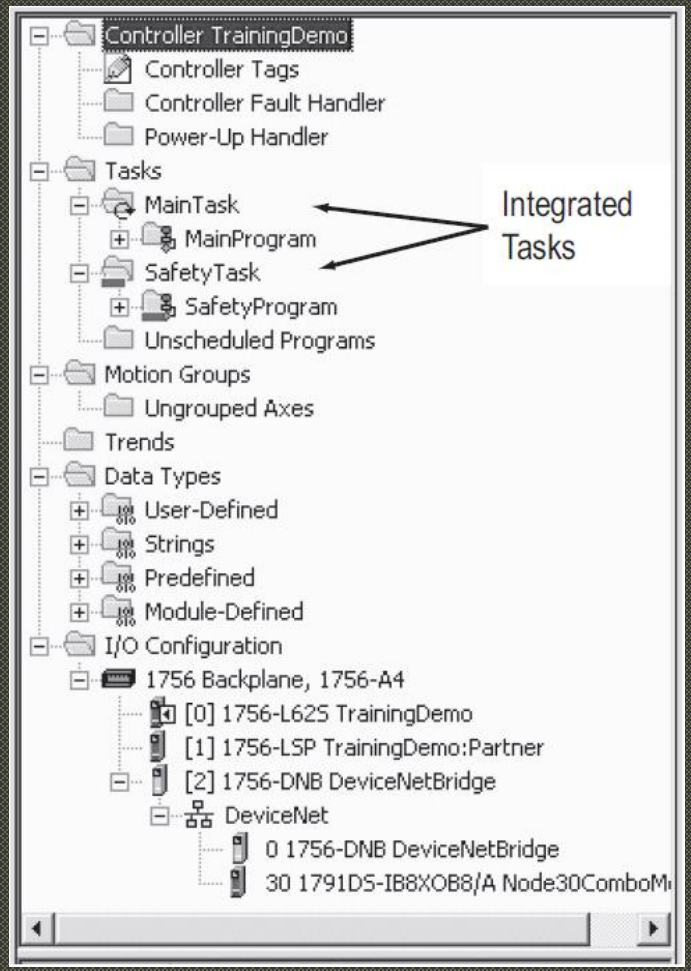
- Standard PLC Inputs:
  - No internal testing capability for input circuitry.
- Safety PLC Inputs:
  - Internal output circuit for each input to test functionality.
  - Inputs driven high and low briefly during runtime for verification.
  - Specialized power supplies for safety systems.
  - Redundant backplane circuitry between controller and I/O modules.



Number	Feature
1	Module status indicators
2	Alphanumeric display
3	Node address switches
4	Baud rate switches
5	USB port
6	DeviceNet communication connector
7	Terminal connectors
8	Input status indicators
9	Output status indicators
10	IP address display switch
11	Ethernet connector
12	Service switch

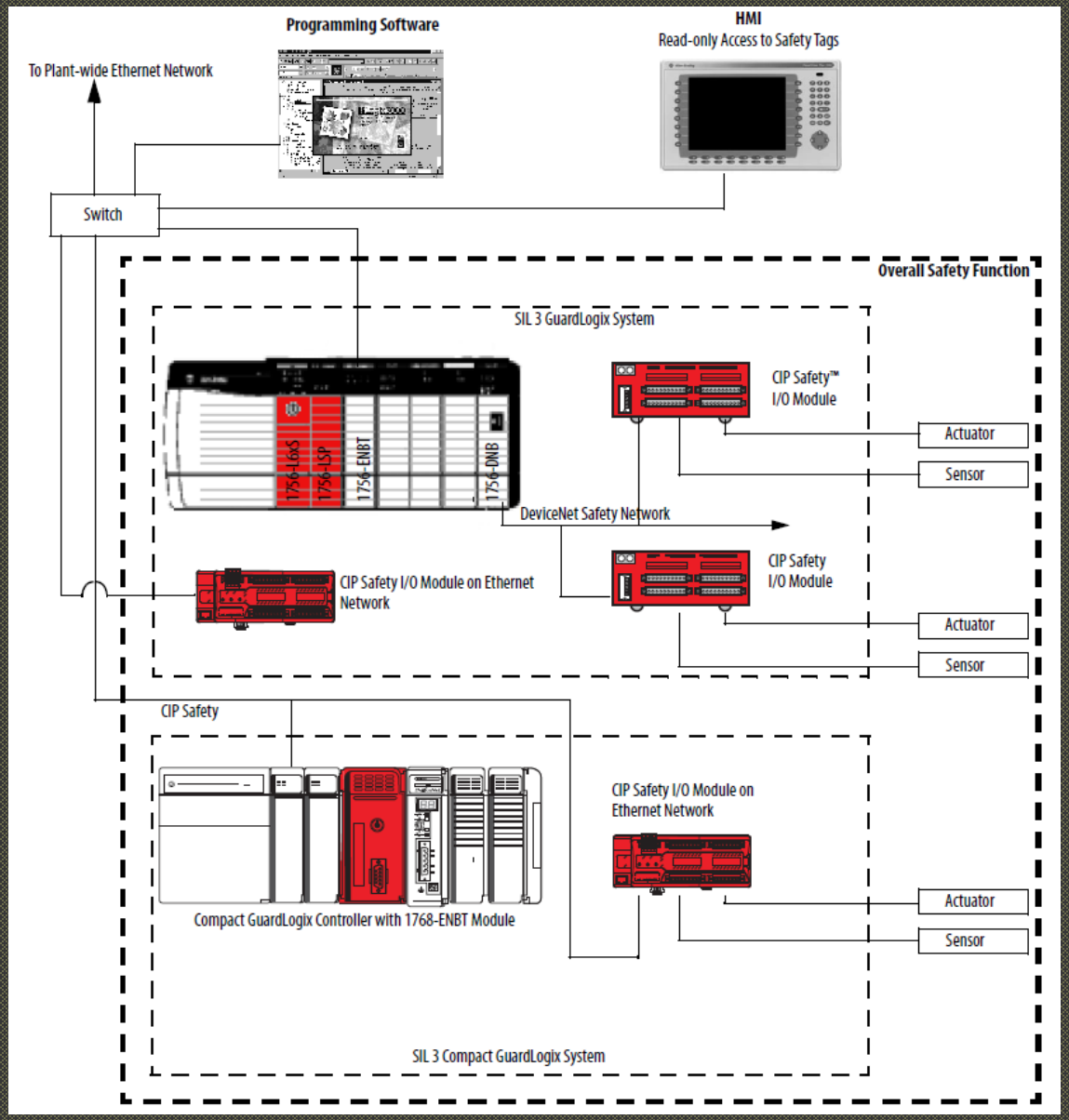
Figure 9-21 Safety PLC.
Source: Image Courtesy of Rockwell Automation, Inc.

SOFTWARE



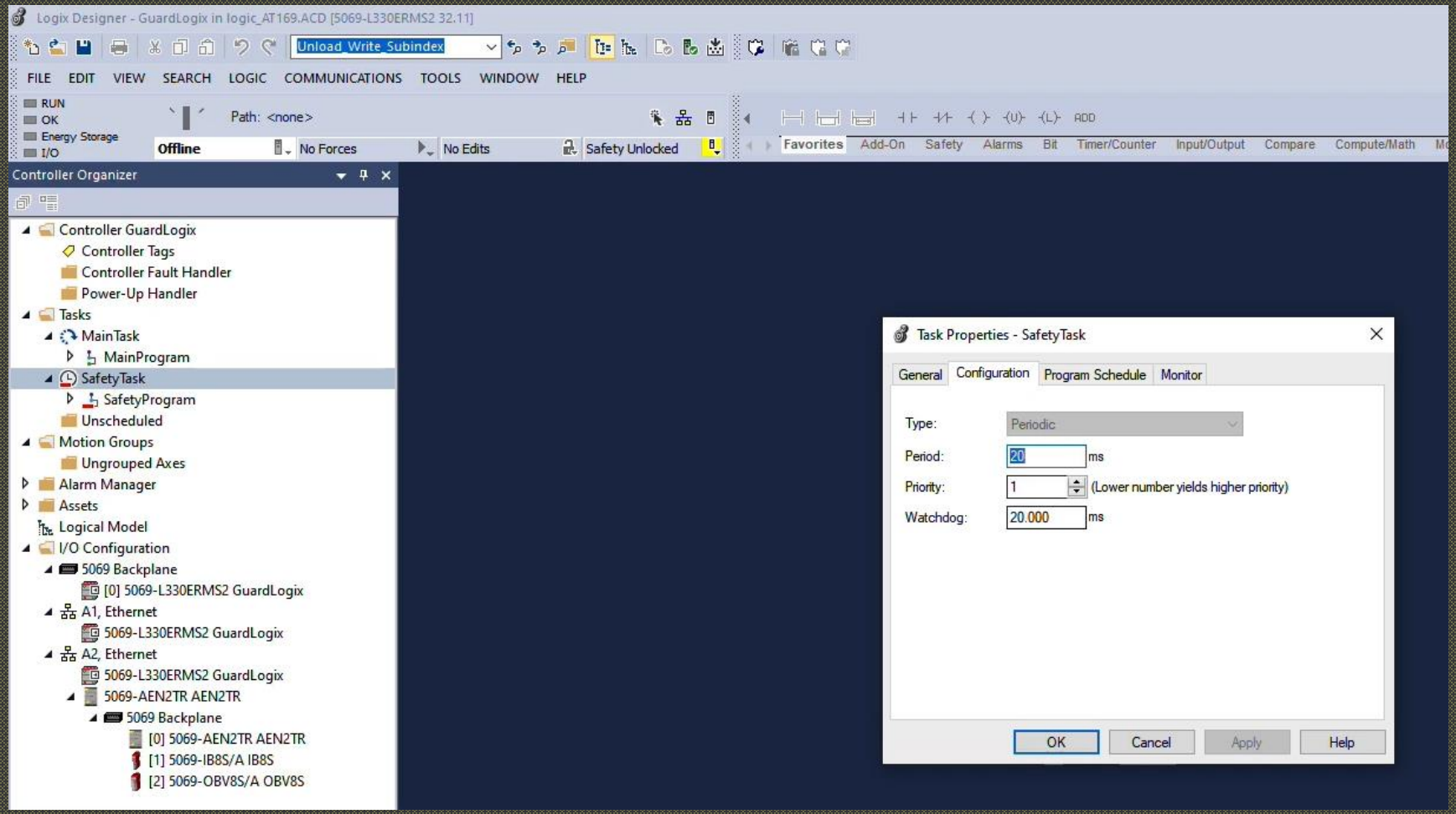
- Programming: Safety PLCs program similarly to standard PLCs.
- Diagnostics: Automatic background diagnostics and error checking.
- Safety Instructions: Mimic safety relay functions (e.g., Emergency Stop).
- Simplicity: Complex logic handled within certified function blocks.
- Programming Methods: Function Blocks and Ladder Logic are common.
- Compliance: Certified safety instructions ensure standards compliance.
- Device Support: Function blocks support various safety devices.
- Simplified Wiring: Inputs/outputs connect to any safety I/O terminals.
- Integration: Safety and standard control functions coexist in one controller.
- Capabilities: Supports motion, drive, process, batch, high-speed control, and SIL 3 safety.
- Cost Efficiency: Common tools and technologies reduce expenses.
- Task Separation: Non-safety functions in Main Task; safety functions in Safety Task.
- Interaction: Standard and safety functions interact via safety tags.
- Hardware: Use of common safety and standard control hardware, distributed safety I/O, and shared HMI devices.
- Troubleshooting: Faster troubleshooting and reduced training costs.
- Data Sharing: Safety tags shared between controllers via EtherNet/IP, ControlNet, or DeviceNet.
- Accessibility: Safety data accessible by HMIs, PCs, or other controllers.

TYPICAL SIL FUNCTION



https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

SYSTEM DESIGN

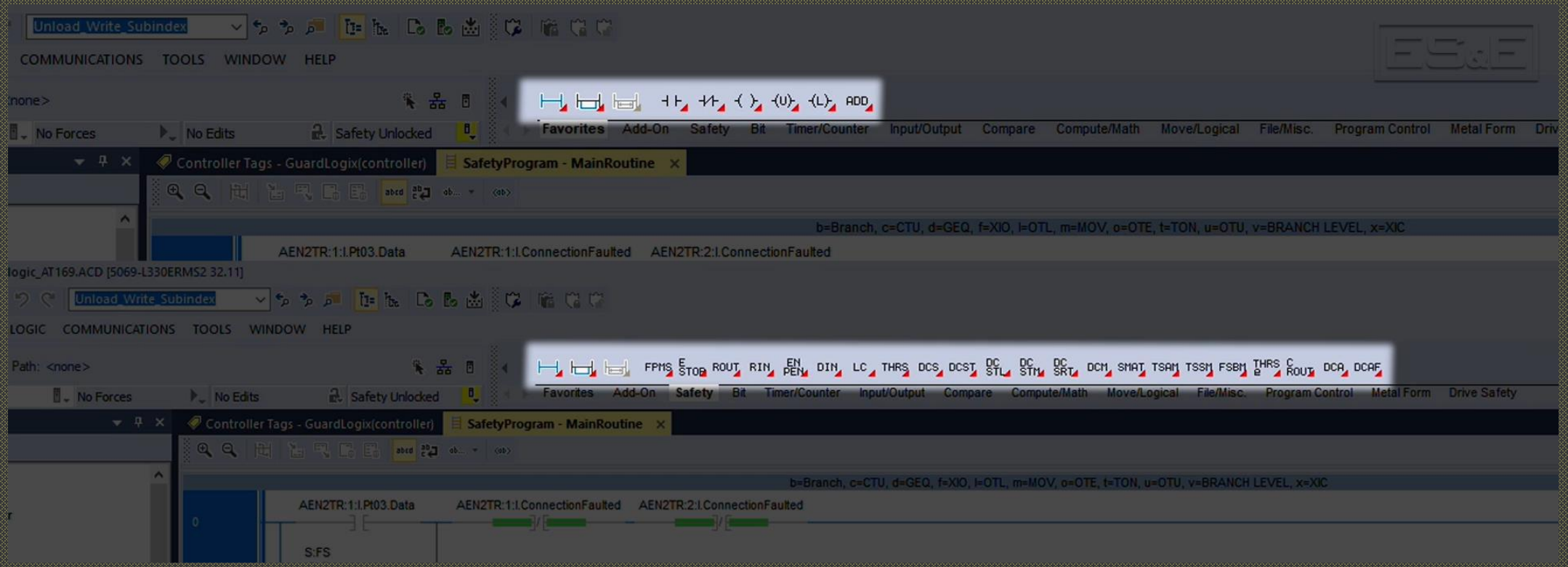


When working with Guard Logix Controllers, the program creates a periodic safety task that cannot be removed. This task will handle all the safety precautions and safety routines.

https://ese-co.com/knowledge/safety-tasks-tags-instructions-guardlogix-part-3

HUMBER

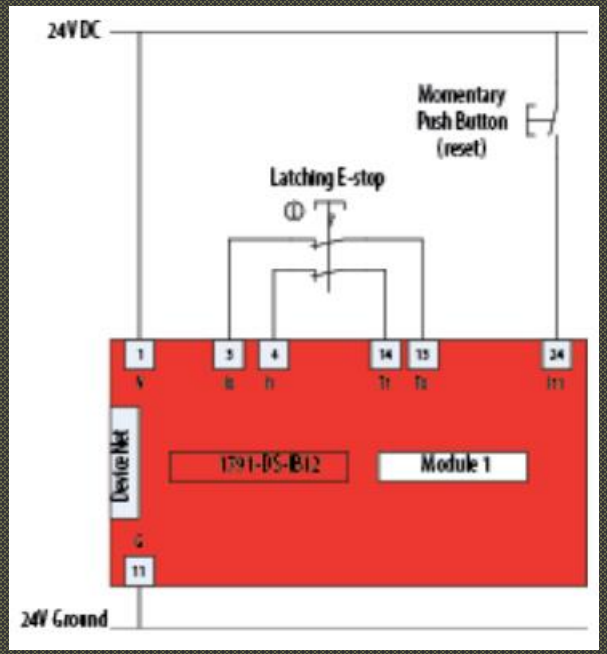
SYSTEM DESIGN

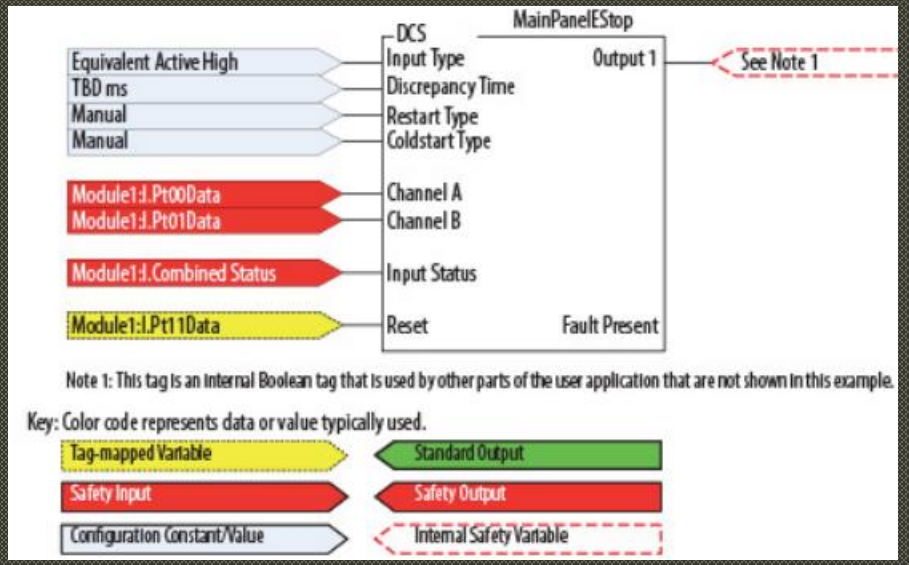


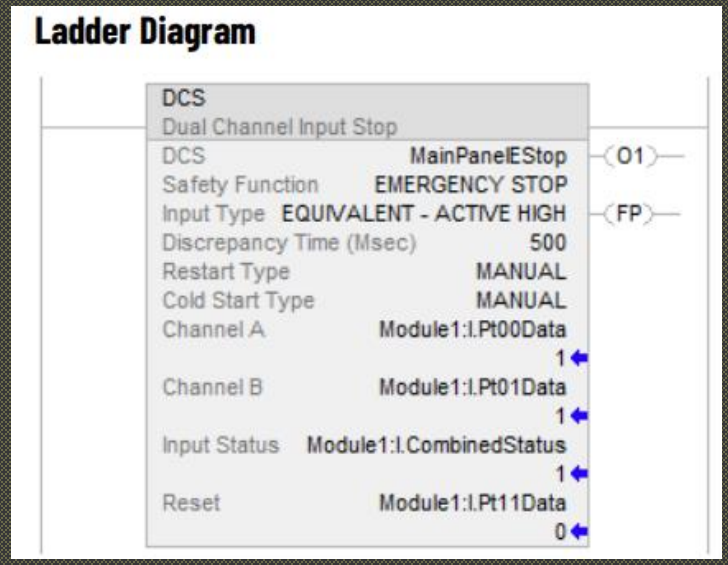
Safety instructions contain a red icon to differ from the standard instructions and are visible only when you are in the safety task.

https://ese-co.com/knowledge/safety-tasks-tags-instructions-guardlogix-part-3

DUAL CHANNEL INPUT STOP – DCS EXAMPLE







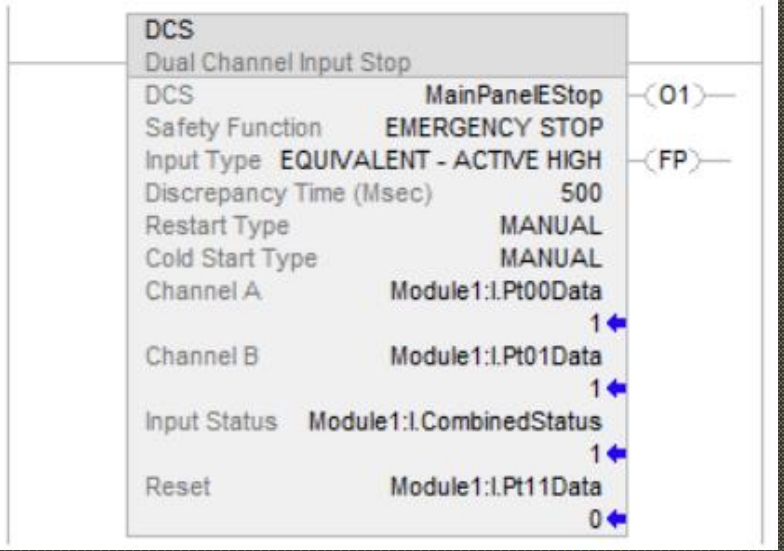
DCS monitors dual-input safety devices whose main purpose is to provide a stop function, such as an E-stop, light curtain, or gate switch.
This programming diagram shows the Dual Channel Input Stop (DCS) instruction with inputs and test outputs.

HUMBER

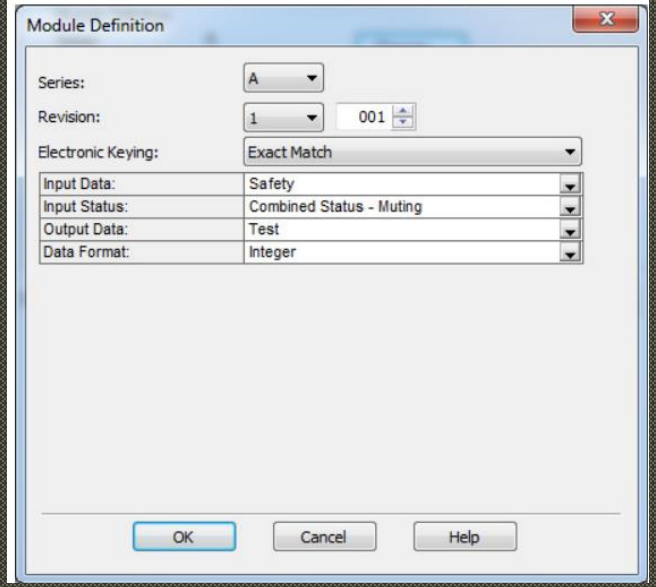
https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

DUAL CHANNEL INPUT STOP – DCS EXAMPLE

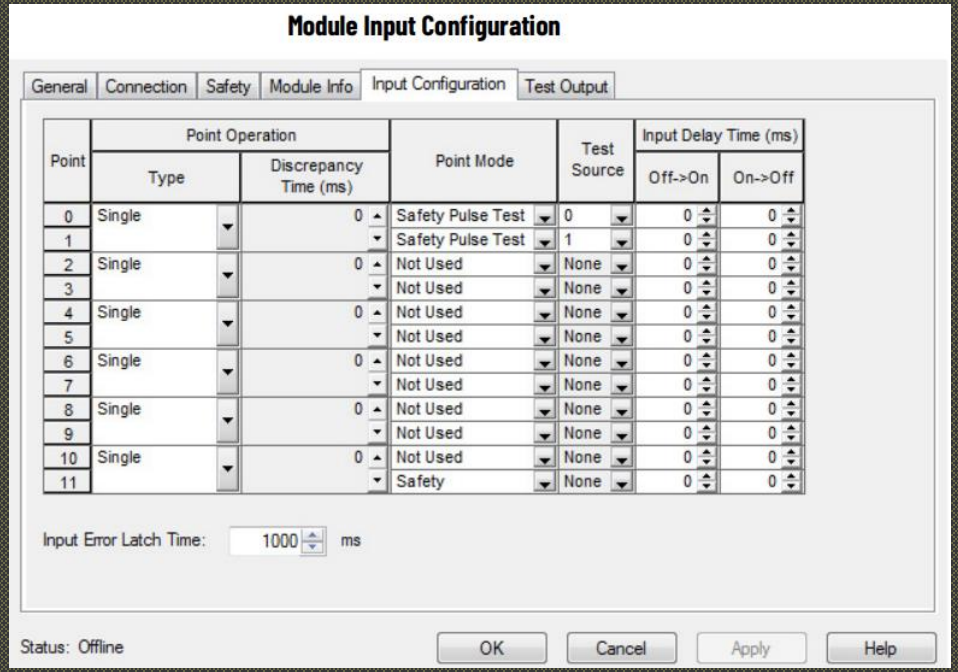
Ladder Diagram



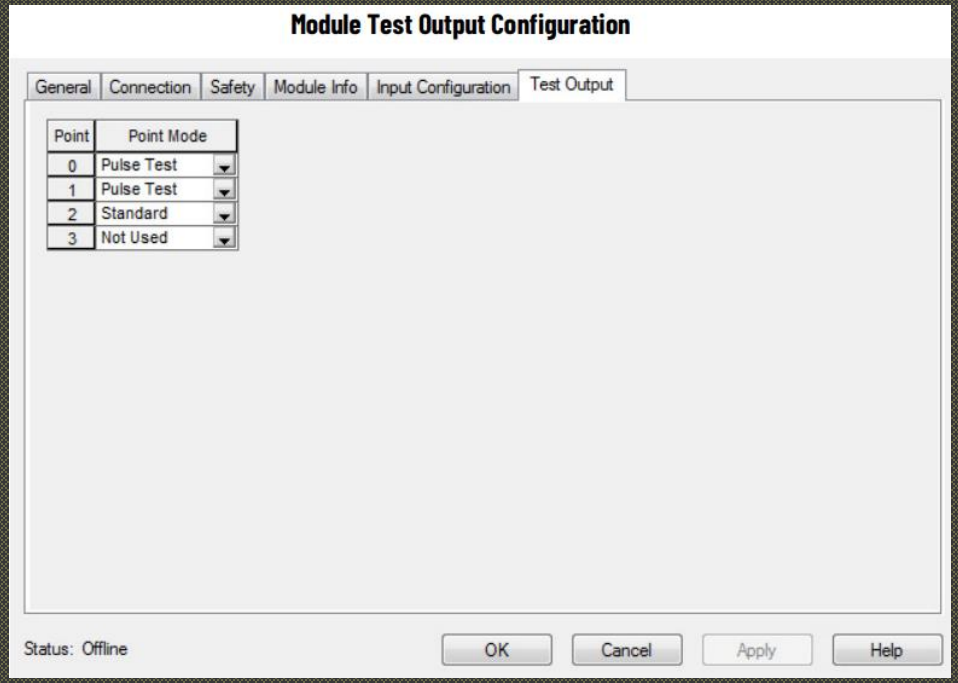
Module Definition



Module Input Configuration



Module Test Output Configuration



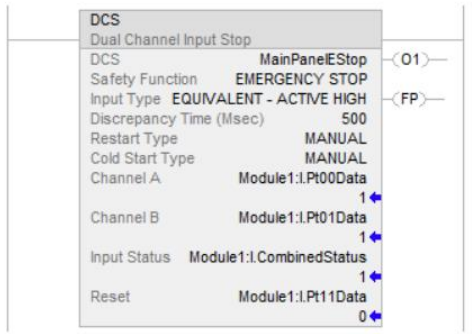
The programming software is used to configure the input and output parameters of the Guard I/O module, as illustrated.

HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

DUAL CHANNEL INPUT STOP – DCS EXAMPLE

Ladder Diagram



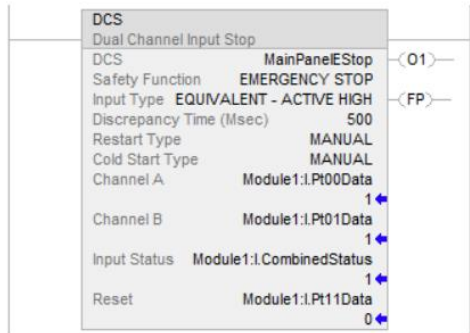
The Dual Channel Input Stop (DCS) instruction in Studio 5000 software is used to monitor dual-input safety devices, such as emergency stops, light curtains, or safety gates. Its primary function is to ensure that a machine stops safely when required. Here's a breakdown of how it works:

Operand	Type	Format	Description
DCS	DCI_STOP	tag	This parameter is a backing tag that maintains important execution information for each usage of this instruction. ⚠ **ATTENTION:** To avoid unexpected operation do not reuse this backing tag and its members. Do not write to any of the tag members anywhere else in the program.
Safety Function	DINT	name	This parameter provides a text name for how this instruction is being used. Choices include E-stop, safety gate, light curtain, area scanner, safety mat, cable (rope) pull switch, and user-defined. This parameter does not affect instruction behavior. It is for information/documentation purposes only.
Input Type	DINT	name	This parameter selects input channel behavior. **Equivalent (0):** Active High: Inputs are in the active state when Channel A and Channel B inputs are 1. **Complementary (2):** Inputs are in the active state when Channel A is 1 and Channel B is 0.
Discrepancy Time (ms)	DINT	immediate	The amount of time that the inputs can be in an inconsistent state before an instruction fault is generated. The inconsistent state depends on the Input Type. Equivalent: Inconsistent state is when: • Channel A = 0 and Channel B =1, or • Channel A =1 and Channel B =0 Complementary: Inconsistent state is when: • Channel A = 0 and Channel B =0, or • Channel A =1 and Channel B =1 The range is 5...3000 ms.
Restart Type	List	name	This input configures Output 1 for either Manual or Automatic Restart. **Manual (0):** A transition of the Reset input from OFF (0) to ON (1), while all of the Output 1 enabling conditions are met, is required to energize Output 1 **Automatic (1):** Output 1 is energized 50 ms after all enabling conditions are met. ⚠ **ATTENTION:** Automatic restart may only be used in application situations where you can prove that no unsafe conditions can occur as a result of its use, or the reset function is being performed elsewhere in the safety circuit (for example, output function).

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

DUAL CHANNEL INPUT STOP – DCS EXAMPLE

Ladder Diagram



Operand	Type	Format	Description
Cold Start Type	BOOL	name	This parameter specifies the Output 1 behavior when applying controller power or mode change to Run. **Manual (0):** Output 1 is not energized when the Input status becomes valid or when the Input Status fault is cleared. The device must be tested before Output 1 can be energized. **Automatic (1):** Output 1 is energized immediately when the Input status becomes valid or when the Input Status fault is cleared and both inputs are in their active state.

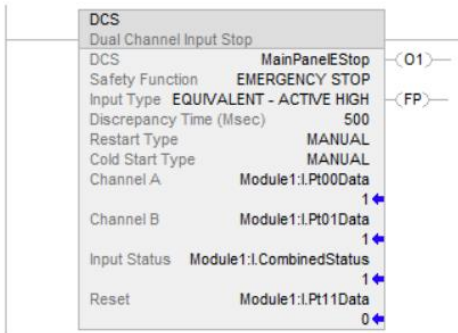
Operand	Data Type	Format	Description
Channel A[1]	BOOL	tag	This input is one of the two safety inputs to the instruction.
Channel B[1]	BOOL	tag	This input is one of the two safety inputs to the instruction.
Input Status	BOOL	immediate tag	If instruction inputs are from a safety I/O module, this is the status from the I/O module (Connection Status or Combined Status). If instruction inputs are derived from internal logic, it is the application programmer's responsibility to determine the conditions. ON (1): The inputs to this instruction are valid. OFF (0): The inputs to this instruction are invalid.
Reset[2]	BOOL	tag	If Restart Type = Manual, this input is used to energize Output 1 once Channel A and Channel B are both in the active state. If Restart Type = Automatic, this input is not used to energize Output 1. OFF (0) -> ON (1): The FP (Fault Present) and Fault Code outputs are reset.

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

HUMBER

DUAL CHANNEL INPUT STOP – DCS EXAMPLE

Ladder Diagram



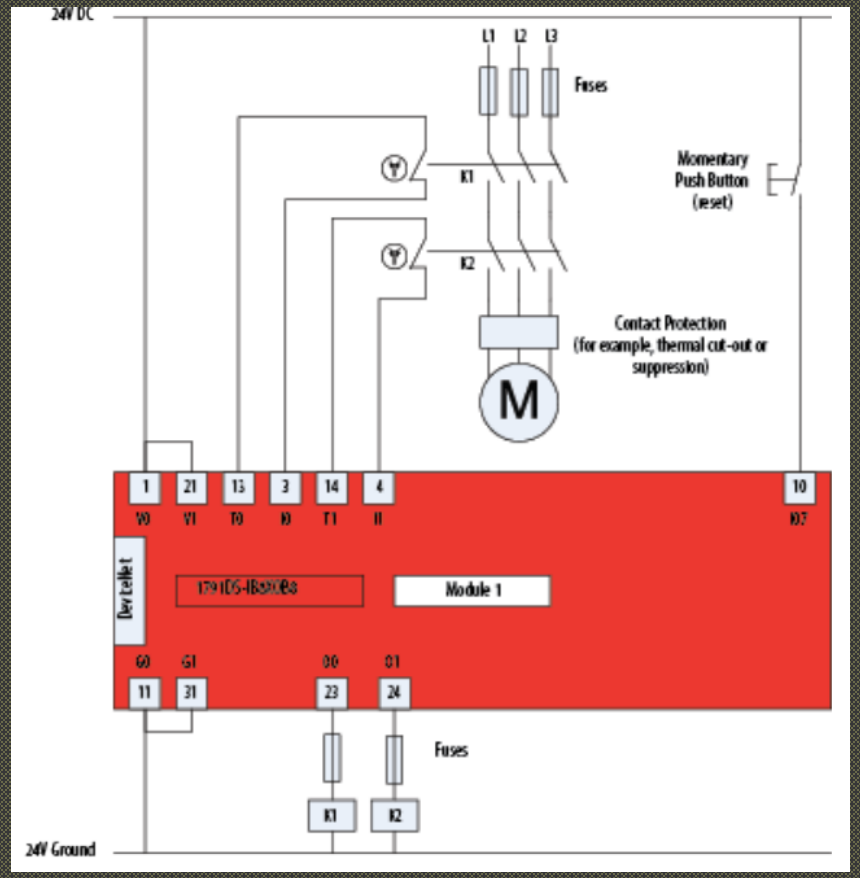
Operand	Data Type	Description
Output 1 (O1)	BOOL	This output is energized when the input conditions have been satisfied. The output becomes de-energized when: • Either Channel A or Channel B transitions to the safe state. • The Input Status is in the safe state.

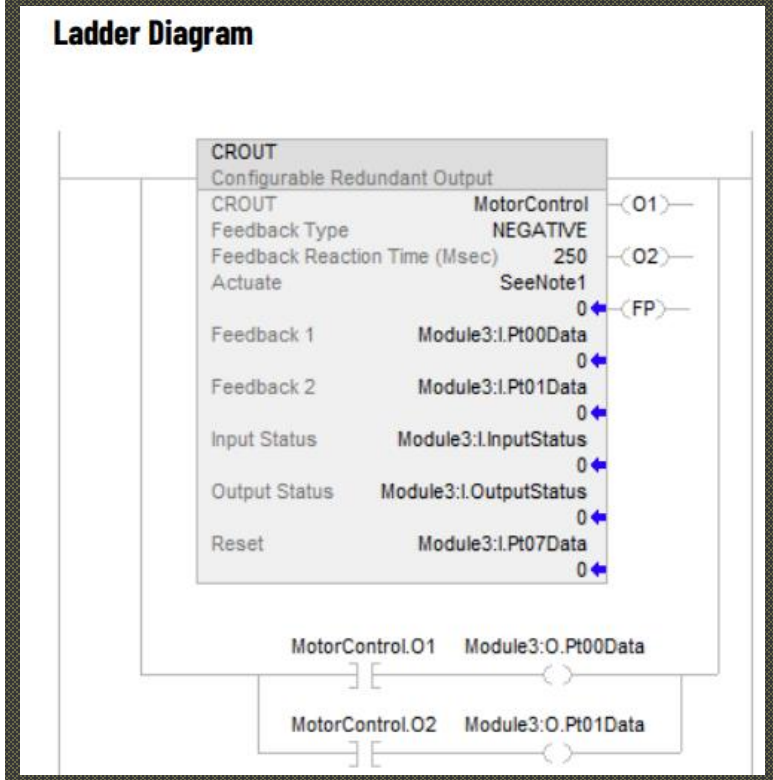
Operand	Data Type	Description
Fault Present (FP)	BOOL	ON (1): A fault is present in the instruction. OFF (0): This instruction is operating normally.
Fault Code	DINT	This output indicates the type of fault that occurred. See the Fault Codes section for a list of fault codes. This parameter is not safety-related.
Diagnostic Code	DINT	This output indicates the diagnostic status of the instruction. See the Diagnostic Codes section for a list of diagnostic codes. This parameter is not safety-related.

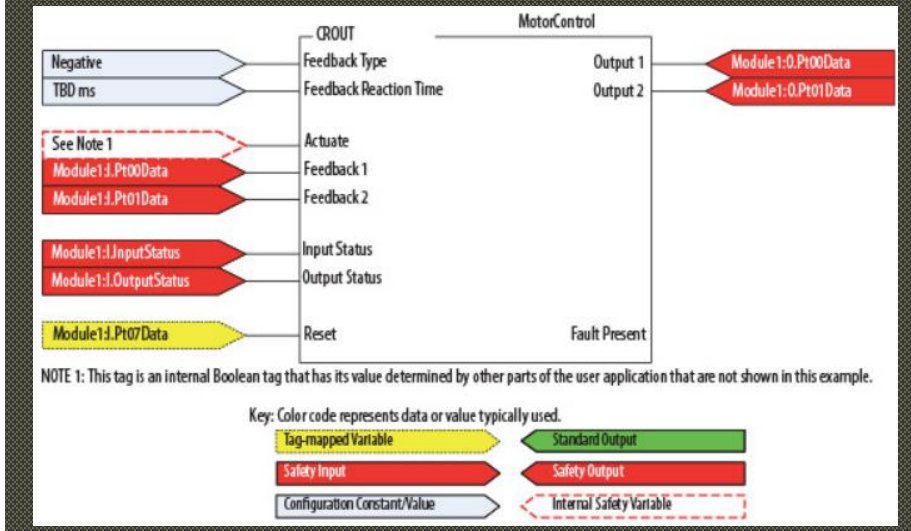
HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

CONFIGURABLE REDUNDANT OUTPUT - CROUT EXAMPLE







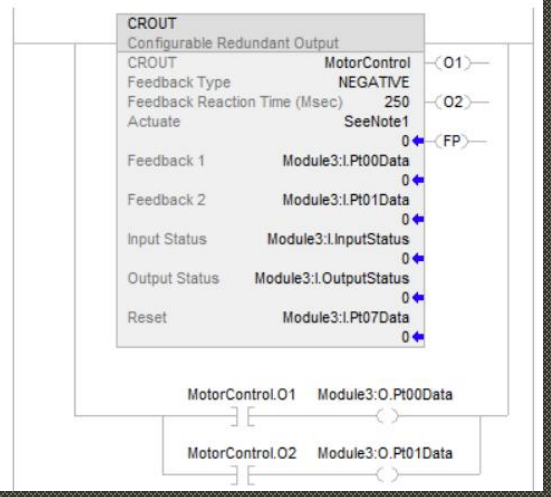
CROUT controls and monitors redundant outputs.
The CROUT instruction has input status for Feedbacks 1 and 2, and output status for the output channels driven by the CROUT outputs O1 and O2. The status tags used in these instructions must be HI (1) for the safety instruction output tag(s) with O1 for input instructions and O1/O2 to energize the CROUT instruction.

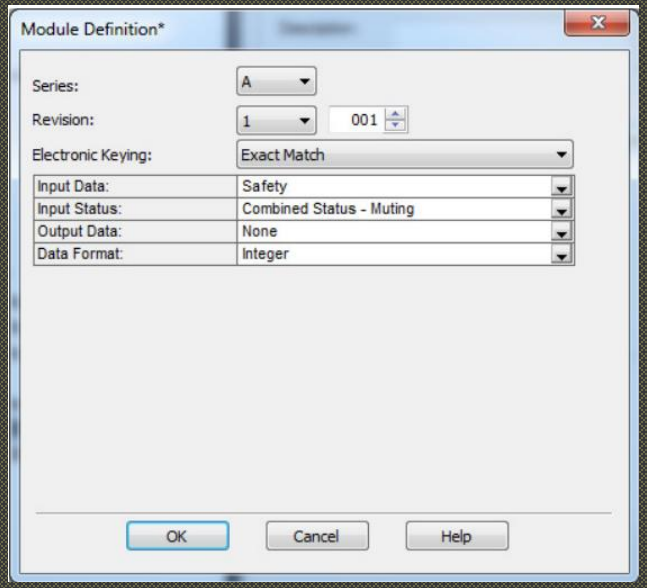
HUMBER

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

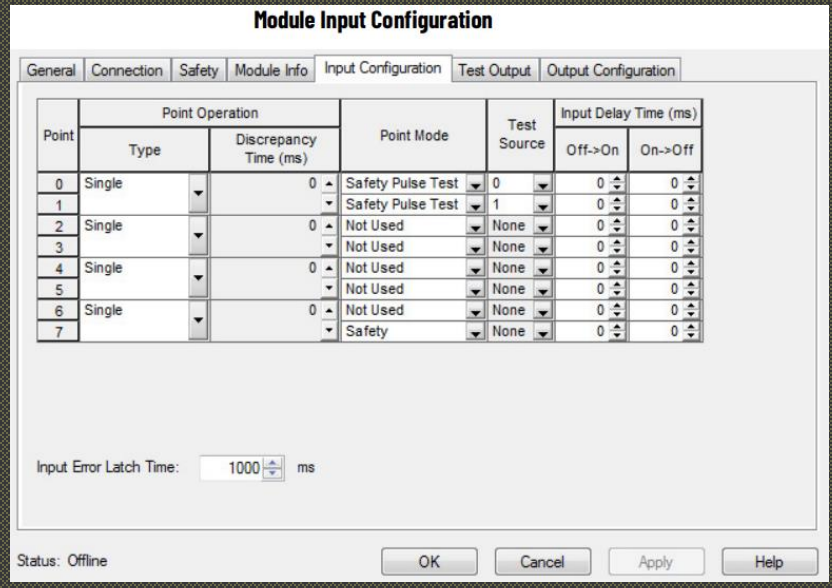
CONFIGURABLE REDUNDANT OUTPUT - CROUT EXAMPLE

Ladder Diagram

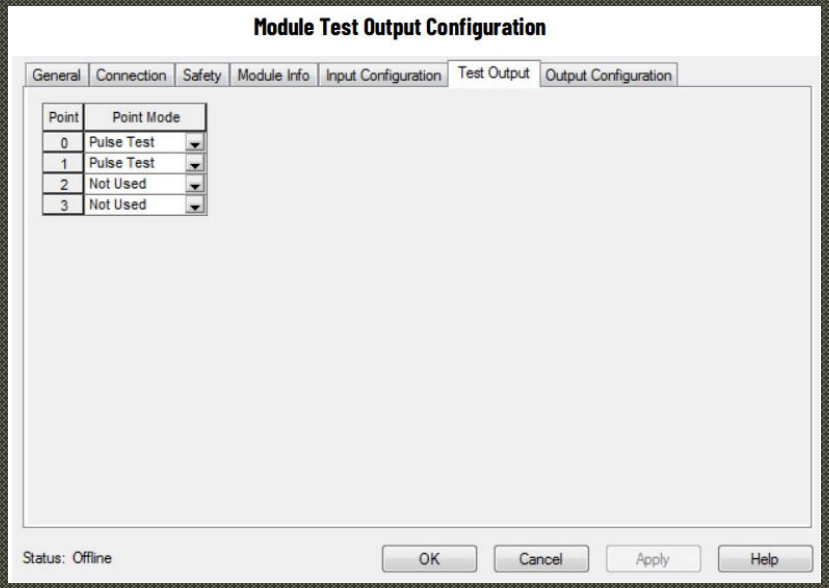




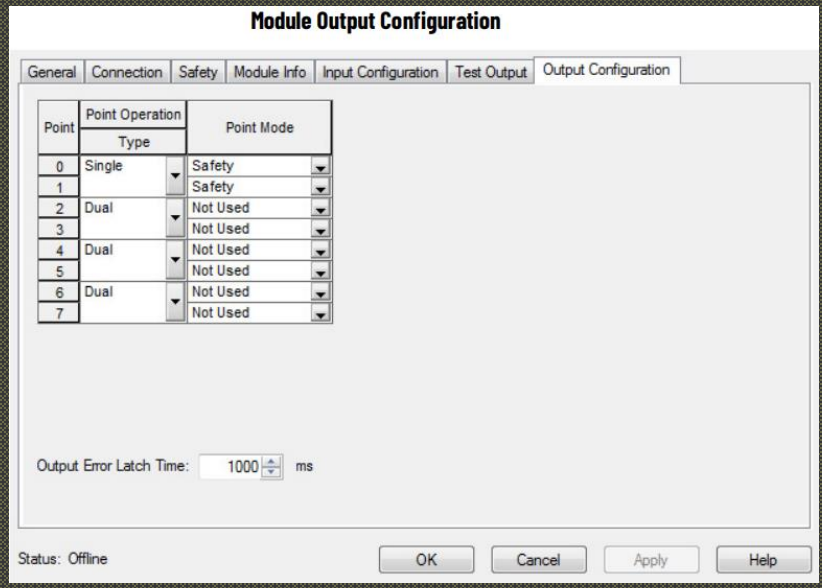
Module Input Configuration



Module Test Output Configuration



Module Output Configuration

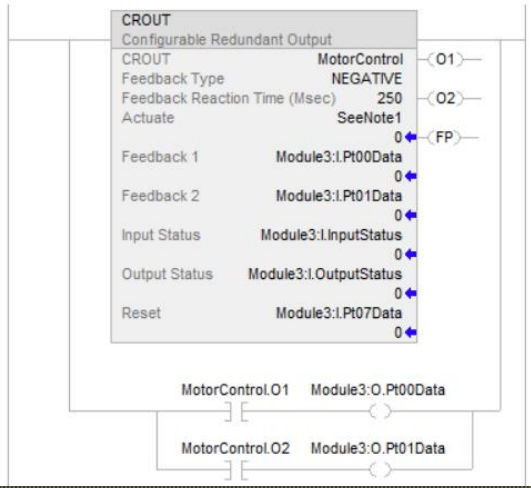


https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

HUMBER

CONFIGURABLE REDUNDANT OUTPUT - CROUT EXAMPLE

Ladder Diagram



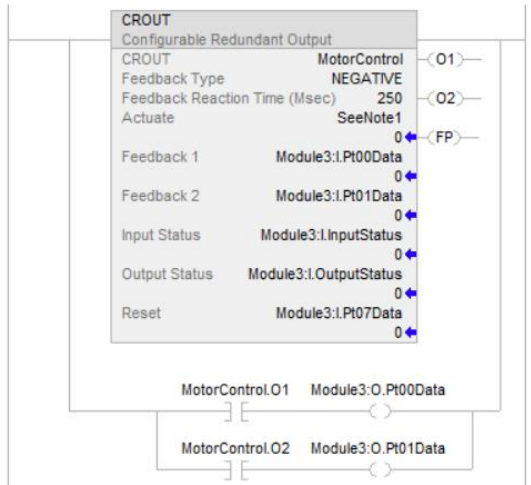
Operand	Data type	Format	Description	
CROUT	CONFIGURABLE_ROUT	tag	CROUT structure	
Feedback Type	BOOL	Drop-down	This operand defines the feedback ON and OFF states.	
			Positive (1)	ON (1): Feedback 1 ON, Output 1 ON. OFF (0): Feedback 1 OFF, Output 1 OFF.
			Negative (0)	ON (1): Feedback 1 OFF, Output 1 ON. OFF (0): Feedback 1 ON, Output 1 OFF.
Feedback Reaction Time	DINT	immediate	This operand specifies the amount of time that the instruction waits for Feedback 1 and Feedback 2 to reflect the state of Output 1 and Output 2 as specified by the configured Feedback Type. The valid range is 5 to 1000 ms.	

Operand	Data Type	Format	Description
Actuate	BOOL	tag	This input energizes or de-energizes Output 1 and Output 2. ON (1): Output 1 and Output 2 are energized if no faults exist. OFF (0): Output 1 and Output 2 are de-energized.
Feedback 1	BOOL	tag	This input is constantly monitored to make sure that it reflects the state of Output 1. When Output 1 transitions, this input must detect the transition within the Feedback Reaction Time.
Feedback 2	BOOL	tag	This input is constantly monitored to make sure that it reflects the state of Output 2. When Output 2 transitions, this input must detect the transition within the Feedback Reaction Time.

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

CONFIGURABLE REDUNDANT OUTPUT - CROUT EXAMPLE

Ladder Diagram



Operand	Data Type	Format	Description
Input Status	BOOL	tag immediate	If instruction inputs are from a safety I/O module, this is the status from the I/O module or modules (Connection Status or Combined Status). If instruction inputs are derived from internal logic, it is the application programmer's responsibility to determine the conditions. ON (1): The inputs to this instruction are valid. OFF (0): The inputs to this instruction are invalid.
Output Status	BOOL	tag immediate	This input indicates the output status of the I/O module or modules used by this instruction. ON (1): The I/O connection and the I/O module are operational. OFF (0): The module has a fault or the connection to the module has been lost.
Reset[1]	BOOL	tag	This input clears the instruction faults provided the fault condition is not present. OFF (0) -> ON (1): The FP and Fault Code outputs are reset.

Operand	Data Type	Description
Output 1 (O1)	BOOL	This output is used to control one channel of a two channel output device. Output 1 is de-energized when 1 or more of the following occurs: • A feedback fault occurs. • Input Status or Output Status inputs become invalid (OFF = 0). • The Actuate input turns OFF (0).
Output 2 (O2)	BOOL	This output is used to control one channel of a two channel output device. Output 2 is de-energized when 1 or more of the following occurs: • A feedback fault occurs. • Input Status or Output Status inputs become invalid (OFF = 0). • The Actuate input turns OFF (0).
Fault Present (FP)	BOOL	ON (1): A fault is present in the instruction. OFF (0): The instruction is operating normally.
Fault Code	DINT	This output indicates the type of fault that occurred. See the Fault Codes section below for the list of fault codes. This parameter is not safety-related.
Diagnostic Code	DINT	This output indicates the diagnostic status of the instruction. See the Diagnostic Codes section below for a list of diagnostic codes. This parameter is not safety-related.

ISO 13849-1 stipulates instruction reset functions must occur on falling edge signals.

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1756-rm095_-en-p.pdf

TROUBLESHOOTING, COMMUNICATION PROBLEMS AND DIAGNOSTICS

Erickson, K. (2016) Programmable logic controllers: An emphasis on design and application (3rd edition). Rolla MO: Dogwood Valley Press.

Chapter 15

Thank you!

Discussions?