Essentials of Machine Controls
Safety Considerations

Heinz E. Knackstedt
TÜV Functional Safety Engineer
C&E Sales, Inc.
677 Congress Park Drive
Dayton Ohio 45459
Phone: (800) 228-2790 x112
Email: hknackstedt@cesales.com
Cell (937) 545-6494

OBJECTIVE

- Encourage participation and free discussions on the subject of application and design of the safety related parts of the control system
- Identify the basic concepts which may be applied to any machine tool or assembly machine control based risk reduction, including robots and fluid power
- Definition of risk reduction requirements
- Review of the risk reduction circuit categories as defined by EN 954-1996, ISO 13849-1:1999 RIA 15.06:1999, ANSI B11.0 and B11.19 through the use of example circuits
- Review control design basics as the backbone of the “new” ISO 13849-1:2006

Overview

- Design of safety circuits for robotic applications typically employ management of hazards from auxiliary equipment
- Injury from robotic applications are frequently caused, not by the robot, but from this equipment
- The risk assessment must identify all sources of harm, not only the robot
- The risks from all hazards to which an individual can be exposed while attending the robot must also be reduced to an acceptable level
- The principles and circuits discussed are generic and may be applied to safety control circuits regardless of task.

References

- ANSI/ISO 12100:2011
- ANSI/RIA/ISO 10218-1:2007
- B11.0:2010
- B11.19:2010
- B11-TR6-2010 (B11.26)
- NFPA 79:2007
- OSHA CFR 29 Part 1910
- RIA 15.06: 2012
- RIA 15.06 TR306 DRAFT:2013
- EN 954-1:1996
- IEC 61496-1:1998
- ISO 10218-2:2010
- ISO 13849-1:1999
- ISO 13849-1:2006
- ISO 14119 : 2013

Warning:

The intent of the diagrams offered is as a suggestion only. These diagrams simply show, in general, how the listed performance is obtained, and may vary with specific product or application requirements.

These diagrams are not designed for any specific application or purpose nor to meet a specific application or functional requirement.

Capabilities and features of devices vary by manufacturer. If specific information is needed, contact the manufacturer directly. Failure to obtain specific product feature capability and assembly instructions could result in injury or death.

Compliance to Federal, State, and Local requirements and safety standards in any application is the responsibility of the end user.

MACHINE SAFETY IS ***NOT*** AN OPTION!

The ***General Duty Clause*** 5(a) (1) of the

OSH Act-1970 Public Law 91-596

requires that:

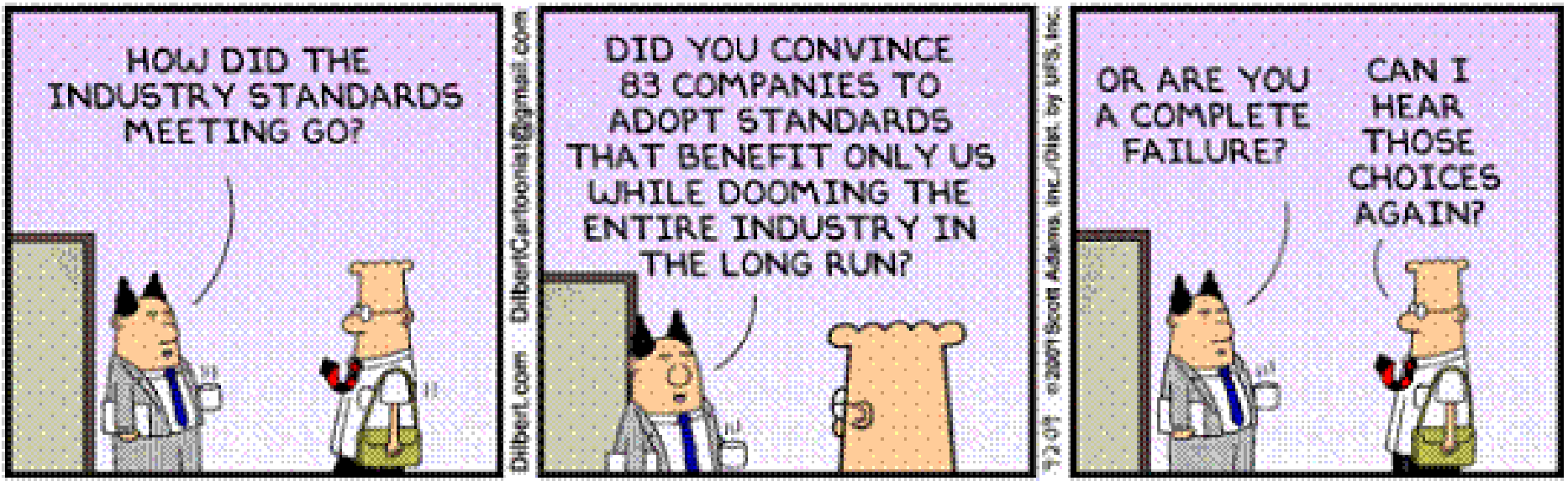
> ***Each employer shall furnish to each of his employees, employment and a place of employment, which is free from recognized hazards that are causing or are likely to cause death or serious physical harm***

Consensus standards help to identify hazards and measures by which acceptable risk may be attained

Consensus Standards

- We hear a lot about them
- What are they?
- Where do they come from?
- Who writes them

An **unfounded** rumor



Dilbert on Standards

Risk and its Reduction for Industrial Machinery

Risk is the "combination of the likely **severity of harm** and the **probability of occurrence** of that harm"

ANSI/ISO12100-2010) ANSI B11.0:2010 formerly in B11-TR3

How to manage risk by its reduction to an acceptable level

Identify the level of risk by performing a Risk Assessment

- ANSI B11.0 "Safety of Machinery- General Requirements and Risk Assessment"
- ANSI/RIA R15.06 TR R15-306-2013 "Robot Risk Assessment"
- ANSI/ISO 12100-2010 "Safety of Machinery – Risk Assessment" now includes ISO 14121 "Principles of Risk Assessment"

Evaluate the risk Is it acceptable?

Then manage the risk using the Risk Reduction Hierarchy

1. Machine/Process Design to eliminate the hazard or to reduce the risk
2. Use of hierarchy of risk reduction measures to reduce risk by limiting exposure to the hazard
   - Fixed Guards
   - Safeguarding Devices
   - Complimentary Measures
3. Use of procedures, warnings, and PPE

What is the "Cost" of safe design

- Total resources in manpower, time, and funds to:
  - Design
  - Acquire
  - Build
  - Commission
  - Maintain functionality of original concept
- The last of these, Maintain Functionality, is often the most costly
- "Operating Cost" if the safety design fails to address the required tasks which must be performed
  - Labor Effort
    - Reach, Travel, Access,
- Each risk reduction effort, even on an existing machine, should first consider change in machine or process before "adding" risk reduction measures

- ***Operating Cost, in production rate and operator effort, can be substantial if a safeguard is not designed correctly***

Poor design is most often the <u>root cause</u> for the circumvention of risk reduction devices and measures

"Value" Analysis by the Operator

***<u>Effort of Use</u>* of risk reduction Measure**

..vs.....

<u>Perceived</u>* Risk and its resultant *<u>Reduction</u>

- **Influences impacting Safety Behavior**
  - **Perception**
    - **How dangerous is it, what is my personal risk ?**
  - **Habit**
    - **I've done it this way " 'cause that's the best way"**
  - **Obstacles**
    - **The safeguard makes it more difficult to ……..**
  - **Barriers**
    - **The safeguard prevents me from ……**

Without a "SAVINGS" the risk reduction measure will not be used

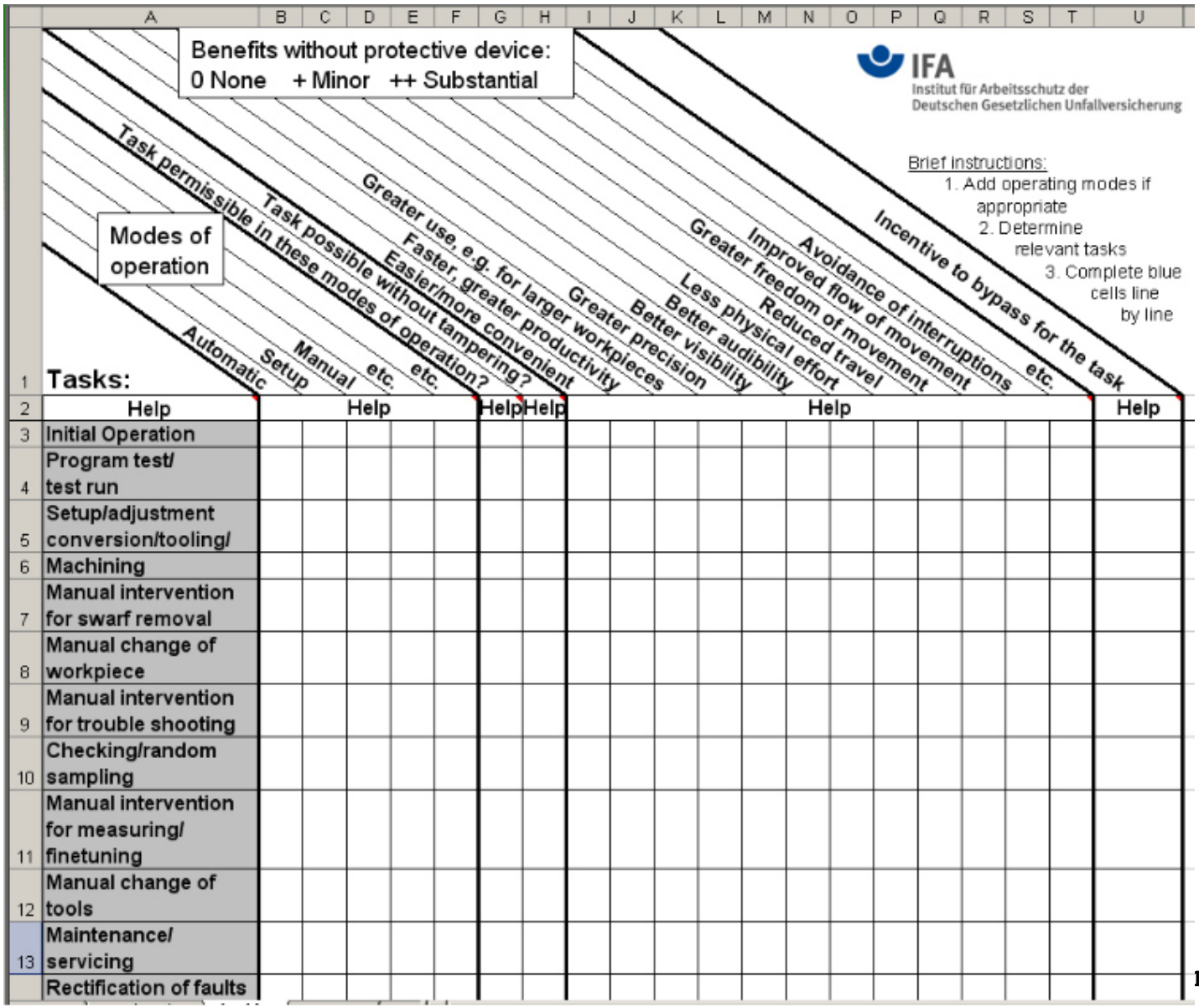
A "GOOD" safeguarding design addresses these concerns

The Safety Function

- Requirement the SRP/CS for each specific task/ hazard pair identified in the Risk Assessment
- Define the requirements of the safety function
  - What determines that exposure to the hazard is possible/imminent
    - Presence sensing
    - Interlocked access gates
    - Machine “Mode of Operation” selected
  - What hazards must be eliminated if access is gained
    - What is involved in the task
    - What controls and power are required
    - What auxiliary equipment exposure is possible
  - What device(s) can control/eliminate the hazard
  - MOST CRYTICAL STEP IN RISK REDUCTION PROCESS

One of the most effective means to increase the effectiveness of a risk reduction measure is to **remove the incentive to defeat it**

Incentive to Defeat Safeguards



Benefits without protective device:
0 None + Minor ++ Substantial

IFA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

Brief instructions:
1. Add operating modes if appropriate
2. Determine relevant tasks
3. Complete blue cells line by line

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	Modes of operation	Task permissible in these modes of operation?	Task possible without tampering?	Easier/more convenient	Faster, greater productivity	Greater use, e.g. for larger workpieces	Greater precision	Better visibility	Better audibility	Less physical effort	Reduced travel	Greater freedom of movement	Improved flow of movement	Avoidance of interruptions	etc.	Incentive to bypass for the task					
1	Tasks:	Automatic	Setup	Manual	etc.	etc.															
2	Help	Help					Help	Help	Help												Help
3	Initial Operation																				
4	Program test/ test run																				
5	Setup/adjustment conversion/tooling/																				
6	Machining																				
7	Manual intervention for swarf removal																				
8	Manual change of workpiece																				
9	Manual intervention for trouble shooting																				
10	Checking/random sampling																				
11	Manual intervention for measuring/ finetuning																				
12	Manual change of tools																				
13	Maintenance/ servicing																				
	Rectification of faults																				

Cause for Manipulation (Defeating) of Safeguarding Devices and Risk Reduction Measures

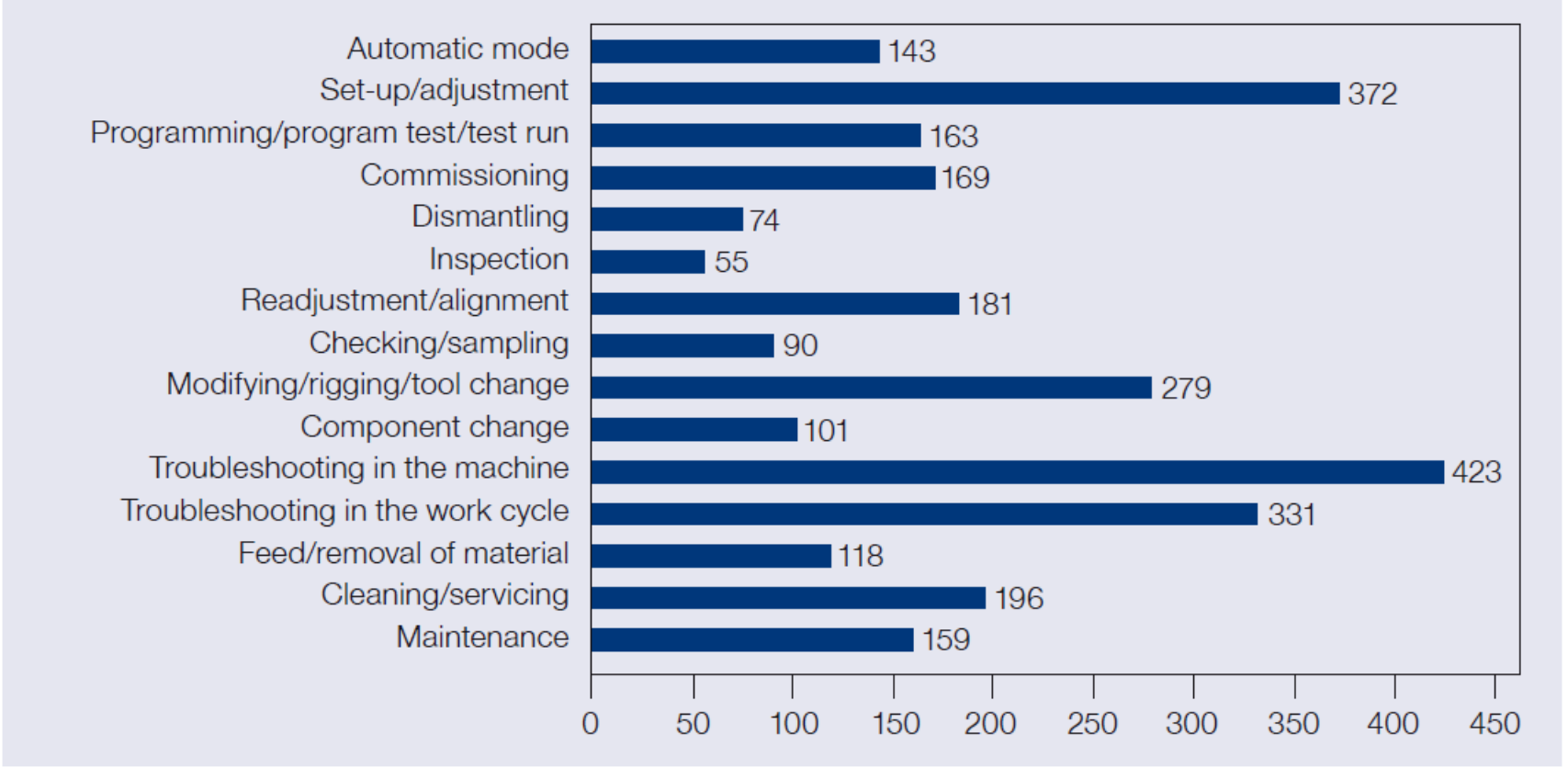
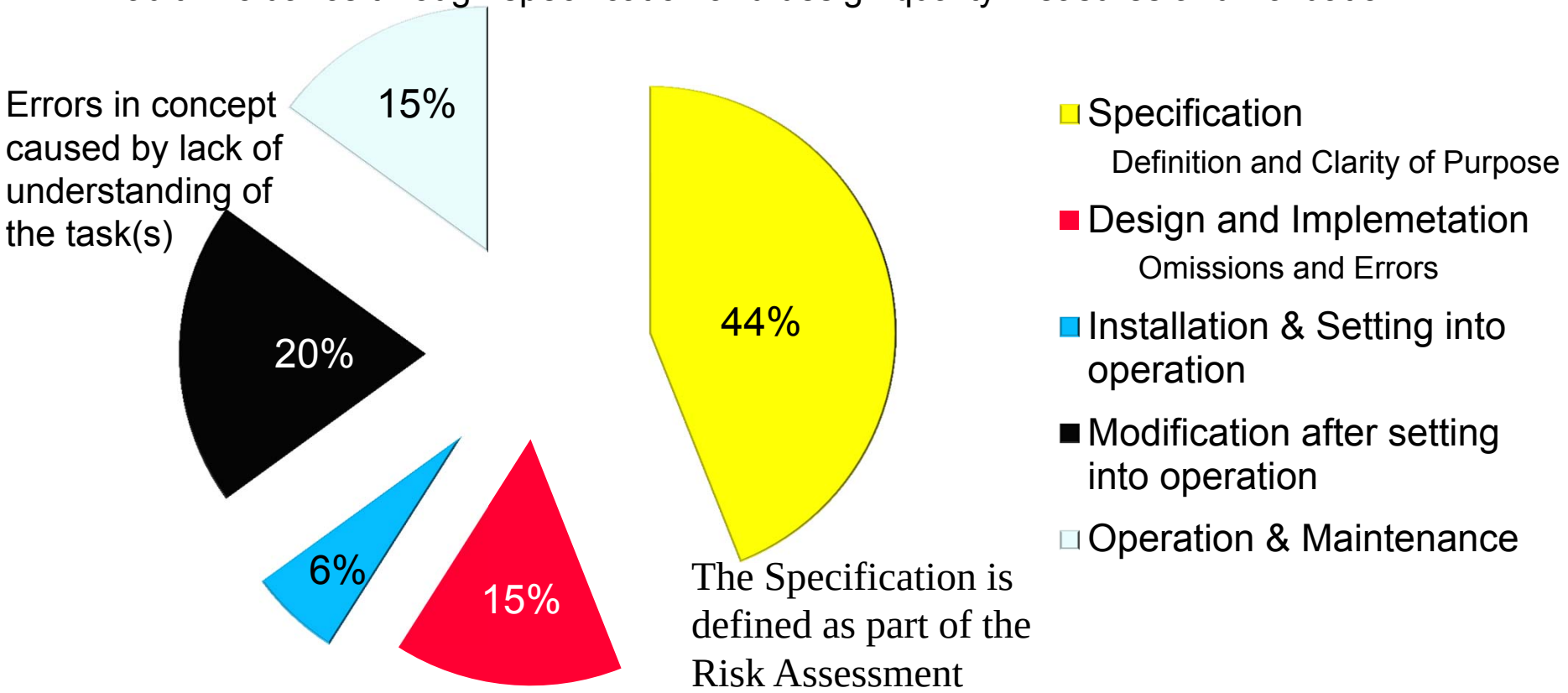


Fig. 12 Subjectively perceived "necessity" of manipulating protective devices according to operating modes (n = specifications as part of an empirical study; multiple answers possible)

Taken from Best of MRL-News "Safety of Machinery and Machine Control Systems" Schmersal/Elan publications Apr 2011

Causes of Process Safety Incidences
Safety Related Parts of the Control System (SRP/CS) did not provide the Required level of Risk Reduction

59% Already wrong before start of operation. These are **Quality** issues not Hardware Failures. Systematic errors which must be Reduced by Fault Avoidance through specification and design quality measures and Validation

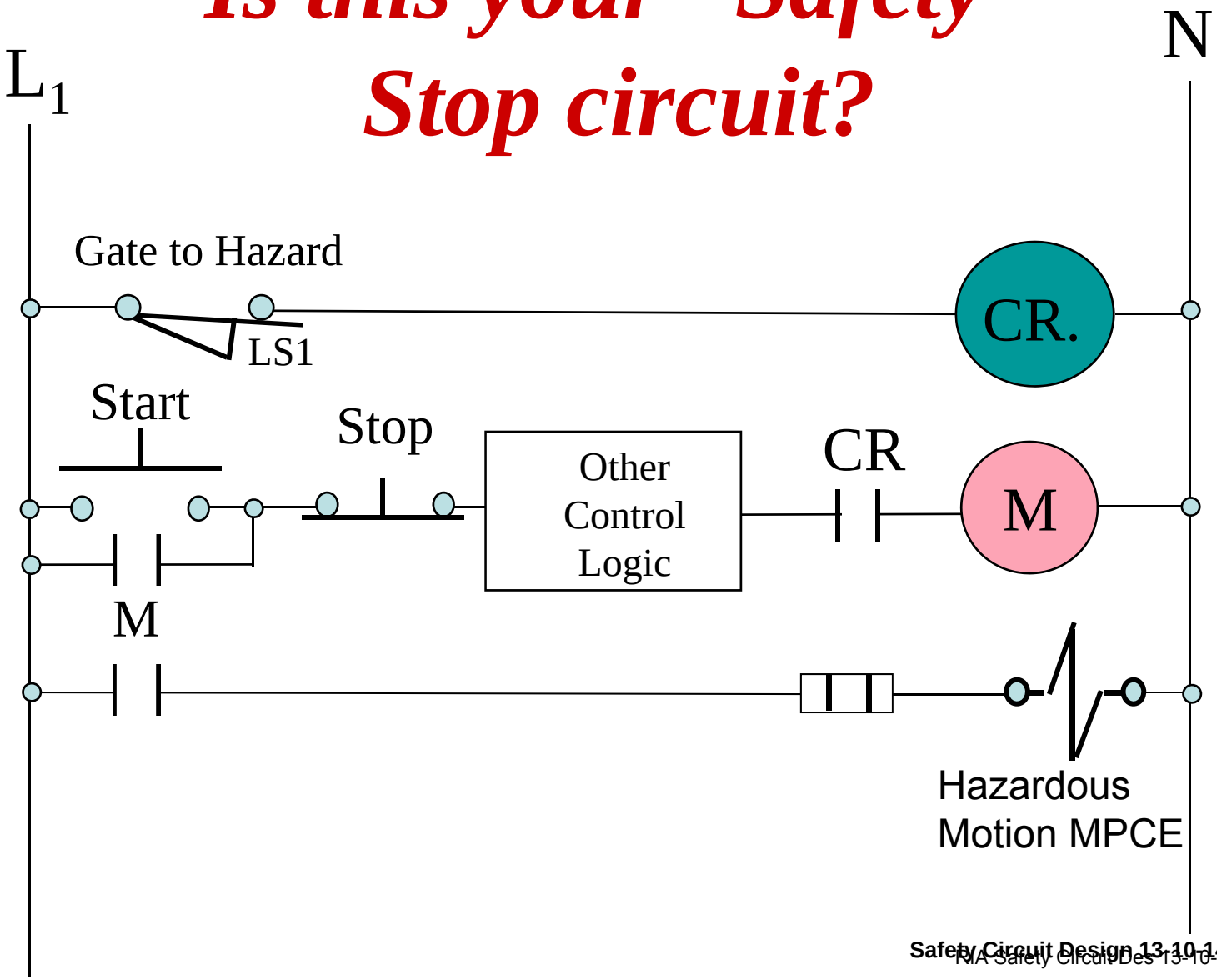


The Specification is defined as part of the Risk Assessment

ONLY 15% ARE FROM OPERATIONS AND RANDOM FAILURES

Source: "Out of Control" UK Health and Safety Executive (HSE) (September 2004)

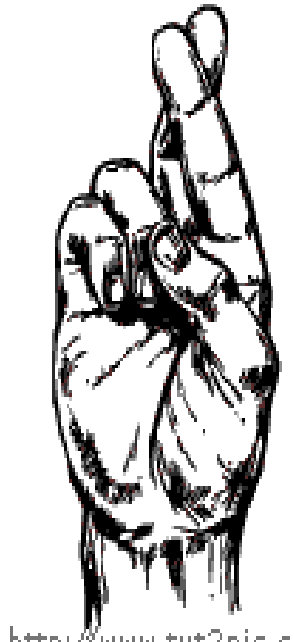
Is this your "Safety" Stop circuit?



If nothing ever failed, safety circuit design requirements *could* be met by any circuit which can eliminate the hazard

BUT……..

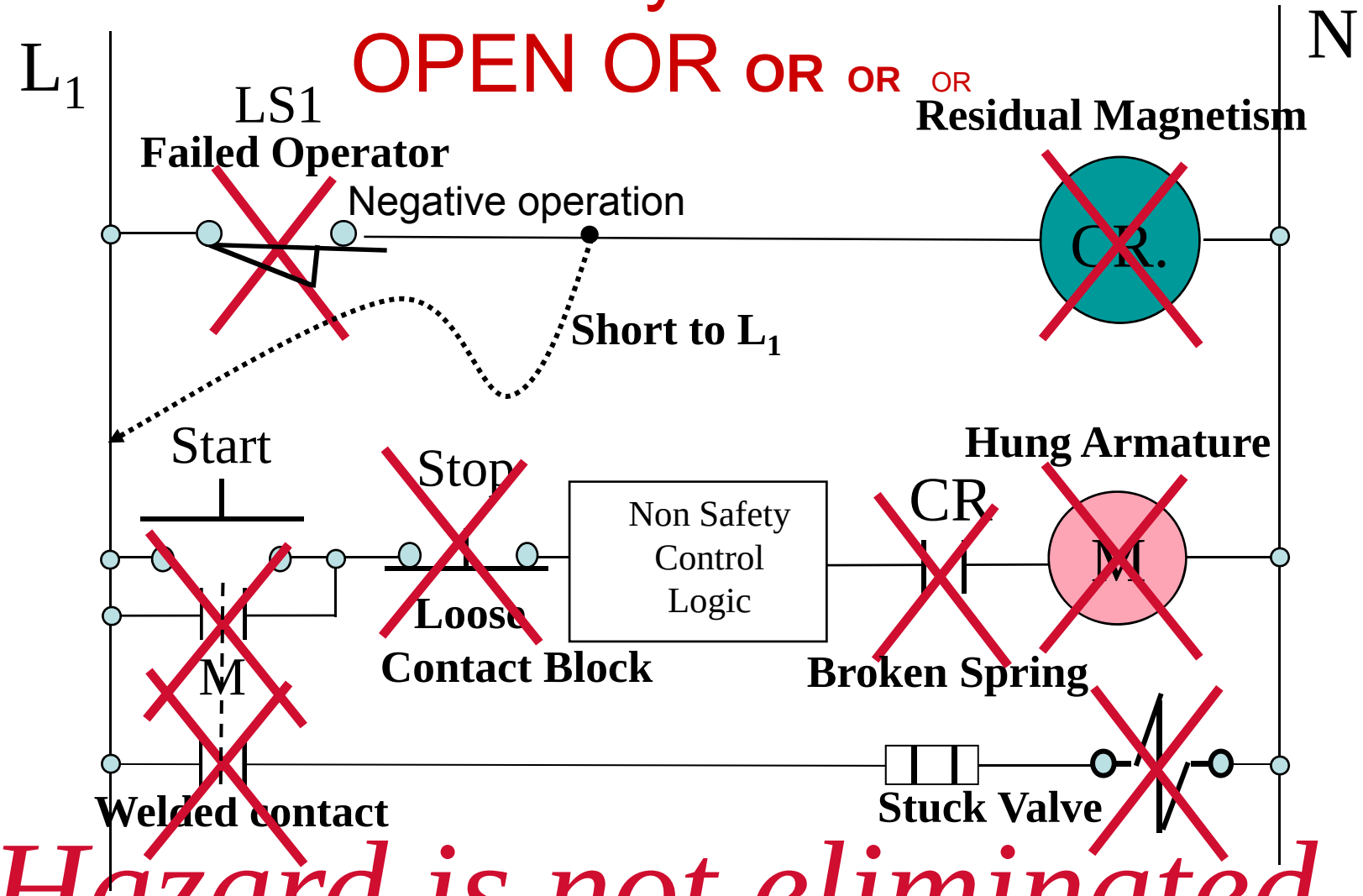
⚠ CAUTION ⚠



Is this the Back-Bone of your Safety Program?

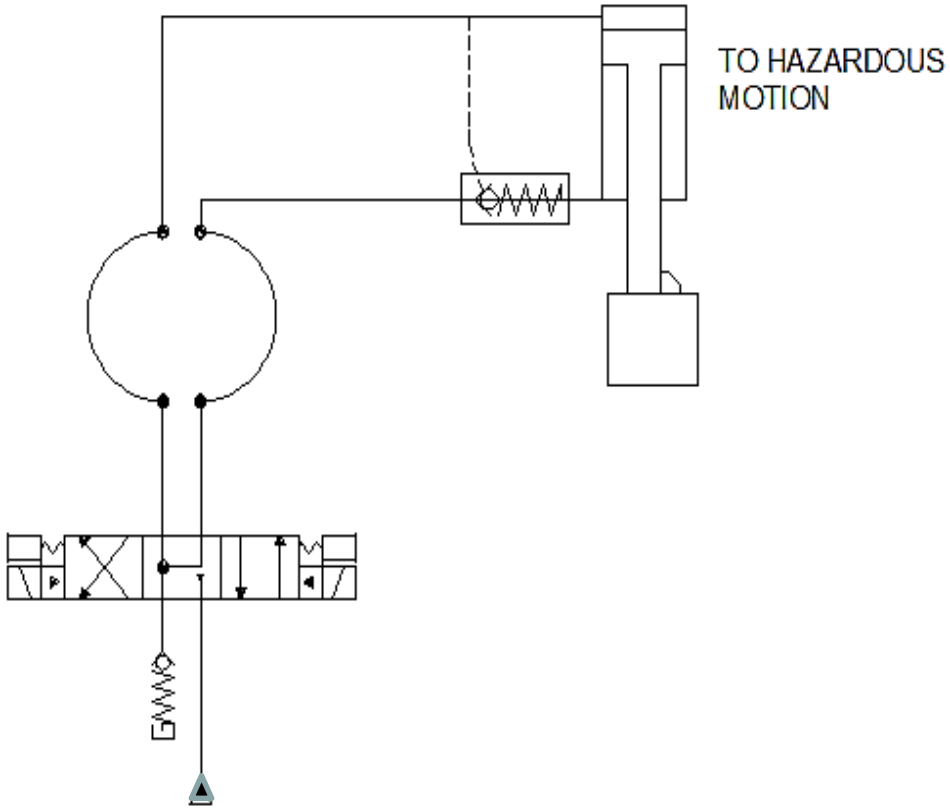
HOPE is not a safety strategy

What if the relay contact fails to OPEN OR OR OR OR



Hazard is not eliminated

Fluid Power is part of the SRP/CS



Removal of power from the solenoid(s) does not guarantee that the cylinder will stop its motion nor that it will stay in a given position

There are **only three** possible **results** due to a failure of the Safety Related Parts of the Control System SRP/CS designed to prevent exposure to a hazard:

1 Failure is detected automatically or by manual testing

A paradigm shift :
An **ACCIDENT** is an *unexpected* event,
usually with an undesirable result

2 Accident which results in a “close call” or “near miss”

Most (9 out of 10) injury accidents are preceded by one or more close calls

3 Accident which results in an injury

The variables which enabled the avoidance of the injury accident will not always be present in the same measure

Safety Design is a matter of managing the failures What are the options?

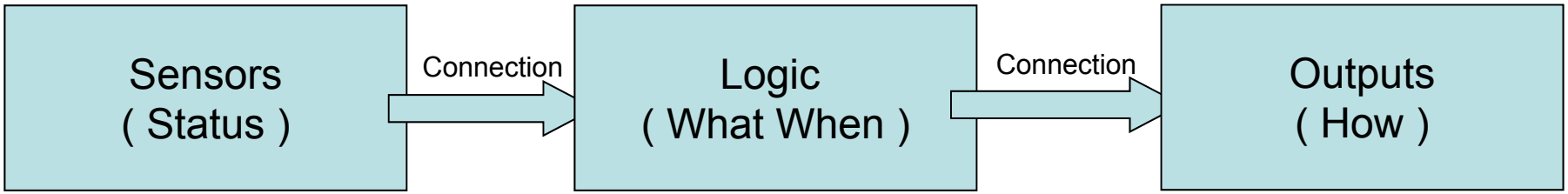
- Have such a low risk that failure of the risk reduction circuit to failure is acceptable
- Use Extremely large failure interval components so that failure is not a concern for the intended mission life
  - Impossible to accomplish over any reasonable length of use
- Manage the failures so that they do not cause the loss of the safety function
  - Assure that the safety function continues to eliminate the hazard with one failure
  - Detect that failure and shut down the hazard
  - Prevent further operation until the failure has been repaired

Functional Safety

- Functional Safety depends on the proper functioning of components and systems for the risk reduction
  - A Fixed Guard is not Functional Safety
  - An interlocked access gate which shuts down the drive of a hazardous machine is Functional Safety
- The failure of a component or sub-system to danger, increases the risk, typically back to its initial level
- To understand the failure mechanism of a circuit, a Functional Safety Block Diagram is developed

Safety Related Part of the Control System

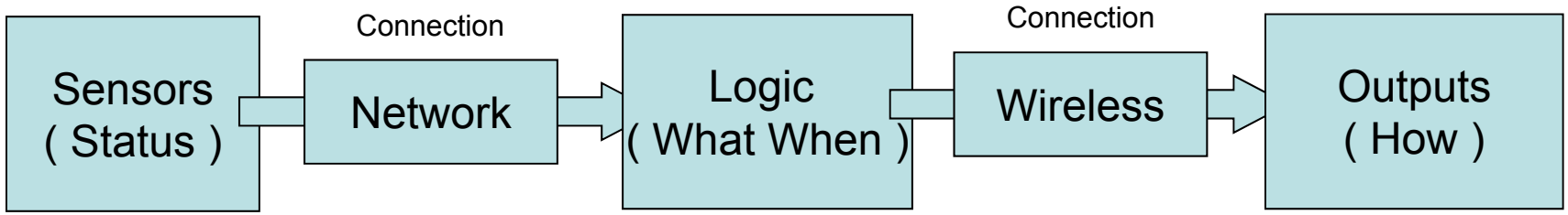
Functional Safety block diagram



Safety circuit block diagram

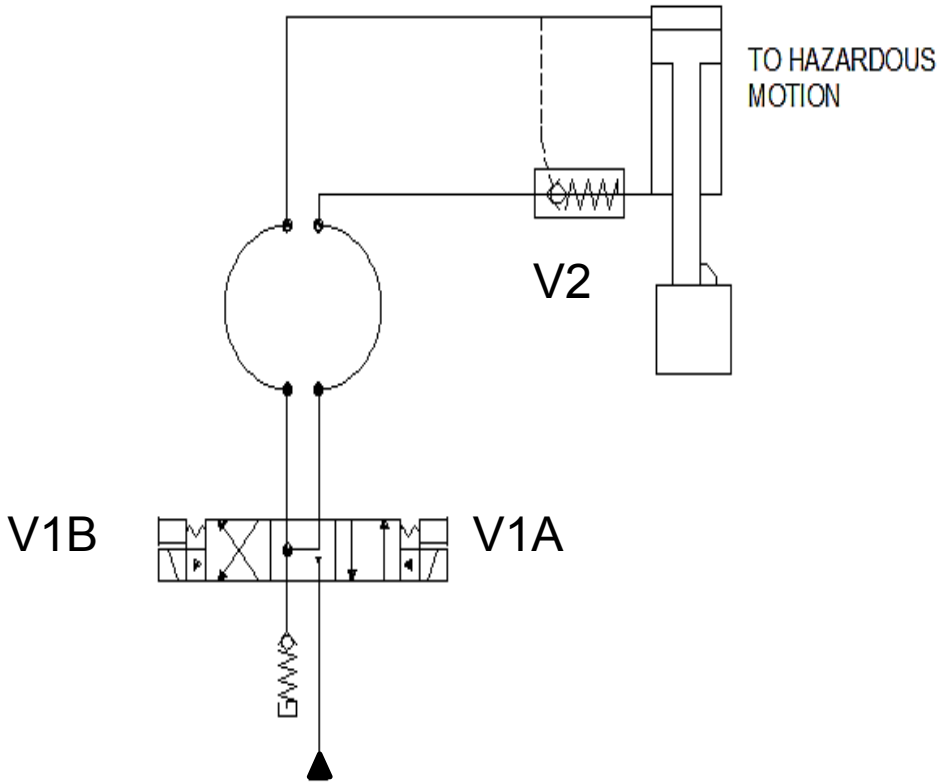
- Each circuit has at least these three elements of either :
  - Individual components
  - Sub-systems which perform that function
- To evaluate safety performance, each proposed SRP/CS must be broken into a block diagram of Series Safety Failure Events
  - This includes the possible failure modes of the interconnection of the blocks
- ***A failure in any block in the series safety block diagram, can lead to the loss of the safety function***
- ***Blocks in parallel require that both fail to lead to a loss of the safety function***

Example of Components in the failure loop

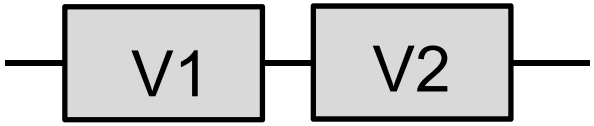


- Sensors
  - Who, What, Where
- Logic
  - For Safety PLC may be separate I/O devices
- Outputs
  - Safety PLC with discrete I/O components may have variations in fault tolerant capability which must be matched to the total system performance requirements
- Interconnection means
  - Technology used has specific failure modes
    - Addressed by the manufacturer as part of the device,
    - Considered by the SRP/CS designer as additional series blocks

Fluid Power is part of the SRP/CS



Remove pressure



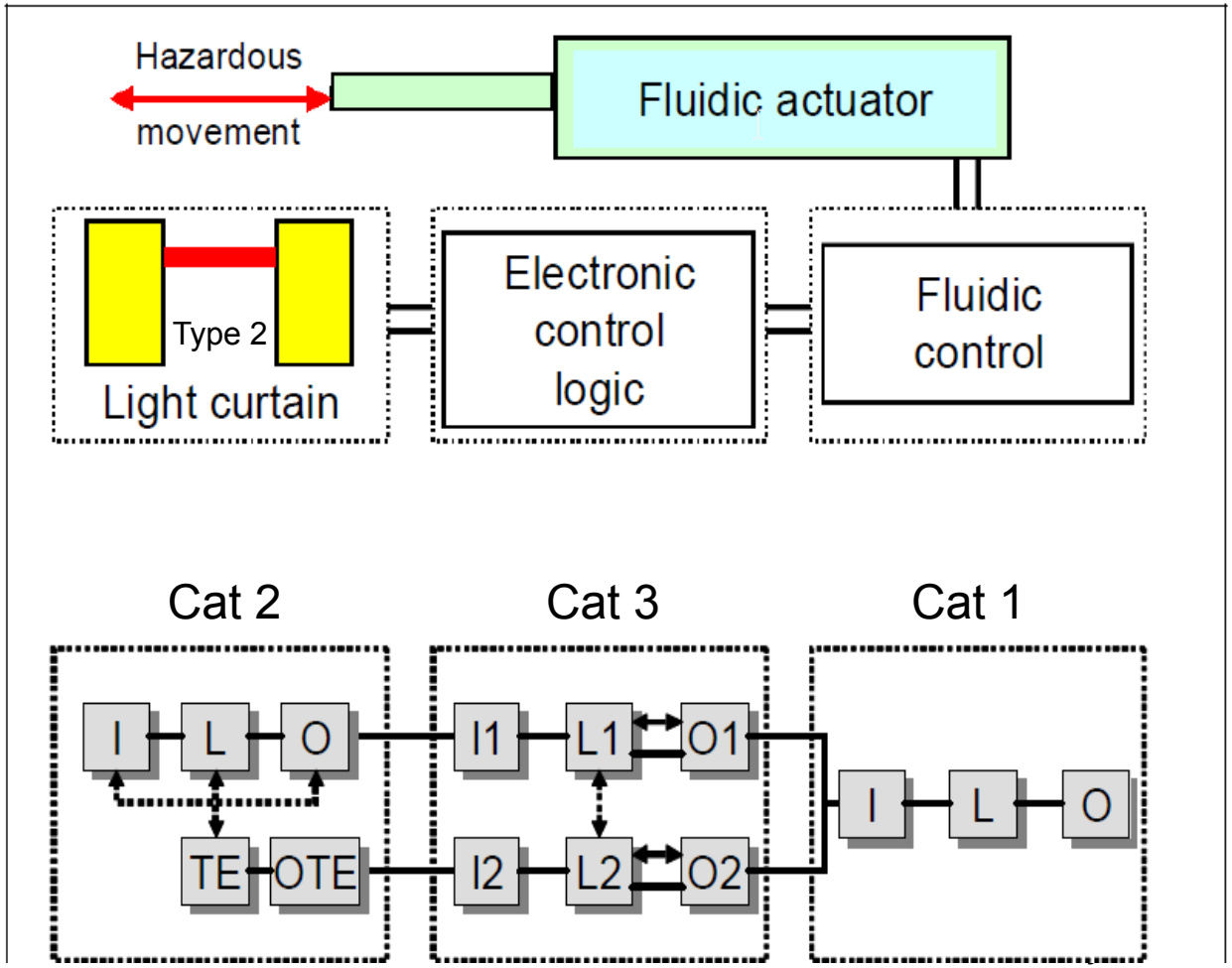
Prevent Motion at mid-stroke

Removal of power from the solenoid(s) does not guarantee that the cylinder will stop its motion nor that it will stay in a given position

V1 drains to tank which leads to unacceptable drift

Devices may be simple or complex sub-systems, each with its own individual S, L, and O functions

Figure 6.13:
Arrangement of subsystems in series for implementation of a safety function



Inputs

- Signaling devices which directly or indirectly detect the development of a hazardous situation
  - Design
    - Active or Passive
  - Function
    - Interlocked Access Gate
    - Safety Light Curtain and Laser Scanners
    - Safety Mat
    - Two Hand Anti-Tie-Down
    - Estop device
- Their status is passed on to the logic element for monitoring, interpretation, and interface to the output device(s)

Logic Function
Capability varies with device/vendor

- Receive and interpret the status of the input devices
- Execute logic functions and set the state of the output device(s)
- Monitor and Detect failures of input and output devices
- Detect internal failures
- Generate failure response output command
- Provide certified safety logic functions
- On complicated systems manage change and records

Commercial Safety Logic Devices

- Safety Interface Modules SIM
  - Formerly known as Safety Relay
- Configurable SIM
- Programmable SIM
- Programmable Safety Controllers
- Safety PLC
  - Safety Only
  - Safety and Control Logic
- Distributed Safety Controls
  - Remote I/O may have micro processors to pre-process the monitor function to unload PLC
  - Physical media Networks
    - Wire
    - Optical Fiber
  - Wireless Safety

Outputs

- Can be intermediate outputs which are still in the pilot control circuit of a sub-system
  - EX: OSSD of a safety light curtain
- **M**achine **P**rimary **C**ontrol **E**lements MPCE
  - That device(s) which physically interrupts the flow of power from the power source to the hazard
  - The last device in the control chain to operate to initiate the hazard
    - Contactor
    - Fluid Power Valve
    - Variable Frequency Drive, Servo Drive, Robot Controller
  - Controlled by the pilot device of the SRP/CS
  - Removal of **CONTROL (PILOT)** power from the MPCE does **NOT** guarantee removal of the power from the hazardous device if the MPCE fails to function correctly
  - Failure of MPCE device to isolate the power flow to the hazard, constitutes a failure to danger

Fluid Power Considerations

- Hazardous motion Actuator must be:
  - Isolated from the pressure source
  - Residual trapped pressure which can cause motion vented
  - Held in position if affected by gravity
  - Consider load creep due to valve or cylinder piston blow-by
- Pneumatic
  - Vent control valve to prevent rapid uncontrolled motion if an actuator was mechanically blocked and then released
    - Possible rapid motion since all back pressure from the exhaust flow speed control escaped as the result of the jam
    - High percentage of injury during clearing of machine jams
    - Consider addition of flow IN to cylinder to limit high speed response due to upstream “air spring” if not vented.
- Hydraulic
  - Accumulators’ output line must be blocked or vented
  - Can hold load by blocking flow out of the cylinder

Lock Out Tag Out vs... SRP/CS

- All sources of unexpected energization, start up, or release of hazardous energy must be locked out or tagged out before exposure to the hazard (OSHA 1910.147)

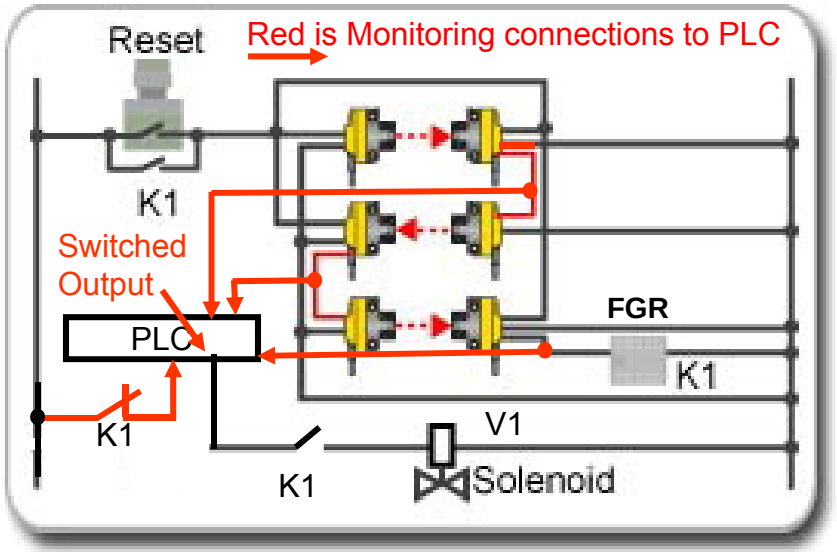
  UNLESS

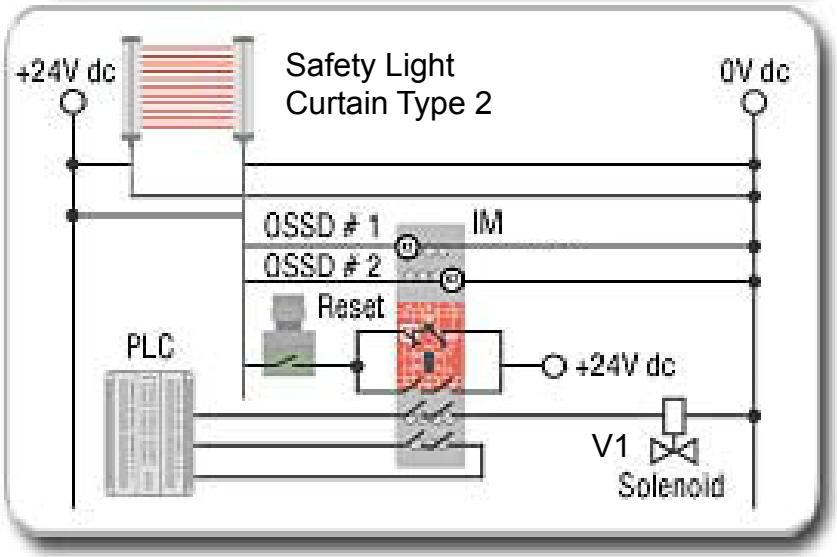
- The task meets all three of the following conditions in the performance of its intended function
  - Routine and
  - Repetitive and
  - Integral to Production
  - OR
  - Task can only be accomplished with power on the machine
    - Teaching Robot
    - Trouble shooting controls
- Only then may risk reduction measures instead of LOTO be applied to reduce the risk to an acceptable level (OSHA Sub part O)
  - These are tasks which constitute minor tool changes and adjustment,
  - Not including maintenance repair, job setting, or clearing of jams

Categories per EN 954-1 and ISO 13849-1-1999

- Determined by the risk assessment
  - If risk reduction is to be accomplished through the application of a safety related part of the control system
- Describes the performance of Safety Circuits
  - Deterministic
    - Functionality requirements are given in descriptive text
    - Different capability circuits meet same category requirements
    - Difficult to “prove” that the required performance has been attained
  - Not intended to be hierarchical
    - Cat 3 safety circuit is not necessarily “safer” than a Cat 2
      - Depends on application and components used
      - Function may be compromised by control system construction and environmental conditions

Example of the “spectrum” within a given category





Three PE with Standard PLC
vs.
Type 2 Safety Light Curtain and IM

These two circuits are both identified under EN954-1 as being the “same” category that is a Category 2

But, do they provide the same level of risk reduction performance?

There may be “logical” arguments for preference of one design over the other, but there is no rigor in the evaluation

Many of the following examples are taken from B11-TR6:2010 Being revised to B11.26-2014

- TR-6 is an ANSI B11 Technical Report which describes the application of components and safeguarding devices to common machine safety control applications
- It uses the ISO13849-1:1999 (EN954-1: 1996) Categories to describe the structure and the capability of a risk reduction circuit.
- Going through major revision
  - Update of drawings and text for consistency
  - Adding an informative clause, an overview of ISO 13849-1-2006

Consider the five identified Categories from EN-954-1-1996 B,1,2,3,4

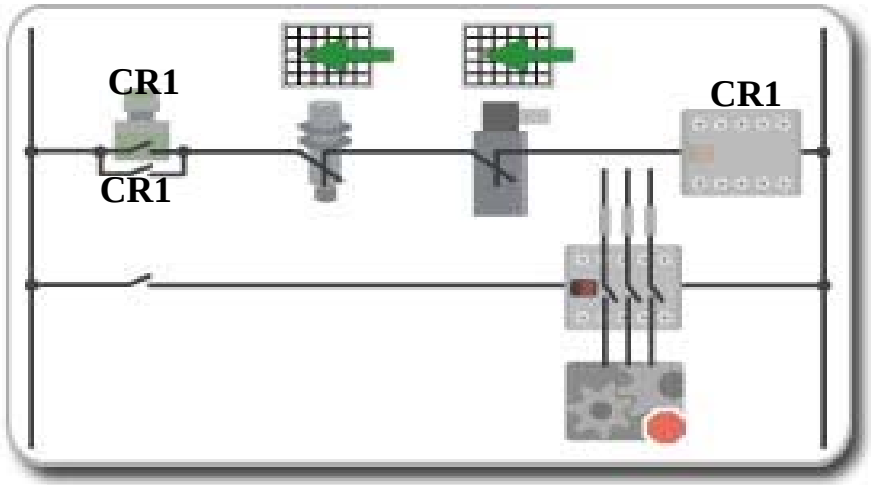
- Circuit topography (structure)
- Functional description of safety performance under component failure
- Each is listed as the minimum requirement to reduce a risk for a severity, exposure and avoidance from a hazard as identified by the Risk Assessment
- RIA 15.06-1999 has mapped its risk assessment risk level results to these categories under different names

Consider for all risk reduction circuits

- Safety Function
- Faults to consider
- Failures excluded
- Safety principles

NOTE: The examples use an Estop as an input device. The principles to meet performance requirements of the Categories shown apply to other input devices, dry contact or OSSD, such as door interlocks, safety light curtains and mats, bypass and muting inputs, mode or feature selector switch, etc.

What does the “category’s” structure look like?

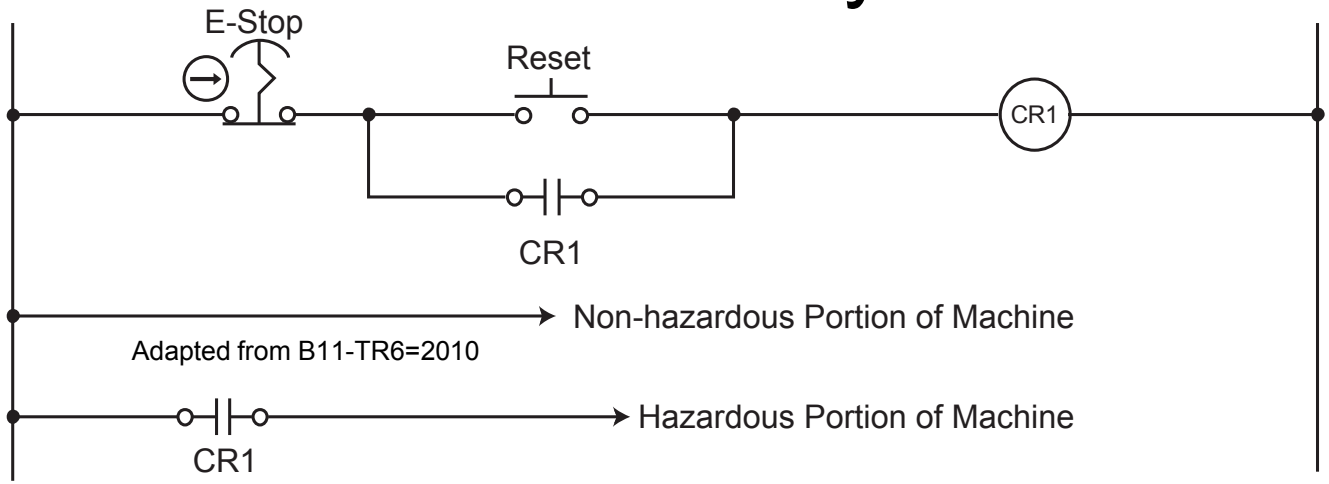


Cat B or 1

Safety Block Diagram

- Cat B = RIA equivalent Simple
- Cat 1 = RIA equivalent Single Channel

Cat B or 1 Functionality



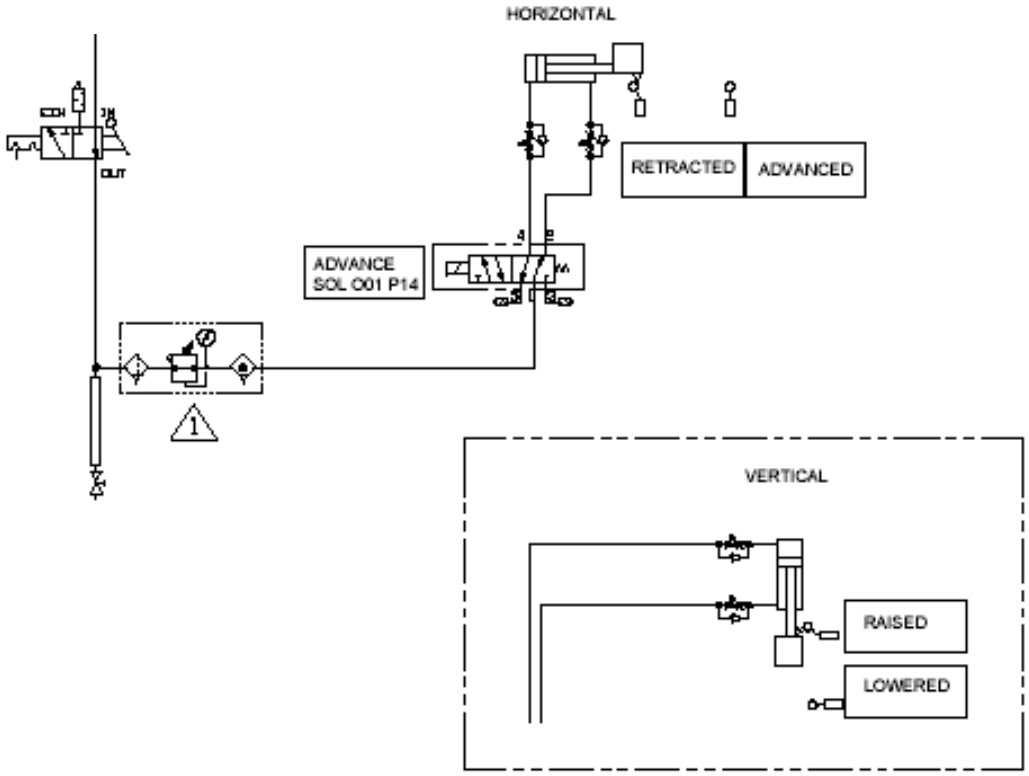
- Functionality
  - When a component fails it will lead to the loss of the safety function
  - Only protection against system failure is the use of components which have a sufficiently low failure rate λd, that is a long mean time between failures MTTFd
  - If used in a low risk application, this failure rate alone may be acceptable
  - **Safety Principles** which reduce the probability of specific modes of failure to danger of the SRP/CS
  - A Cat 1 also uses "well tried' components
    - **Components** to utilize lower failure rate and/or "safety rated" devices which are less likely than "standard" or untried (no history of satisfactory performance in that application devices to fail to danger over the same period of use.

NOT allowed for a Cat 1

Single electronic devices
Standard Electronic Logic
Standard Software

~~Standard PLC~~

Single Channel Pneumatic



Air supply must be adequately filtered and dried, in-line traps drained and cleaned.
If pre-lubed valves are used, consider oil removal desiccant filter
If product require lubrication, use point to point or position in-line lubricator above valve and assure sufficient volume between lubricator and load. Loss of lubrication or water in line cause "varnish" which causes spool valves to freeze

- Solenoid valve driven by logic level. Loss of power at the valve solenoid causes the spring return valve to retract the cylinder. System maintains pressure on rod side of cylinder. Return stroke is not considered hazardous

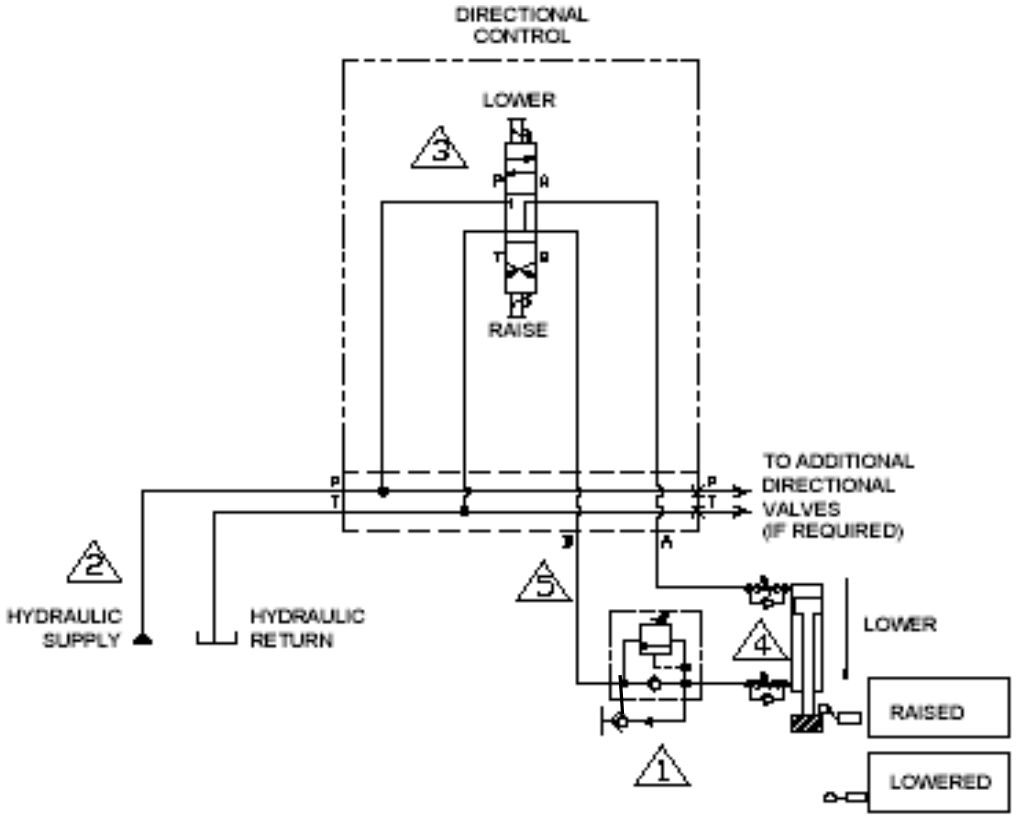
- There is "default" monitoring of the valve during the process cycle

- Use of compressed air filtering both primary and coalescing, will decrease probability of valve failure

- Valves should be chosen based on least likely failure for the application
  - •Steel Spool vs... Flexible Seal
  - •Spool vs.. Poppet
  - •Strong spool spring

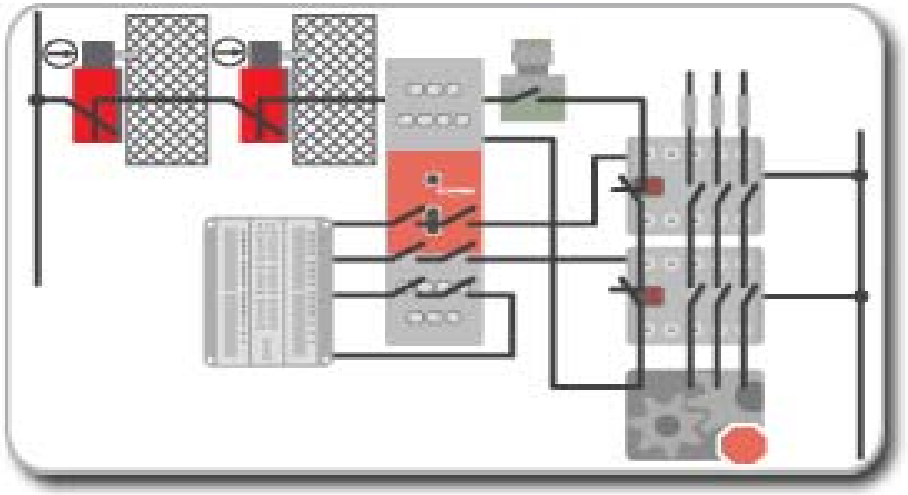
- If there is a strong likelihood that the tooling or work driven by the cylinder can jam, consider bleed IN speed control to reduce the speed of the cylinder after the jam has been cleared if air pressure has not first been manually relieved by the manual dump valve

Single Channel Hydraulic

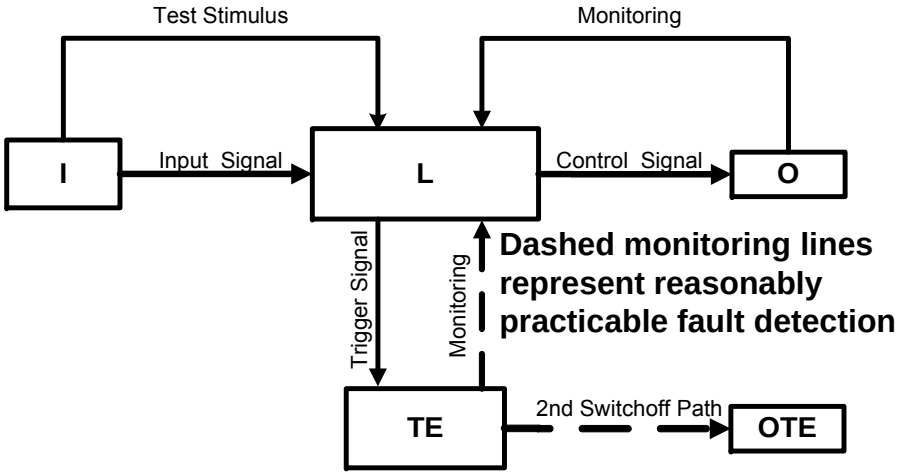


- Attention to fluid filtering and cooling will reduce probability of failure
- For vertical loads, close coupled pilot check or counter balance valves may be required to support the load when valve is in spring centered position.
- Line length should be kept a short as possible. Volume of lines between cylinder and valve must be less than volume of cylinder stroke.
  - This assures an exchange of fluid with flow to and from filter and tank rather than just the circulation of trapped fluid in the lines and cylinder between the valve and the cylinder.
- Operation of valve may be monitored at logic level with pressure switch. Note the load is held by the counter balance valve when directional valve is centered.
- The process operation of the cycling of the cylinder does not guarantee that the valve will spring center for a mid position stop

What does the “category’s” structure look like?



Safety Block Diagram



Cat 2

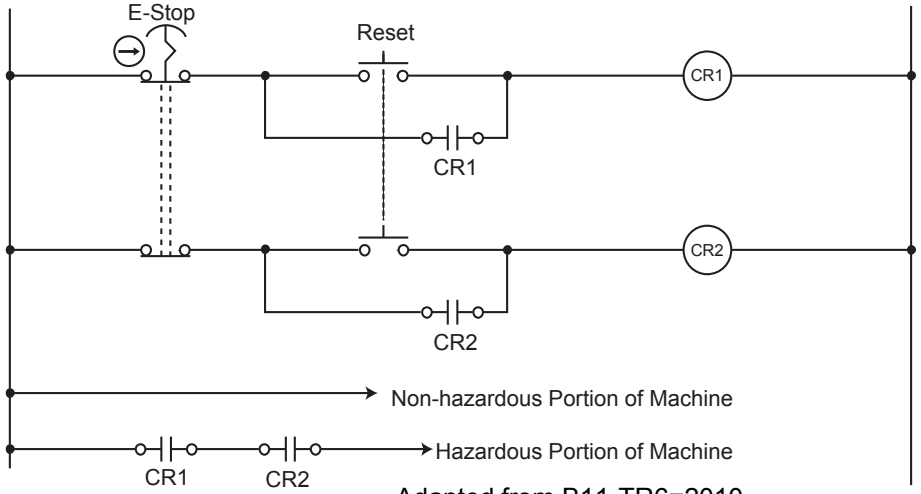
Cat 2 = Single Channel with monitoring

Monitor **at “suitable”** interval **≃ 100x Channel use rate**

Not all designs are able to shut down the hazard, but may only warn and/or inhibit next hazardous cycle/situation

- RIA equivalent Single Channel with monitoring

Cat 2 Functionality

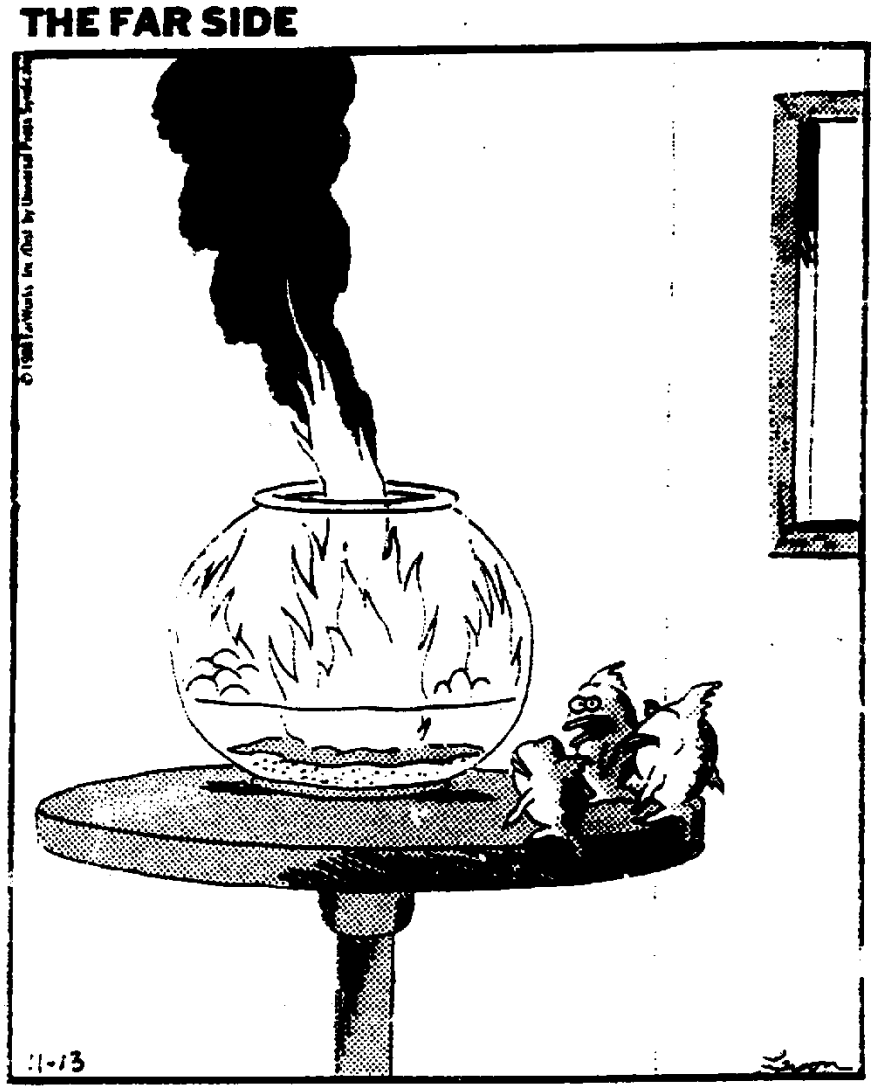


Adapted from B11-TR6=2010

- Functionality
  - The occurrence of a component fault will lead to the loss of the safety function
  - Safety function is tested at suitable intervals
  - When a failure is detected by the circuit it shall:
    - Provide warning or
    - Eliminate off the hazard

Potential circuit to detect system failures in single channel with monitoring
To accomplish this, additional components are added to the single channel of a Cat 2 circuit
BUT
that leads to another issue

Engineering Compromise Or Does my "risk reduction Measure" have a FLAW? A NEW hazard or failure brought on by the "solution"



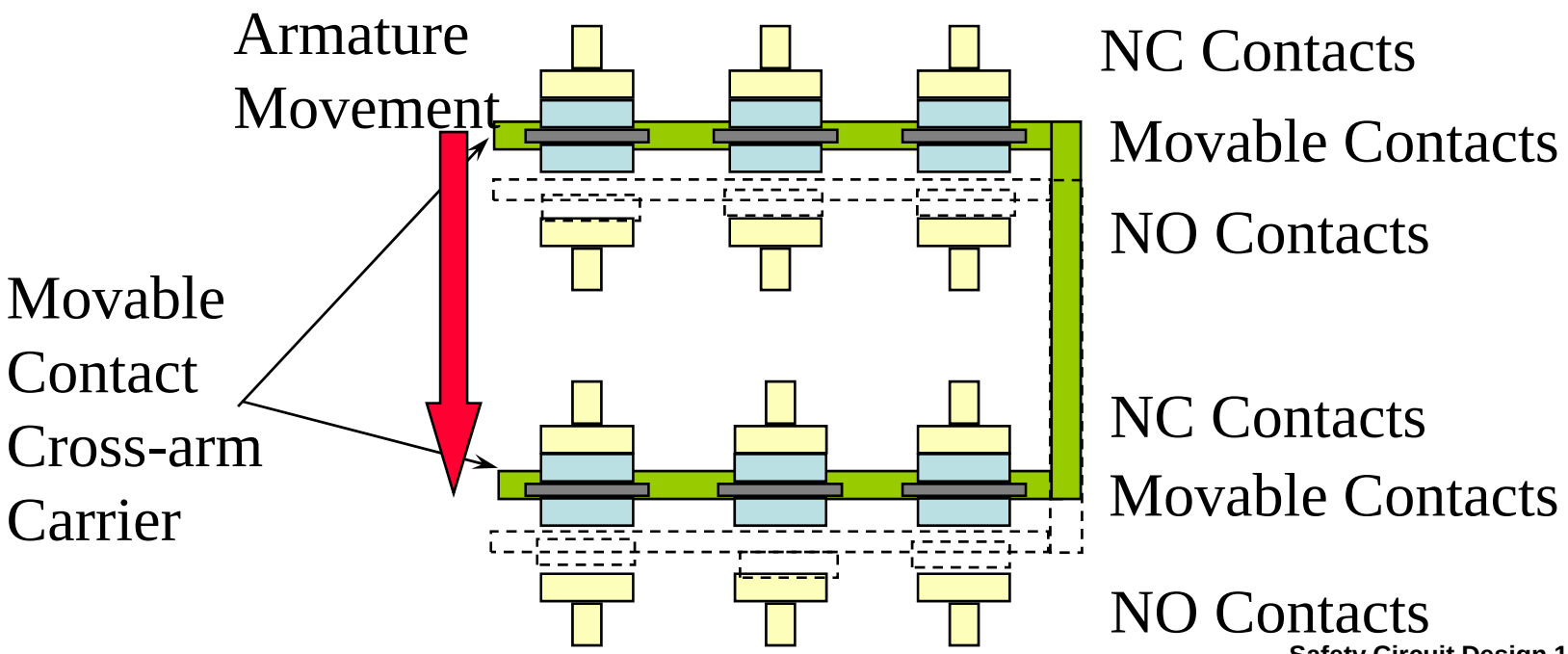
"Well, thank God we all made it out in time. . . . 'Course, now we're equally screwed."

When we need to proof the relay's contacts' state:

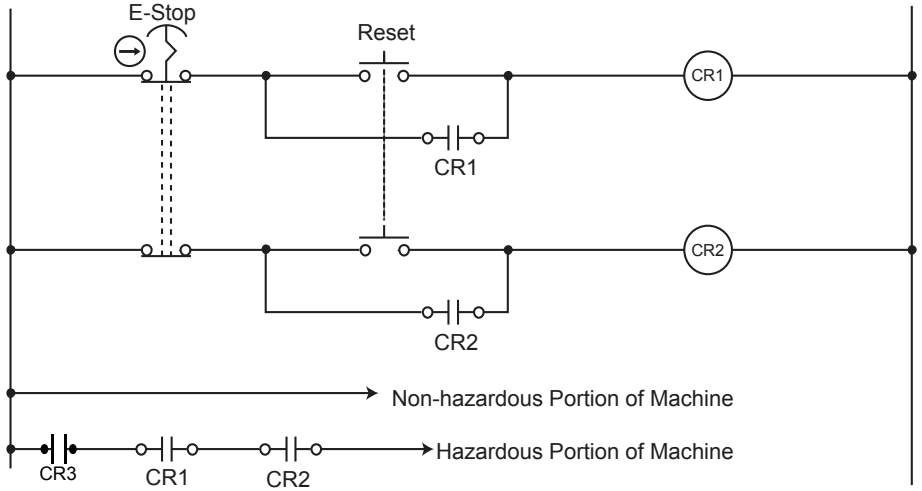
"Force Guided" contacts on relay

When a contact fails to release, none of the **opposite** state contacts will close.

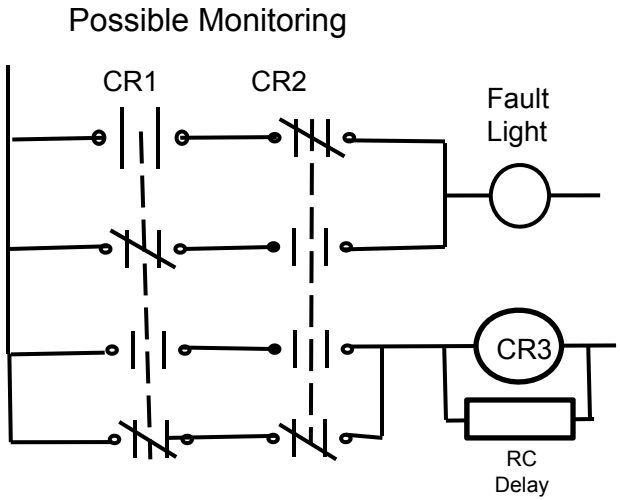
N.O. and N.C. contacts can NEVER be closed at the same time
Therefore when a given contact is CLOSED we are assured that its opposite function contacts are ALL OPEN



Cat 2 Functionality

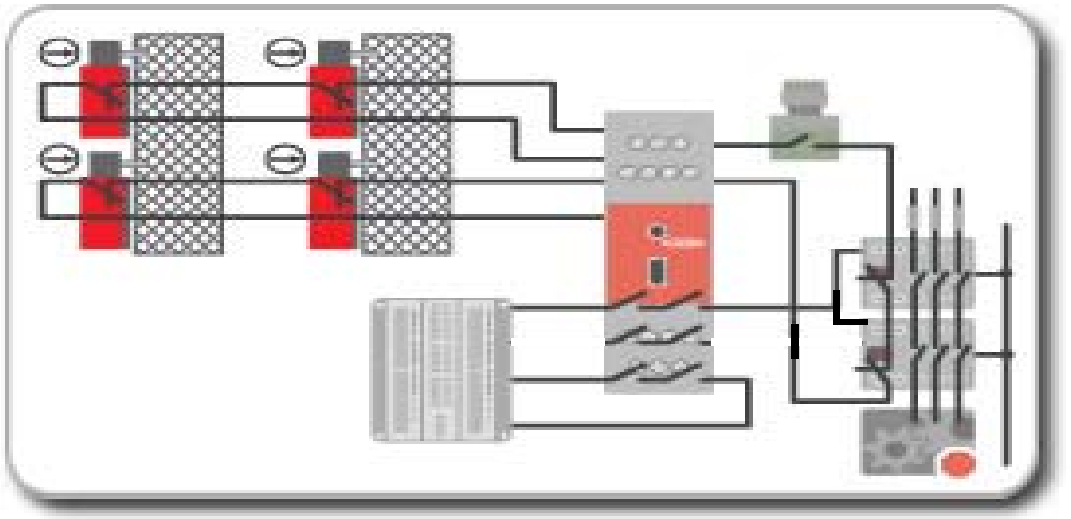


Adapted from B11-TR6=2010

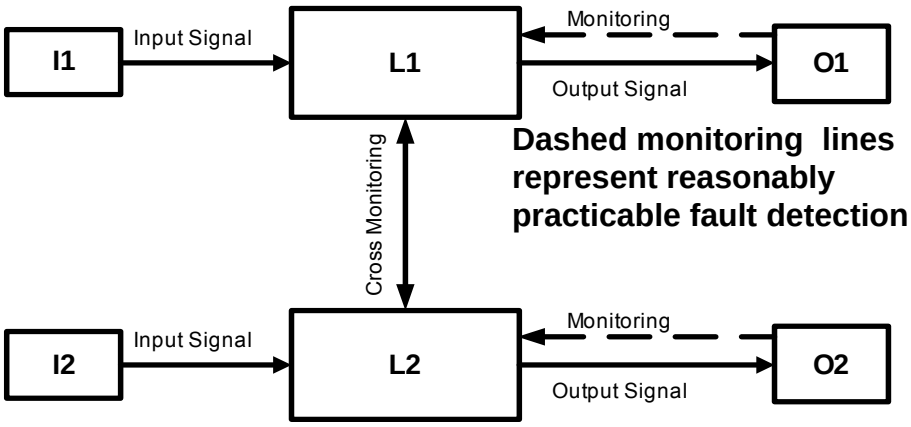


- Functionality
  - The occurrence of a component fault will lead to the loss of the safety function
  - Safety function is tested at suitable intervals
  - The when a failure is detected by the circuit it shall
    - Provide warning or shut down off the hazard
  - Loss of the monitoring function causes the circuit to behave like a Cat B or 1 after the loss of one CR depending on components' performance

What does the “category’s” structure look like?



Safety Block Diagram



Dashed monitoring lines represent reasonably practicable fault detection

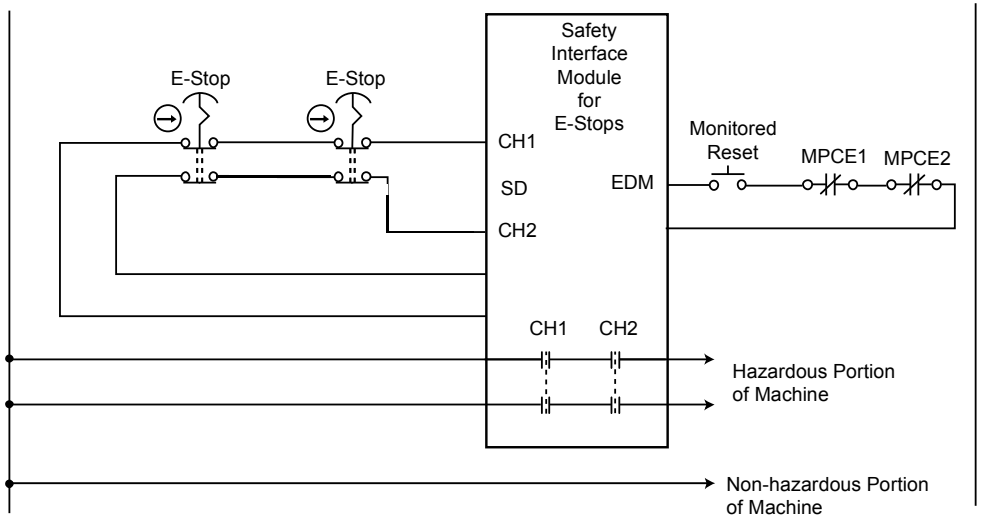
Cat 3

Cat 3 = Dual Channel HFT=1 (1oo2)

w/ Conditional Monitoring
(May not detect all failures)

- RIA equivalent Dual Channel with monitoring
- Control Reliable

Cat 3 Functionality



Adapted from B11-TR6=2010

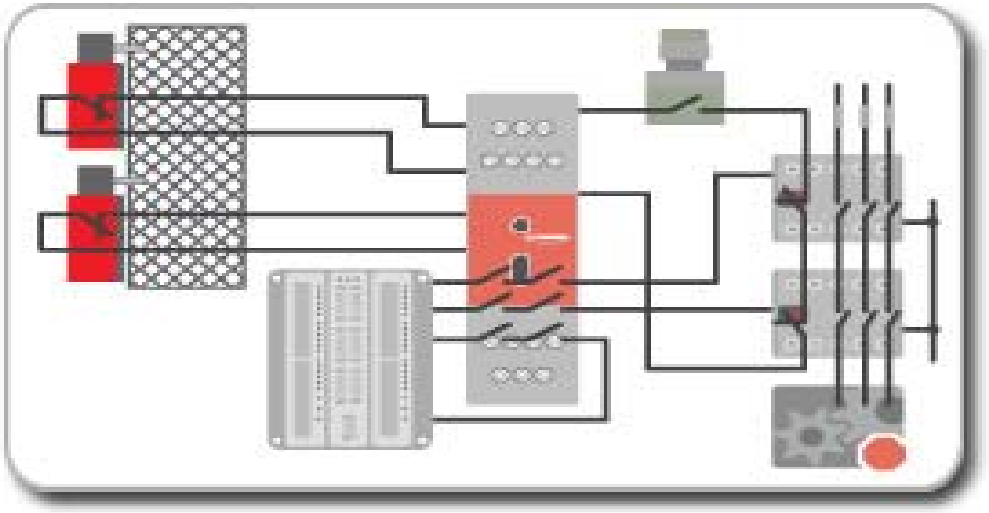
- A single fault does not lead to the loss of the safety function
- Whenever reasonably practicable, the single fault shall be detected at or before the next demand on the safety function
- Some but not all of the failures are detected
- An accumulation of undetected faults may lead to the loss of the safety function

Control Reliable

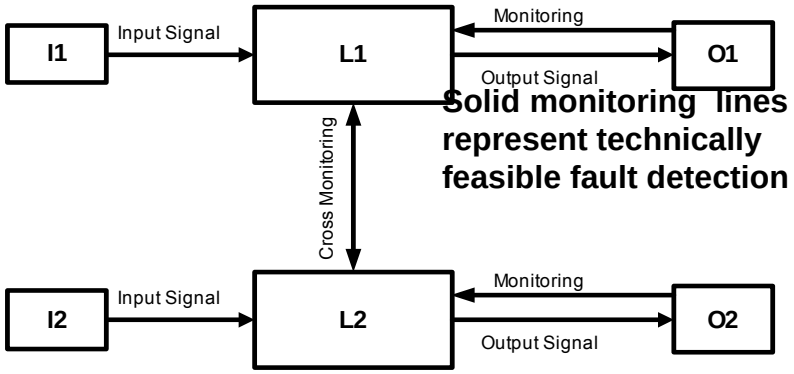
The U.S.A. ANSI standards use the term “Control Reliable”

The performance of such a safety related control system is defined by B11.0 and B11.19 as basically that of the Category 3 controls system as was described here.

What does the “category’s” structure look like?



Safety Block Diagram



Solid monitoring lines represent technically feasible fault detection

Cat 4

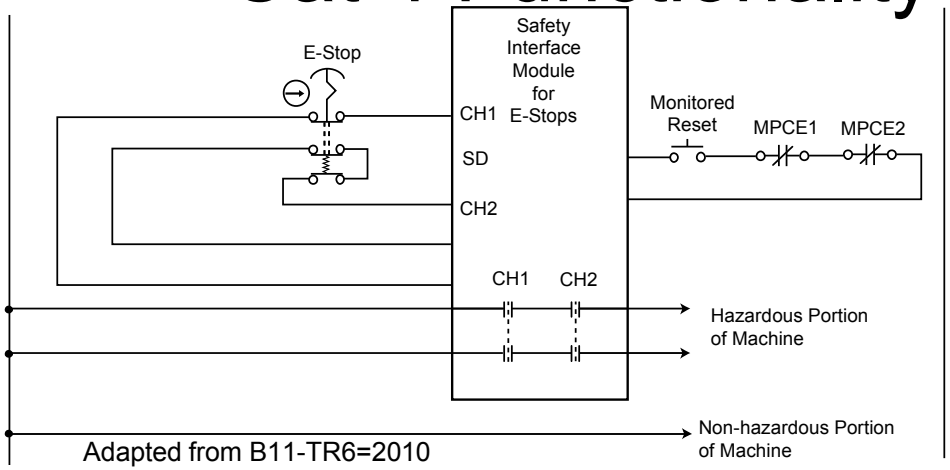
Cat 4 = Dual Channel HFT=1 (1oo2)

w/ Complete Monitoring

Must detect first fault or continue to protect with this and the next fault, this combination must be detected

Not included in RIA, assumed to exceed typical Robotic application requirements

Cat 4 Functionality



- Single fault does not lead to the loss of the safety function
- Where possible, all failures will be detected
- The undetected fault will not lead to the loss of the safety function with the occurrence of the next fault.
- The safety system will continue to function without loss of the safety function until the combination of accumulated faults is detected, and the hazard eliminated
  - Typically at the detection of the second fault

RIA has no equivalent in RIA 15.06-1999 as Robotic System hazards are considered to be a risk level which requires a risk reduction capability which generally does not rise to the requirement of Cat 4. The Risk Assessment may discover extreme risk which can require Cat 4

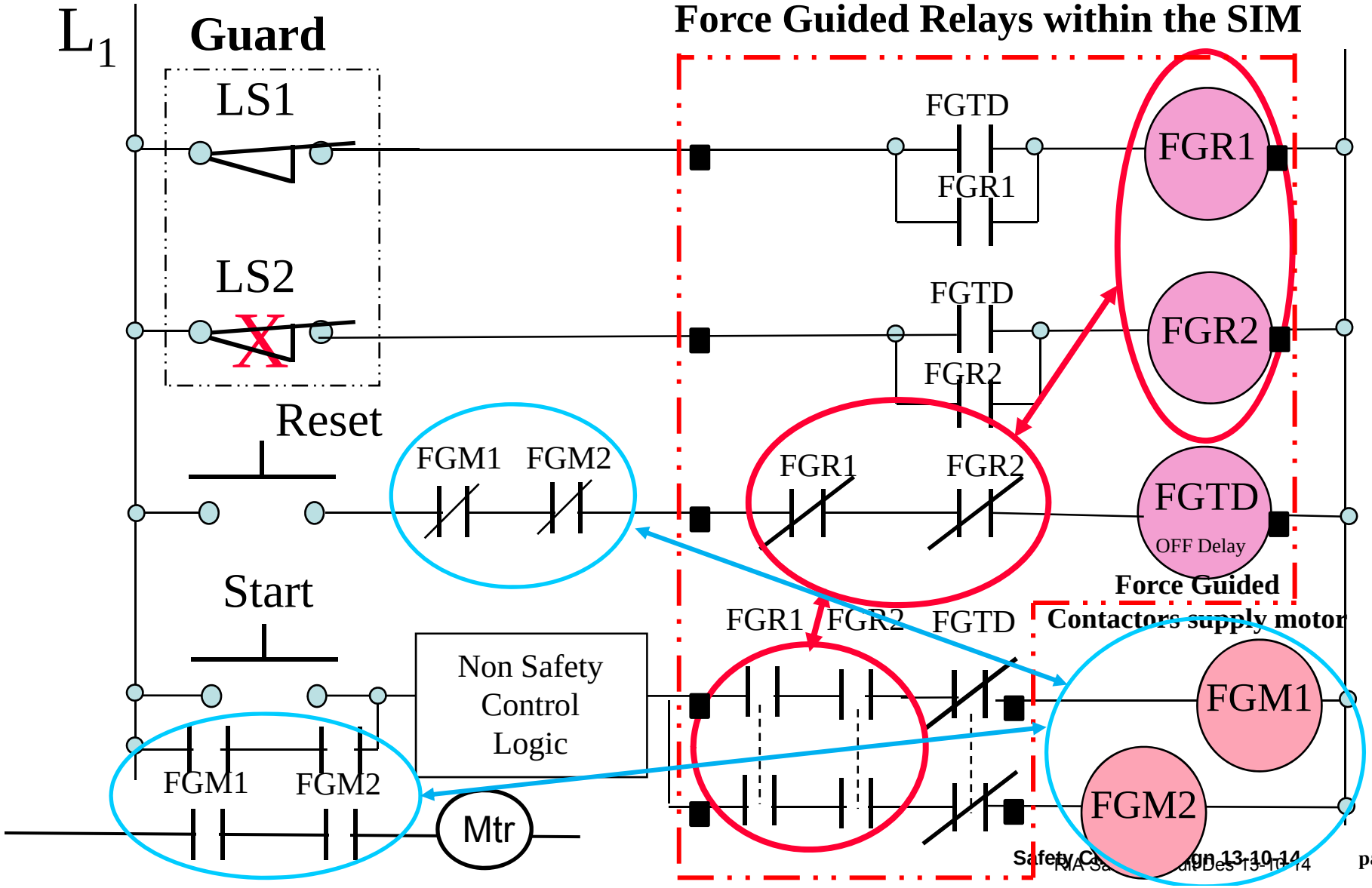
NOTE on Categories

- Category B and 1 presume that the devices' reliability in avoiding failure to danger is adequate to meet the risk reduction requirement
- Category 2 may detect a failure but could loose the monitoring function due to a failure in its own structure, and a detected fault may only provide a warning, not an elimination of the hazard
- Category 3 & 4 provide two means of eliminating the hazard and detect a system fault to various degrees.
- The monitoring and detection of faults before the circuit fails to danger raises the performance of the circuit beyond that of the individual components

Impact of a circuit's performance by external factors

- Before going into the diagnostic, performance with fault(s) capabilities of specific circuits, we must review certain features which impact the performance of a circuit's ability to reliably detect failures which may lead to the loss of the safety function
  - Detection of Failures
  - Common Cause Failures
  - Hidden or Disabled fault detection
  - Multiple Fault
  - Exclusion of Failures

Safety Interface Module::



Dual Channel Bypass

Device Terminology

- Force Guided Relay
  - Electromechanical relay so constructed as to assure that a NO and a NC contact can never be closed as the same time, as required for monitoring
- Safety Relay / Contactor
  - Electromechanical relay with Force Guided contacts all of which are permanently affixed to the relay.
  - Contactors having permanently affixed auxiliary contacts
  - Manual operator removed to prevent circuit over-ride

  Both of the above devices MUST interface with an

- "***Intelligent***" device capable of detecting a system fault in order to perform any SAFETY function
- **S**afety **I**nterface **M**odule, (SIM) often just Safety Module
  - **Intelligent** module using multiple electric and electronic components to monitor input, output, and internal status, detect faults, and enable outputs only under predetermined conditions
  - Some times still called, incorrectly, Safety Relay (See above)
  - Generally using Force Guided Relays in their design and as their outputs
  - Starting to market series, pulse tested, dual or quadruple transistor outputs

Common Cause Failures CCF

- In the design of Cat 2, 3, and 4 care must be exercised so that a single failure does not affect the components such that the monitoring becomes ineffective.
  - These types of failures are known collectively as “Common Cause Failures”
    - The failure of two devices from one cause and not causes of each other.
      - These are typically simultaneous
    - NOTE this is not common Mode failure which is the “same” failure of multiple devices but NOT due to common cause.
    - Consider a common drive connection on a multiple cam limit switch used to monitor a punch press crank.
      - Loss of cam switch drive chain would provide inaccurate drive information,
      - Direct monitoring of the two limit switches will not detect the erroneous position data received
      - The chain is a common cause failure of both limit switches
    - Environmental impacts are also common cause
      - Power surges, Voltage Spikes, EMI, RFI

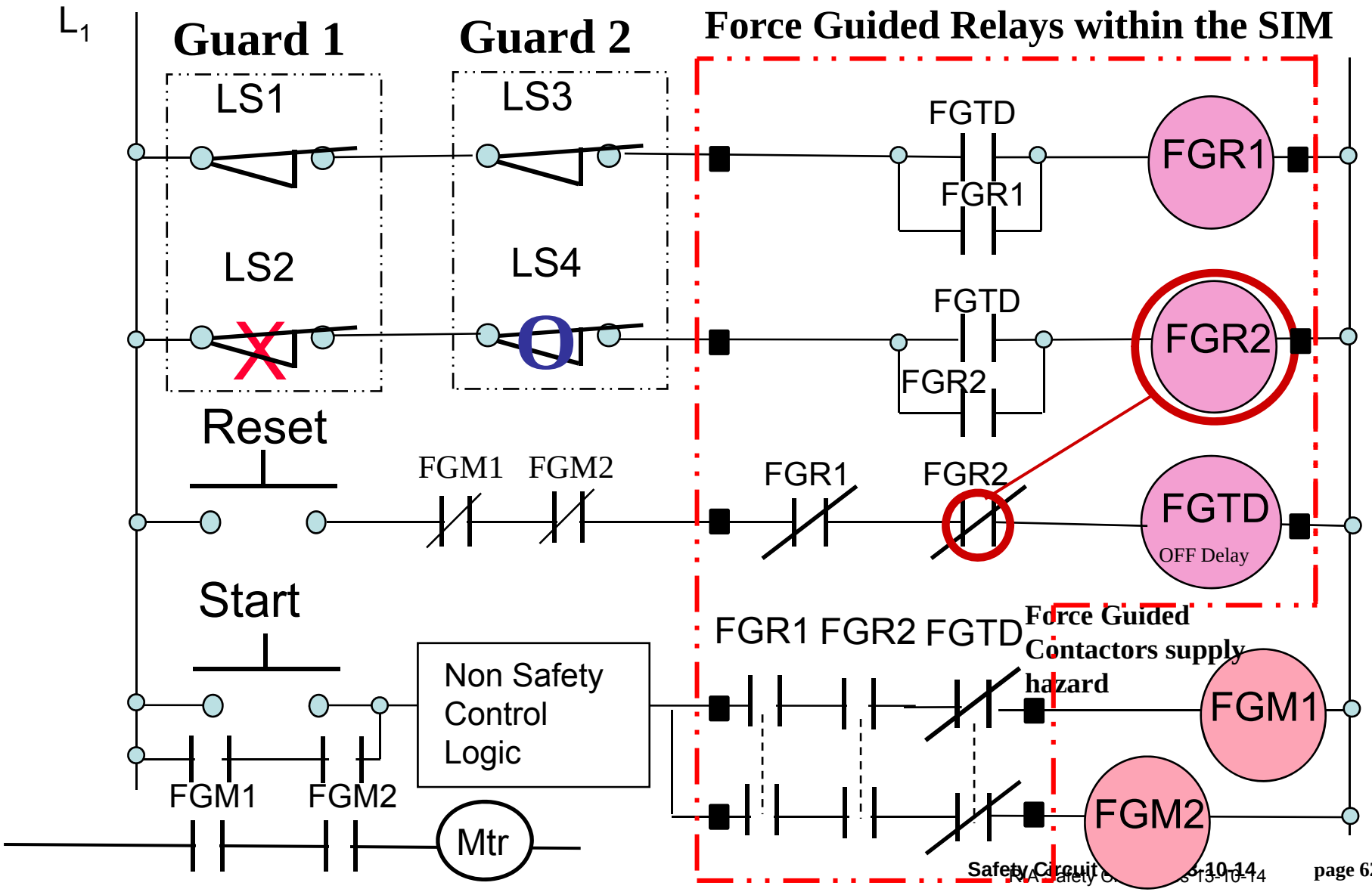
Some ways to reduce Common Cause Failure

- The common cause impacts each device differently
  - Diverse Redundancy
    - N.O. N.C. operations on two limit switches
  - Different technology
    - One Inductive proximity and one photo-electric opposed sensor
- Remove the Common Cause Mechanism
  - Physical separation of conductors
  - Avoid common mounting surfaces which could fail
    - Mounting two limit switches on the same sub-plate
  - Avoid common drives and operators
  - Overdesign of common hardware
  - Overdesign of current carrying devices and/or employ conservative overcurrent protection
    - Welded contacts on overcurrent/short circuit

Hiding or Disabling Fault Detection

- Some configurations may cause what otherwise appears to be a perfectly acceptable circuit to fail to accomplish the expected task

Disabling fault detection in the system



Hiding or Disabling Fault Detection

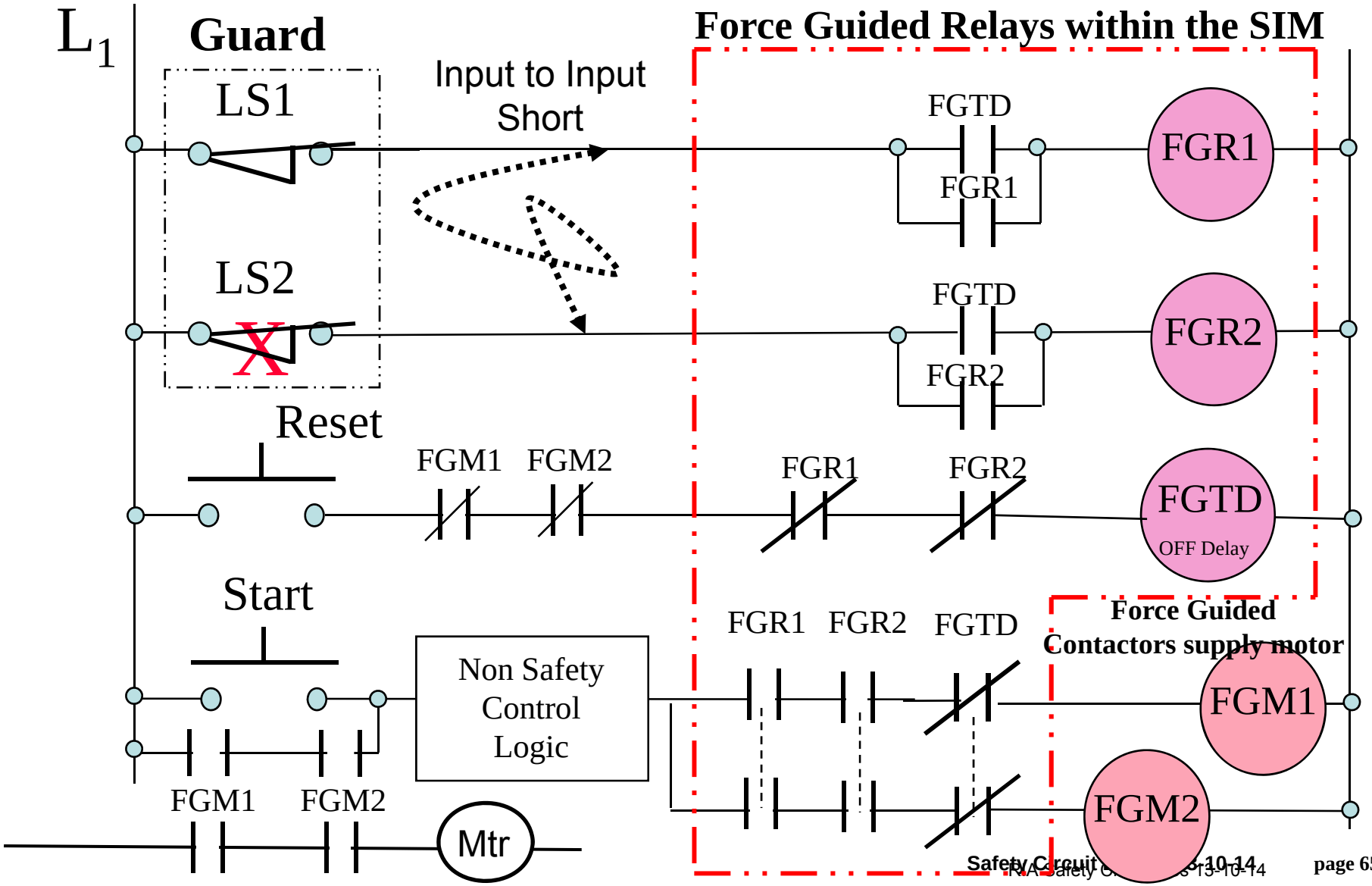
- Series Contacts such as LS2-LS4 should not be used in High Risk Safety Circuits as they provide a “work a round” for a failed component
- Shorted contact in LS2 **X** Operation of LS4 at **O** will mask failure of LS2 by dropping FGCR2 thus allowing a Reset by the reset push button and enabling machine operation with a “known” fault.
- If LS4 were to open first, the fault of LS2 would not be detected with this series connection to the SIM
- Series connections are allowed in Emergency Stop applications
  - It is highly unlikely that multiple Estops are operated at the same time
  - Operational procedures may reduce this even further

Multiple Faults

- Circuit design assumes that only one fault occurs at a time, giving the detection an operation cycle to detect the fault before assuming a second fault
  - Basis for low CCF requirement
- First fault might not lead to the loss of the safety function:
  - Sets up the failure to the second fault to become a failure to danger
  - Possible in Category 3 structure
  - Not possible in Category 4
    - First fault is Detected

      Or
    - Second fault may not lead to the loss of the safety function
    - The combination of the two faults must be detected and the hazard eliminated

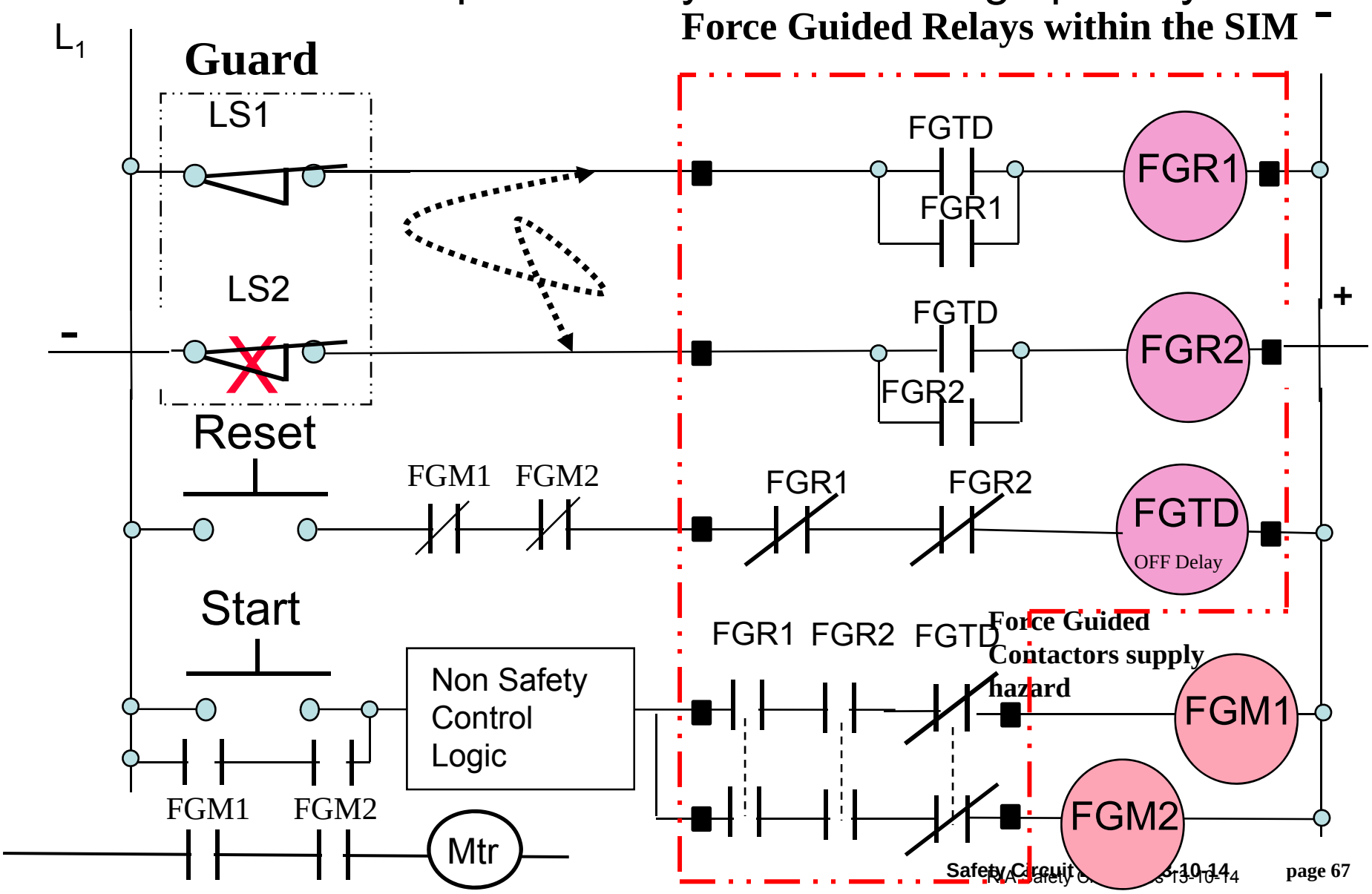
What if first fault is not detected, a second fault may lead to dangerous failure



Wire to wire short

- Input
  - Short between inputs
    - Pulse on dry contact source
    - Diverse Polarity on dry contacts
    - Active safety devices can detect these by pulsing their outputs
  - Short to supply source
    - Pulse on dry contact source
    - Diverse polarity only if short to opposite polarity
    - Active safety devices by pulsing outputs
- Output
  - Short between outputs
    - Pulse outputs
    - Diverse action
  - Short to supply source
    - Pulse outputs
- Either I or O
  - Use of exclusion
    - Separate runs
    - Short run, protected within common cabinet or enclosure

+ Detection of input short by diverse voltage polarity



Detectable Faults

- Some faults are difficult to detect, others may not have an economical detection capable solution
- When must a fault be detected?
  - Depending on the Category of the SRP/CS it may be permissible not to detect some faults
  - Some faults, though possible to detect, are so unlikely to occur that their detection would not provide a discernible reduction of risk
  - An alternative to detection of a fault is to be able to justify its exclusion from consideration
    - The steps taken to justify exclusion should be documented

What about the undetected failures

- Potentially undetected failures
  - Wire to wire shorts on the input or monitoring
  - Multiple devices in series
  - Safety output drive wire shorts to uncontrolled source of power
  - The directional valve, although capable of cycling under the control of the solenoids does not spring center
  - Contact block of Estop not closely coupled to operator mechanism, does not open contacts on operation
  - Valve silting, slowing down system response to a stop command
    - Increases the safety separation distance for presence sensing safeguarding devices
- It must be determined in each case if it is acceptable that these faults (and any others) remain undetected
  - The requirement is that most (where reasonably possible) of these should be detected or excluded through design and construction using sound and “well tried” safety engineering principles

Justify exclusion of a Fault when:

- The fault is so unlikely to occur, that to detect it would add little or nothing to the safety performance of the SRP/CS
- Some faults are typically more likely to occur and if not detected, their probability of occurrence must be lowered by design and/or construction, which for this case, is sufficiently low to justify their exclusion.

  EX:

  – For a Cat 4 design, it must be assured that both MPCE cannot fail due to shorting control wires to an alternate source of power.

  – This is typically done with two separate outputs which are monitored by the logic unit to assure that the wires are not shorted either together nor to another source.

  – If this is not practicable the failure mode may be excluded by:

    - Running the wires in separate conduit or paths isolated from each other and from a second source of power

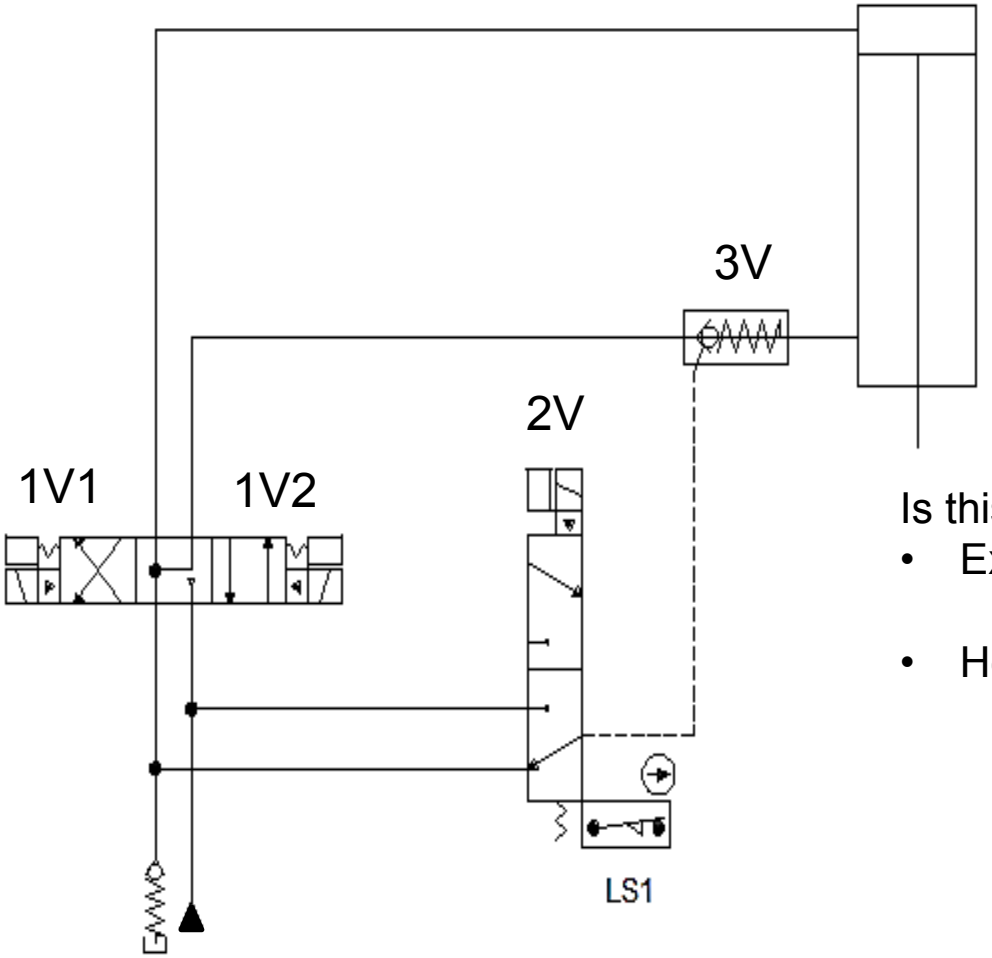
Lessons Learned

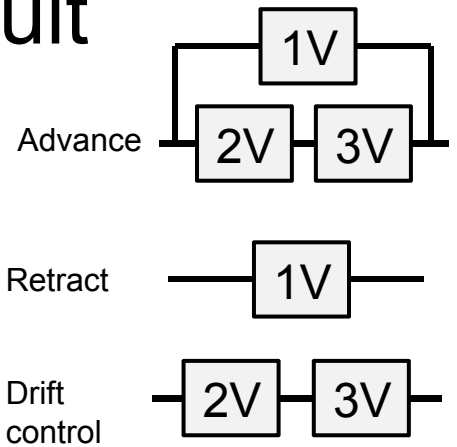
- Even a “good” design with safety components is subject to variations in performance due to circuit configuration or structure
  - Higher level devices often remove these variations as they support the correct architecture
- The level of risk presented by the hazard is, determined by a **R**isk **A**ssessment
- The R.A. helps to determine what level of risk reduction must be achieved, and to define the circuit structure, installation requirements, and to some degree, the components which must be used.

Analysis of SRP/CS whose performance depends on the ability to detect failures and to conserve the safety function in their presence

- Safety block diagrams focus on the failure modes and their impact on the performance of the safety function

Cat 3 Hydraulic Circuit





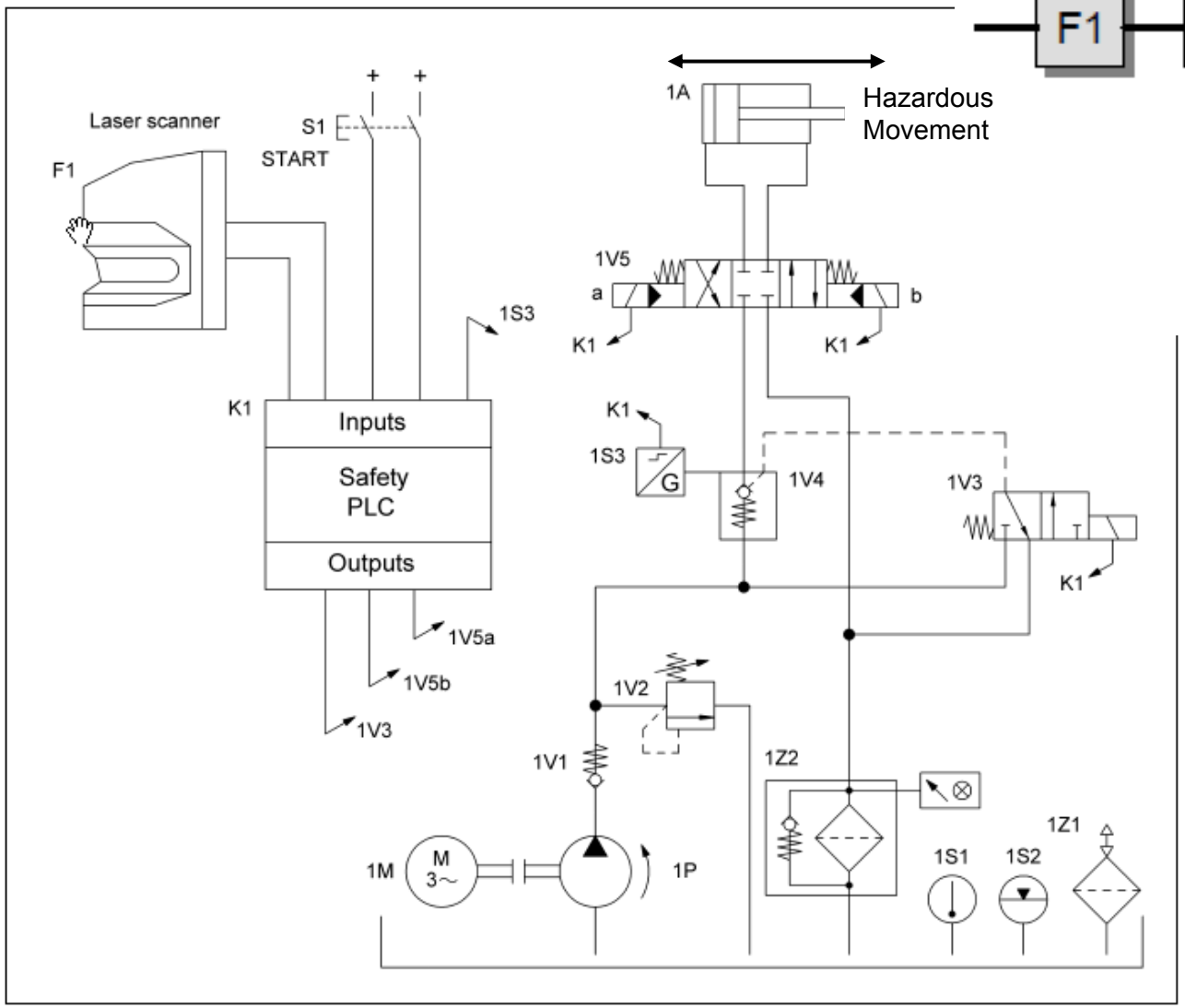
Electrical signals have been left off for simplification

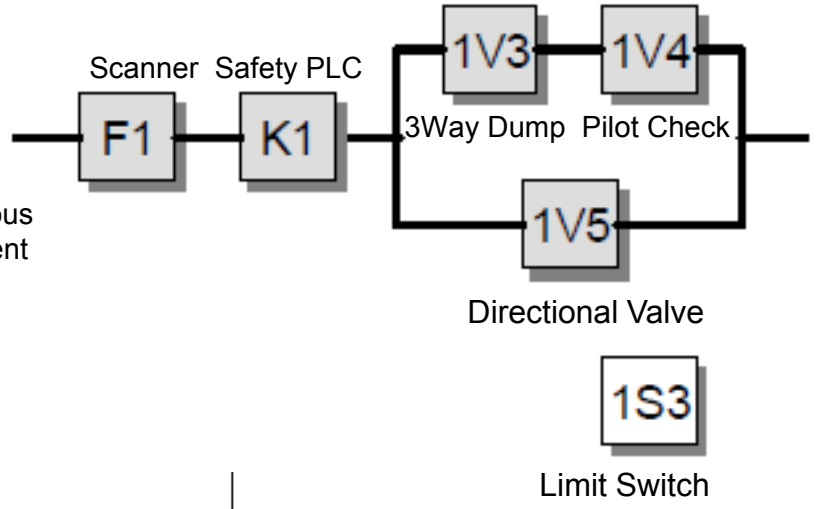
Is this a true Cat 3 circuit?

- Extend is dual channel
  - IF I may exclude failure of the check valve
- How are the valves monitored
  - Blocking valve V2 with LS1
  - Directional 1V valve by monitoring process
    - Excluding failure to spring center
  - Check valve 3V could be dynamically tested by halting cylinder above full extension and monitoring resultant position
- Retract single channel
- Drift control is single channel

BGIA Report 2/2008e

Figure 8.28:
Detection zone monitoring by laser scanner with electro-hydraulic deactivation of the hazardous movement

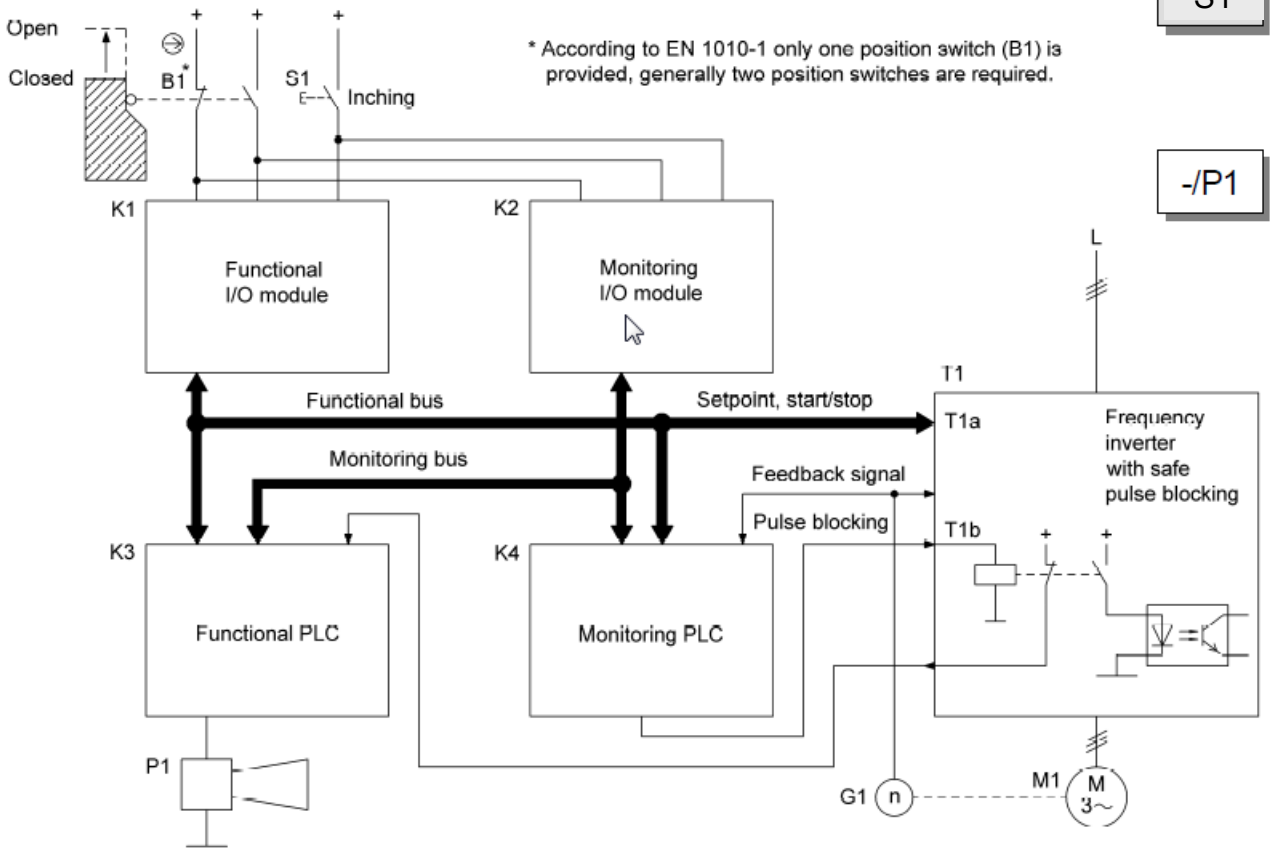


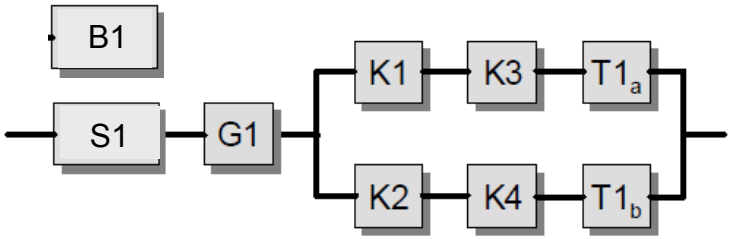


The limit switch, 1S3 although it performs a necessary function of monitoring pilot operated check valve 1V4 and indirectly, the dump valve 1V3, is not part of the safety block diagram since its failure does not lead directly to the loss of the safety function. Good design will monitor its cycling in co-ordination with the machine control circuit.

Remote I/O and Safety PLC

Figure 8.42:
nching mode with safely limited speed on a printing machine with two-channel
nicroprocessor control





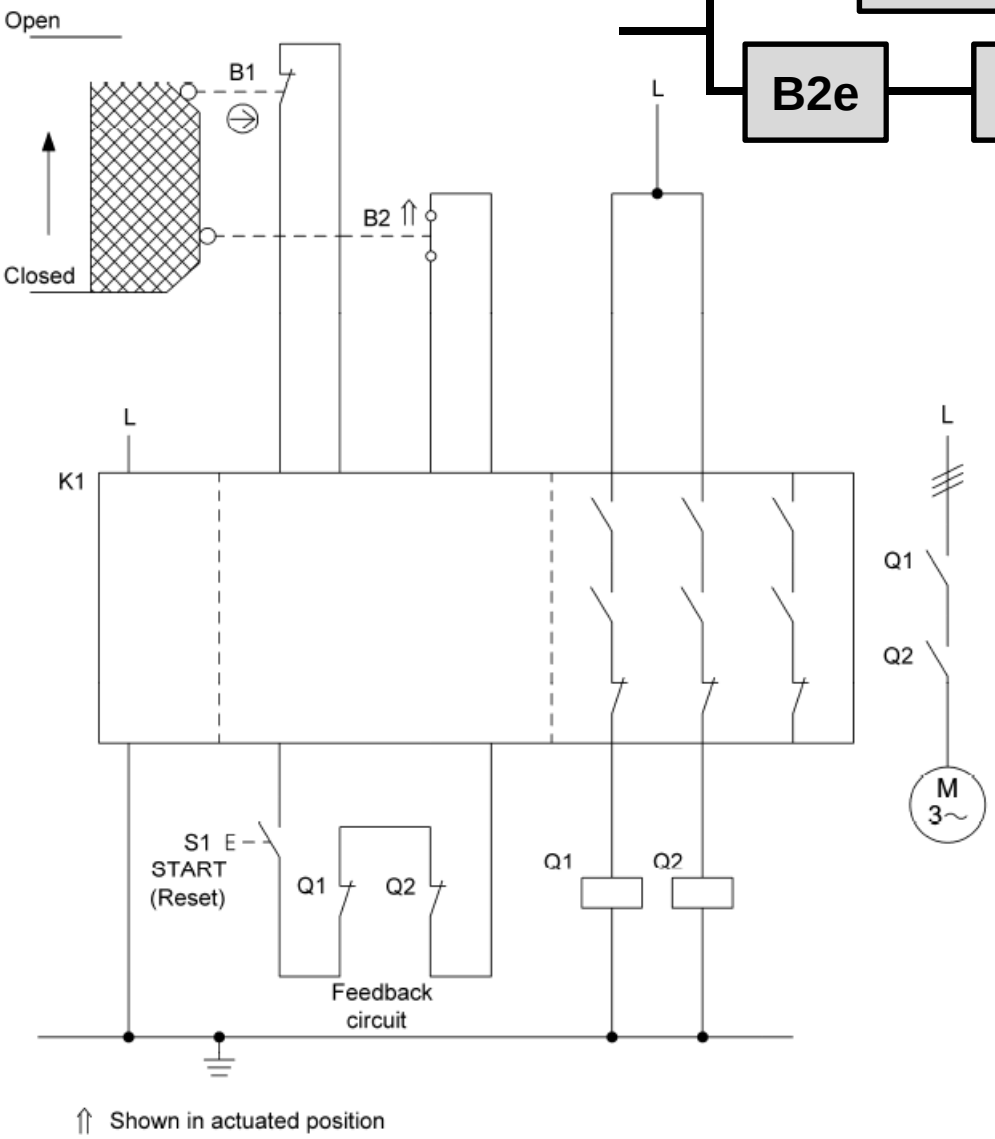
-/P1

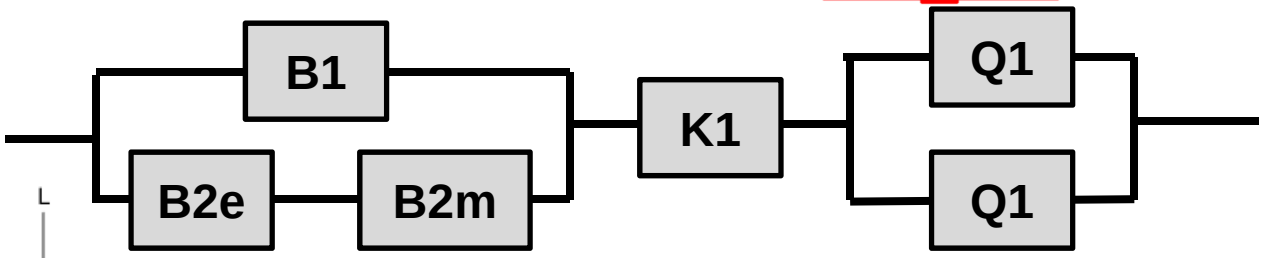
Note each PLC has an independent remote I/O module

S1 and the horn P1 are a Cat 2 warning sub-system

T1a is a SS1
T1B is a SLS

A separate safety function is developed for the Gate interlock by replacing S1 data with B1 and using the same remaining configuration





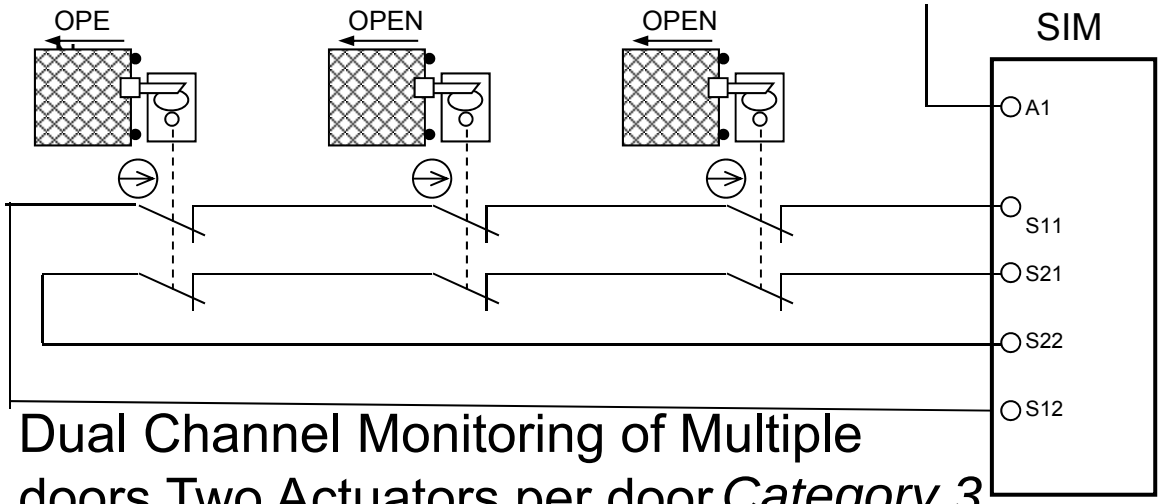
B1 is a direct acting Limit Switch for which the mechanical action of the contact failure may be excluded

B2 is a negative operation standard limit switch which has both a mechanical contact failure mode B2m (spring opening) as well as the electrical contact failure mode which is the same for both B1 and B2e

This not typically shown as two stage but done so here to illustrate the concept and how the values are treated

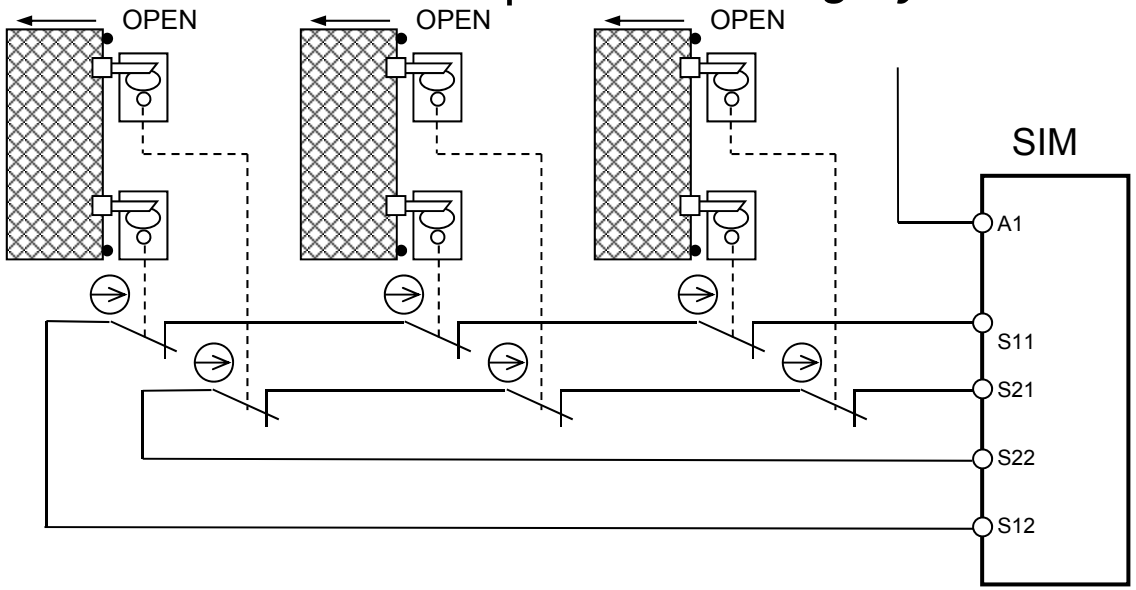
A similar dual function may exist with output devices, particularly relays which may have a mechanical operations and a separate contact operation specification which is a function of the contact load. These may be shown in the safety block diagram or simply used in the calculation

Dual Channel Monitoring of Multiple doors One Actuator per door *Category 2*



- Series connection may hide electrical fault:
- Shorted contacts or wires
- Certain mechanical failures **WILL NOT** be detected:
- Broken Head
- Actuator Off Door
- Note cycling of any other door will hide or reset the detected fault
- Should be tested INDIVIDUALLY at regular intervals by a qualified individual

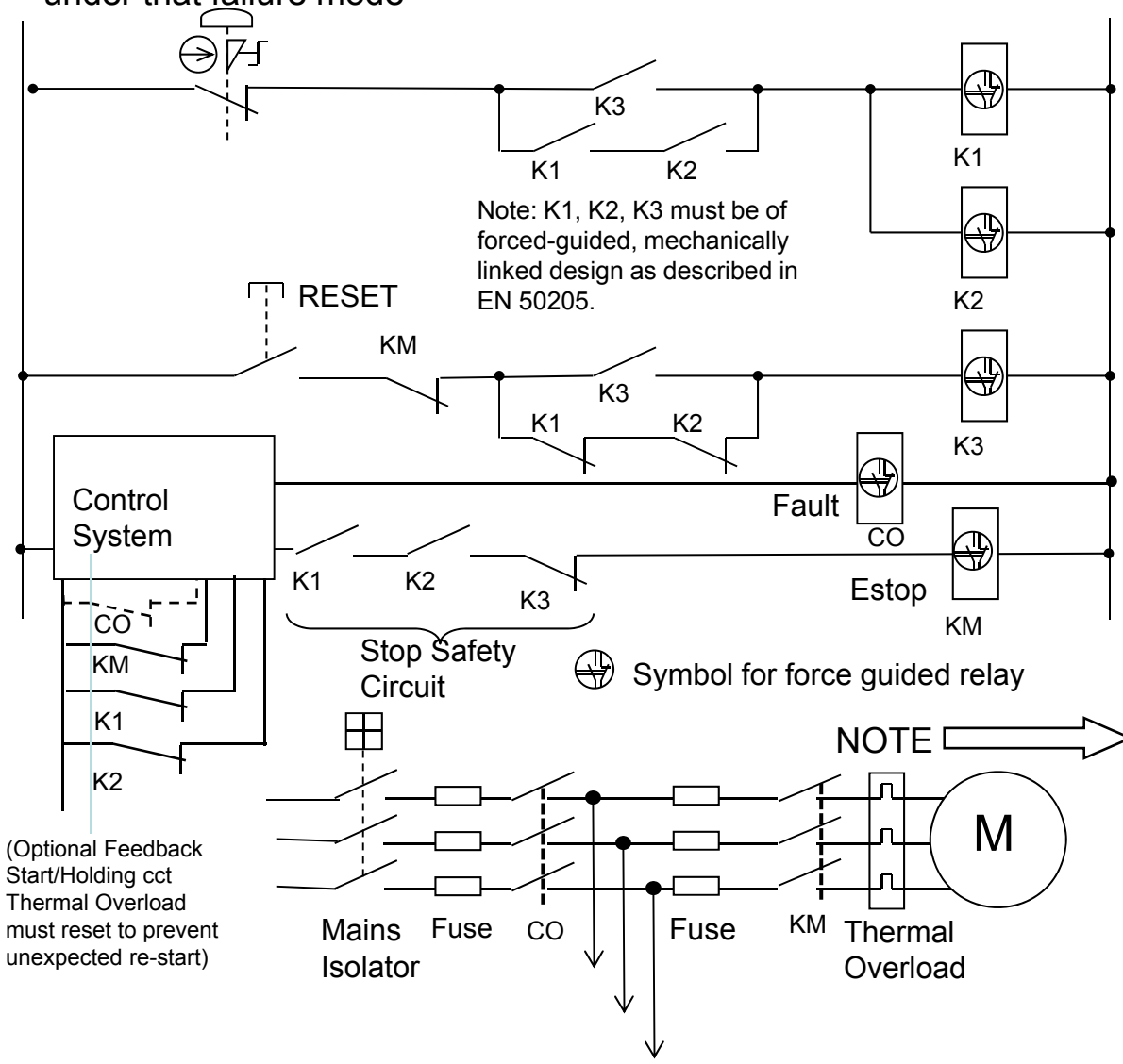
Dual Channel Monitoring of Multiple doors Two Actuators per door *Category 3*



- Series connection may hide faults which are detected
- Electrical shorts or
- Certain mechanical failures **COULD BE** detected through the dual contact sets:
  - Broken Head
  - Actuator Off Door
- Note cycling of any other door will hide or reset the detected fault
- Should be tested INDVIDUALLY at regular intervals by a qualified individual

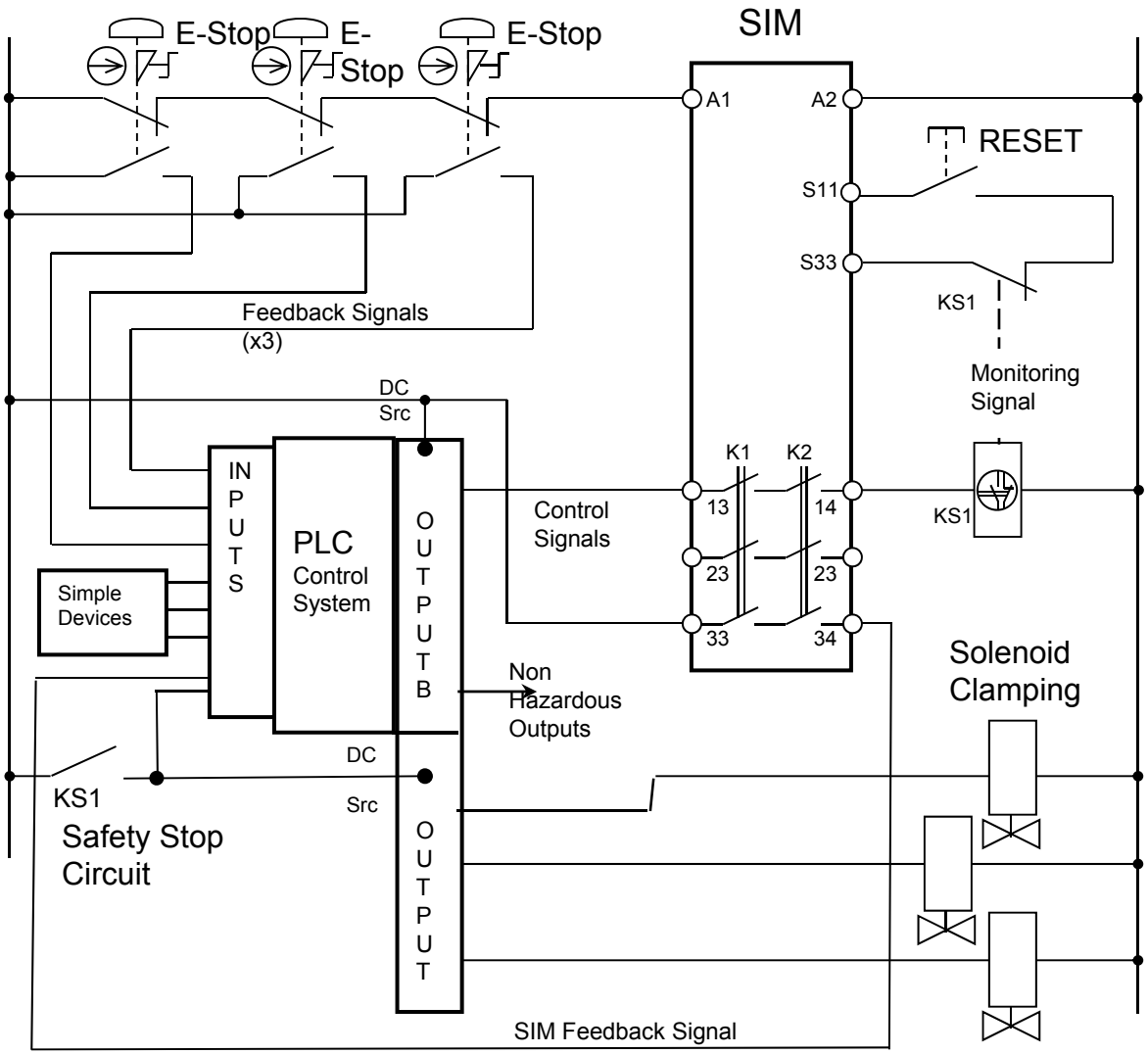
Single Channel with Monitoring

Designed to detect only the failure of K1, or K2 and to prevent reset under that failure mode



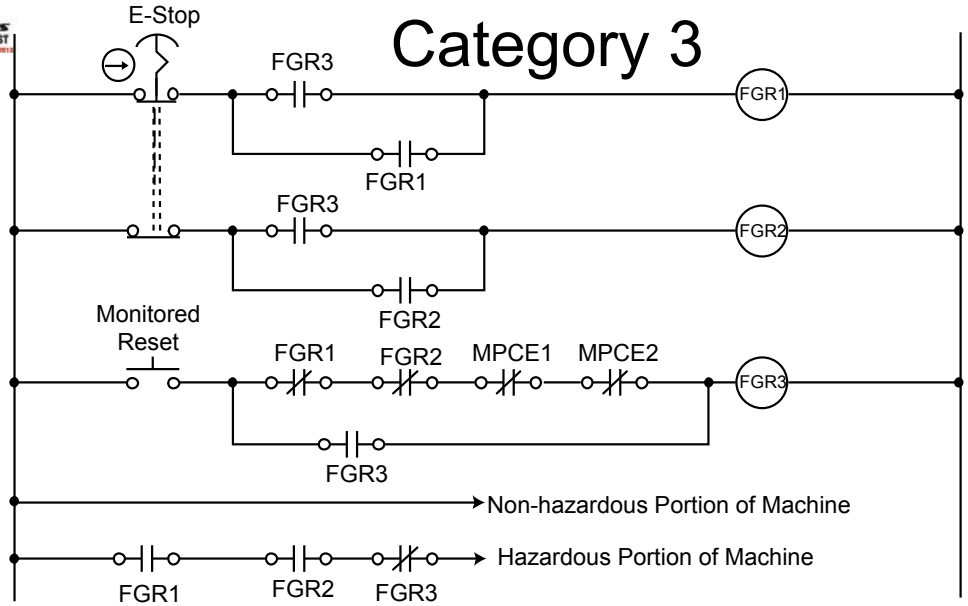
- Only the relays are monitored.
- The PLC and reset can prevent KM from being re-energized if the contact hangs, but cannot over-ride that failure
- KM is monitored at K3 which will not reset if KM fails in the ON state, but there is no control of M, the hazard if this failure mode occurs.
- In some applications, a secondary contactor CO is added which feeds the power drop to the hazardous and other functions. Here it is controlled by the PLC's monitoring function. CO cycles only on a fault and should be tested on a regular basis
- The NC contact of K3 in series with KM provide monitoring of K3
- The NC of K3 also provides reset anti tie down
- For monitoring to be valid, all relays are monitored with N.O./N.C. contacts which must be FORCE GUIDED
  - Some relays many have Deck Force Guided contacts only on the lower deck, not on top or add on deck

Single Channel with Monitoring



- This single channel with feedback circuit features monitoring capability of a safety interface module in the power circuit.
- KS1 is monitored by the safety interface module preventing re-energization of the coil.
- Reset may be anti-tie-down depending on the design of the SIM (Time based or trailing edge)
- Power is supplied to the valves only if KS1 is energized by both the logic PLC and the safety interface module, and the logic is true for that specific valve
- Estop operators are monitored by the PLC through individual Estop contacts and state of the SIM and can provide secondary shut off of the PLC output to KS1 as well as the valves when failure is detected
- Failure of the valves to shift on removal of power may result in the loss of the safety function

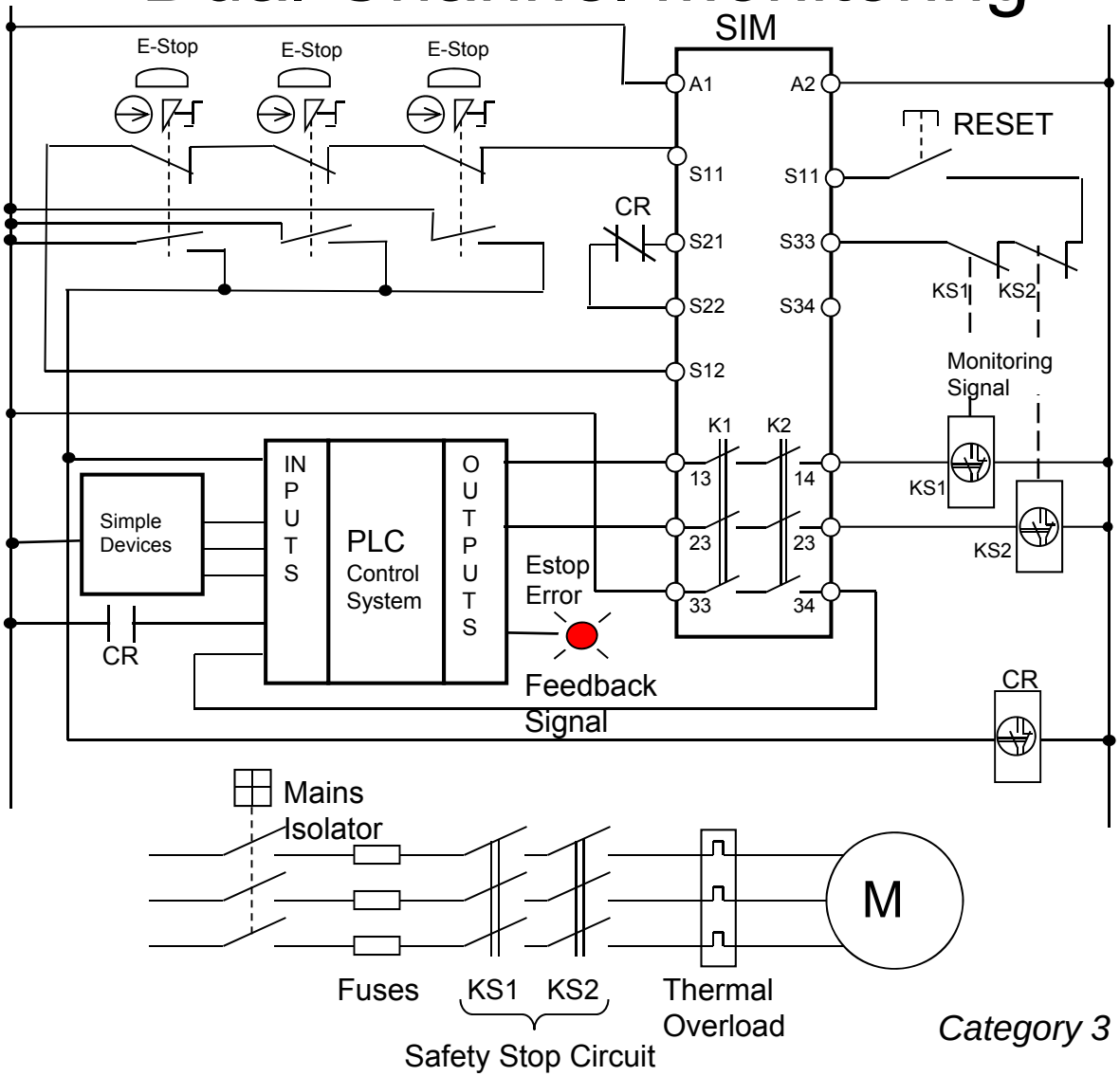
Category 3



Adapted from B11-TR6=2010

Safety Function:	**When the E-stop is pressed, the power to the coil of FGR1 and FGR2 is removed.** **When the E-stop is reset, the hazardous portion of the machine does not automatically restart.**
Faults to Consider:	**E-stop contacts falling off the push button actuator.**
Fault Exclusion:	**Welded E-stop contacts can be excluded since direct opening action contacts are used.** **The NC and NO contacts of FGR1, FGR2 or FGR3 cannot be in the closed state at the same time since mechanically linked contacts are used.** **Catastrophic failure of the e stop device can be excluded if designed and installed per ISO 13850 and tested at periodic intervals.**
Safety Principles:	**The normally open contacts of FGR1 and FGR2 open and remove power to the hazardous portion of the machine.** **While the E-stop is in the depressed state, the power to the hazardous portion of the machine remains off.** **When the E-stop is rest, the hazardous portion of the machine must not restart. Restart is accomplished by a separate deliberate action.** **To achieve a Category 4, prevent a short circuit between E-stop contacts, use complimentary switching or bi-polar switching. Category 3 requires dual contactors. Monitoring of at least one contactor is required; monitoring of both is recommended.**

Dual Channel Monitoring

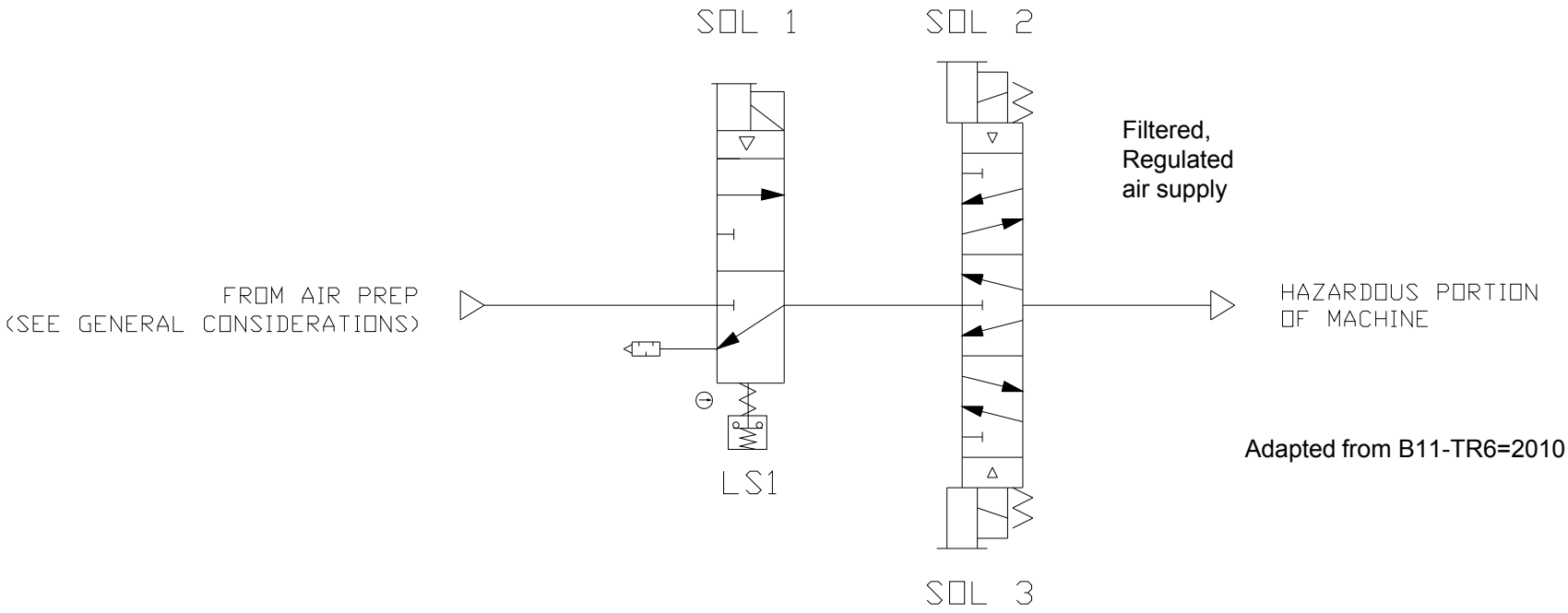


- Monitor of Estop contacts with contact follower force guided relay CR at safety interface module and in PLC. .
- Failure of CR to cycle with operation of Estop results in failure detected by the SIM
- Provides device status output without the addition of a third contact per device
- Estop Series connection still permits the work around of a shorted contact. Can be detected by the PLC. If permitted to continue, a second fault may lead to the loss of the safety function
- Alternative, independent feed to PLC of each N.O. Estop contact and drive CR relay with PLC logical OR output. This will provide individual contact fault status for HMI indication

Category 3 may be 4 with exclusions

Air supply Blocking/Venting valve and spring centered directional valve

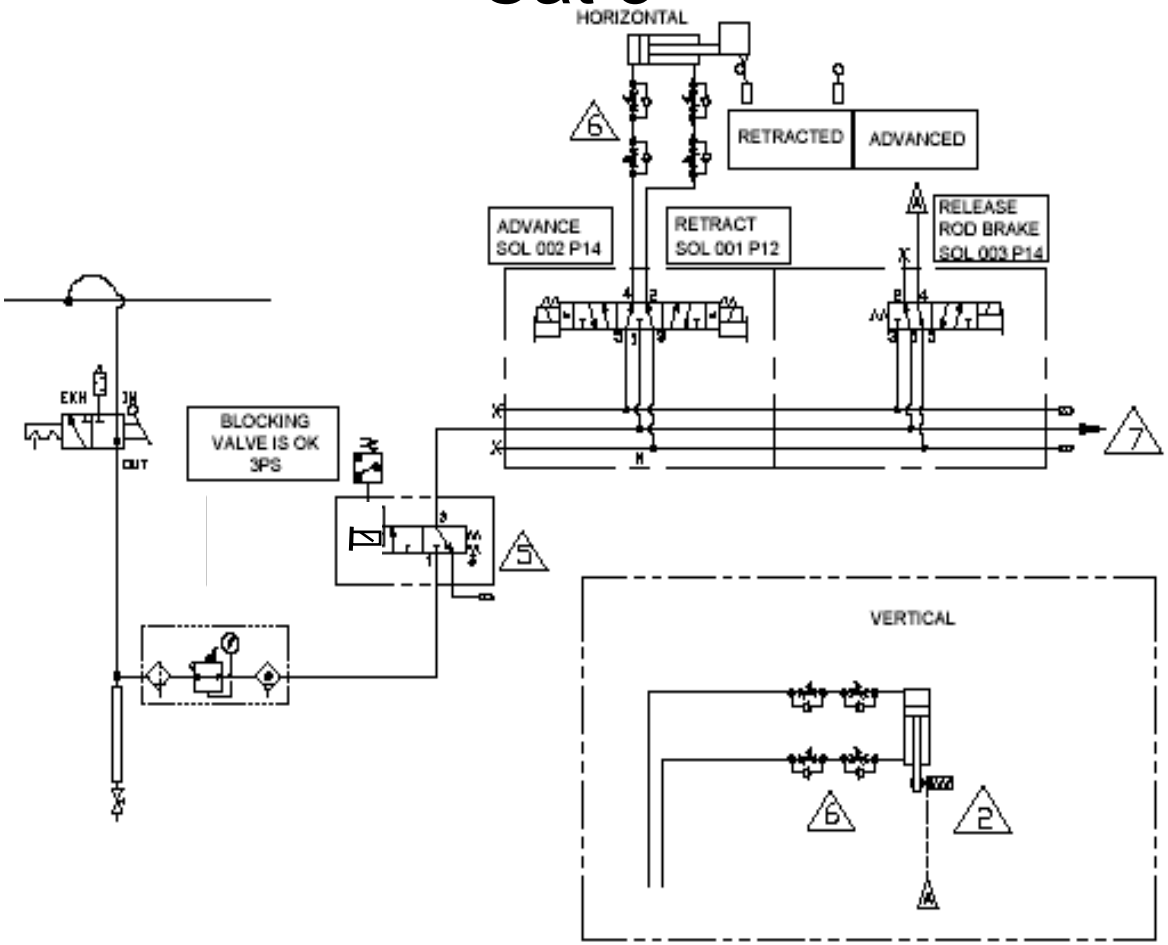
Category 3



Adapted from B11-TR6=2010

The spring centered directional valve provides the second means of stopping air flow to the hazard. However it is not monitored since while it may shift under the power of the solenoids, it might not center under spring force alone. To meet the requirement of a Cat 4 structure, a direct or indirect monitoring of the spring centered valve must be provided

Dual Channel with Monitoring Pneumatic Cat 3



- Blocking valve limit switch is monitored by either the PLC or the safety circuits

- Even though the directional valve has been cycling, as evidenced by the running machine, it is not assured that it will center providing the second channel of control

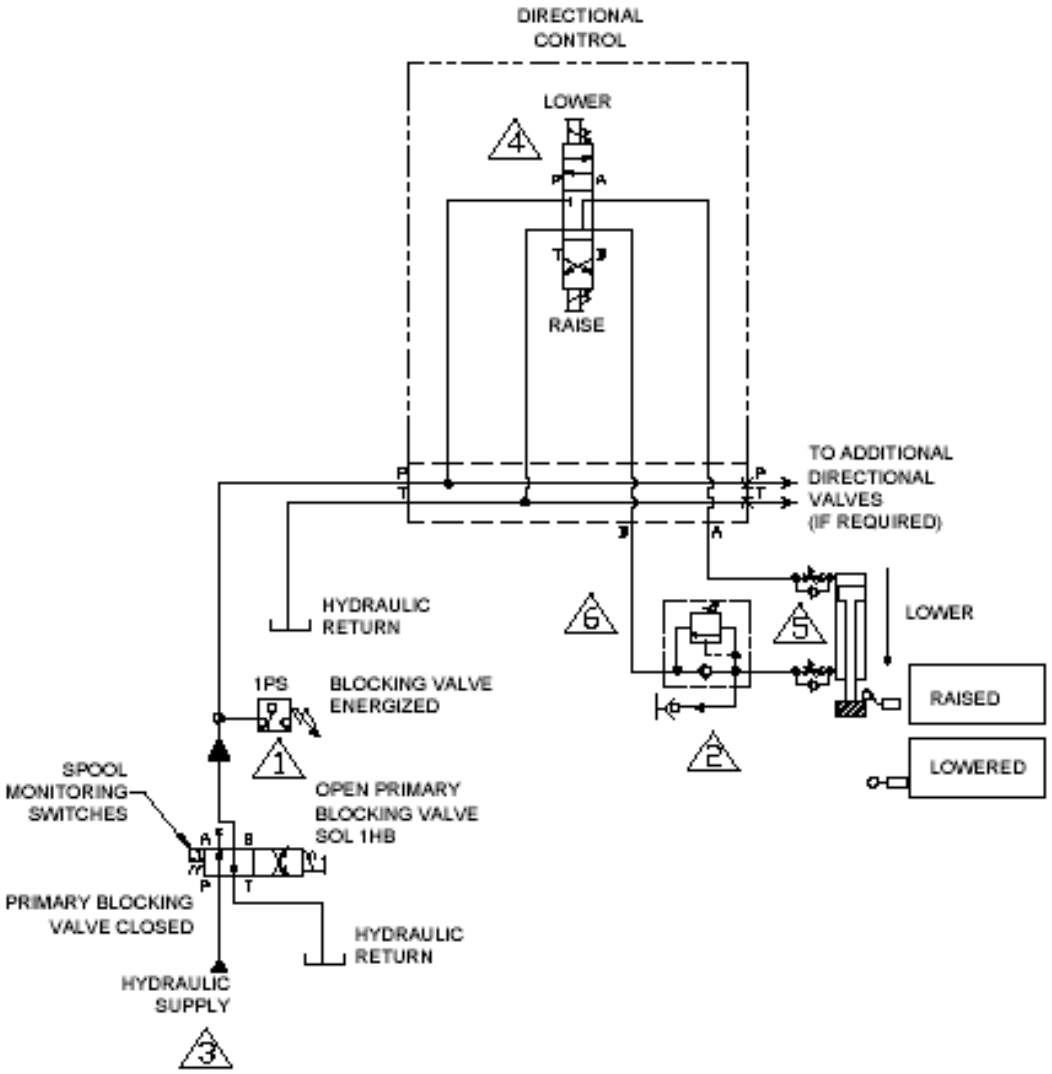
•The use of spring centered valves allows the holding of the cylinder in mid-stroke, but with potential drift due to blow-by.

•This design also shows a cylinder brake solenoid for vertical component loads. Since it cannot over-ride the pressurized piston, it does not add to the safety channels. The static hold is single channel

•Both flow IN and flow OUT speed control is shown. Flow out is the slower setting controlling the maximum rod speed. Flow IN is to limit speed if back pressure is lost after the release of a tooling jam.

•Vertical load is held by a spring to engage rod bake, alternate solution is a pilot operated check valve in the lower cylinder port. If controlled by a separate valve, it would add another control channel but only in the down direction, as it can counter the pneumatic force if the directional valve fails to center

Dual Channel with Monitoring Hydraulic Cat 3



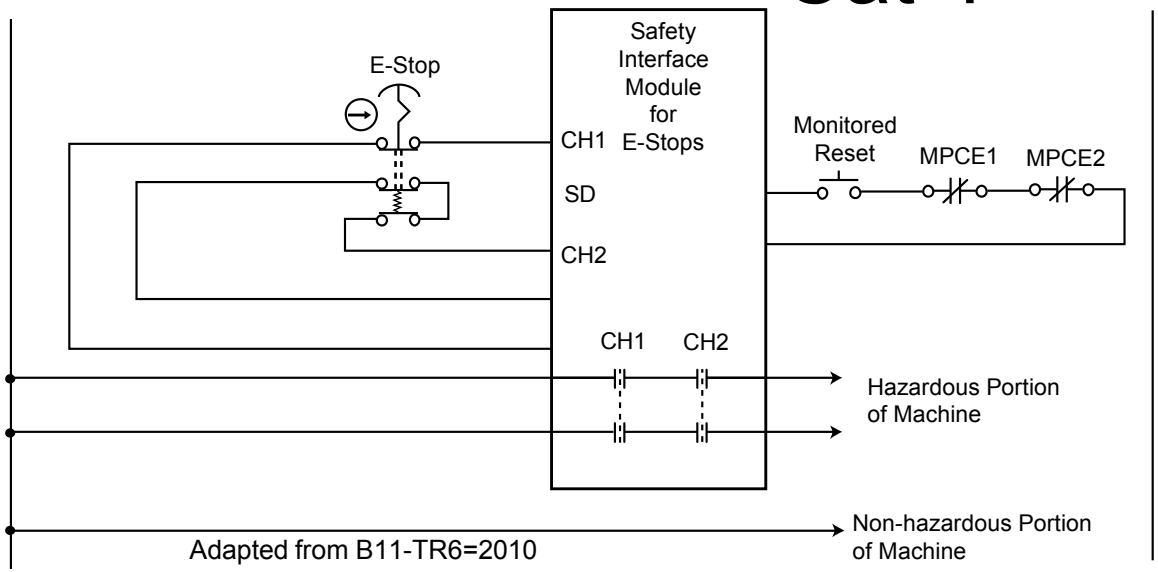
- Primary blocking valve is controlled by the safety interface relay to energize the solenoid

- Even though the directional valve has been cycling, as evidenced by the running machine it is not assured that it will center providing the second channel of control

- Performance of the primary blocking valve is monitored by either the PLC or the safety interface relay. Blocking valve could be monitored by internal spool sensors or pressure switch as in 1PS.
  - Pressure switches typically do not have force guided contacts. Add FG relay to obtain contacts
  - NC contacts are monitored in the safety interface module
  - Cycling of the contacts should be monitored in the PLC

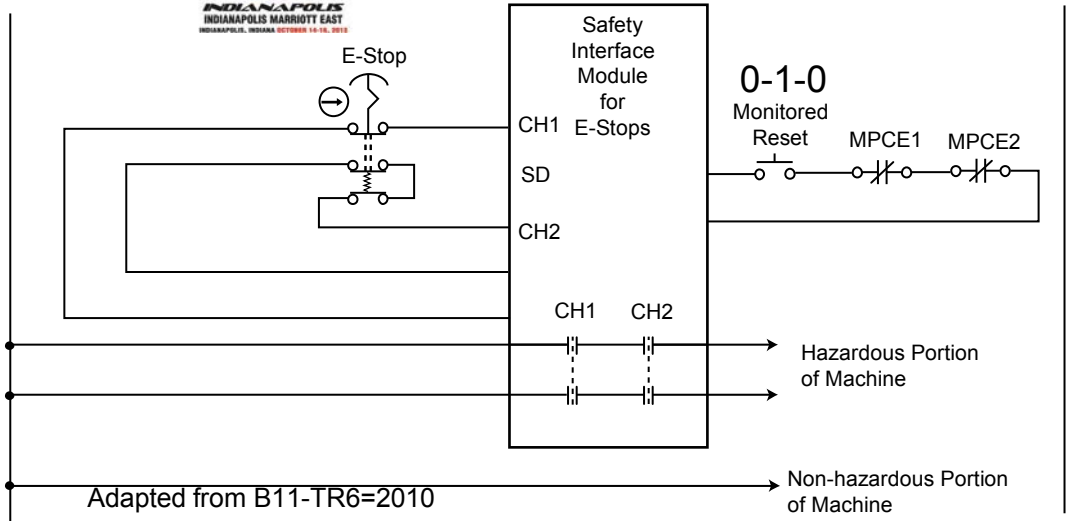
- Note that any vertical component of the cylinder and tooling must be separately managed. The blocking valve only removed hydraulic pressure, the directional valve controls kinetic and potential energy. The foot valve holds the static load. As such, the static holding is a single channel circuit, and requires that at least one of the other valves function

Cat 4



The means of detecting a separation of contact block from push button operator is symbolic as the means are varied and vendor specific

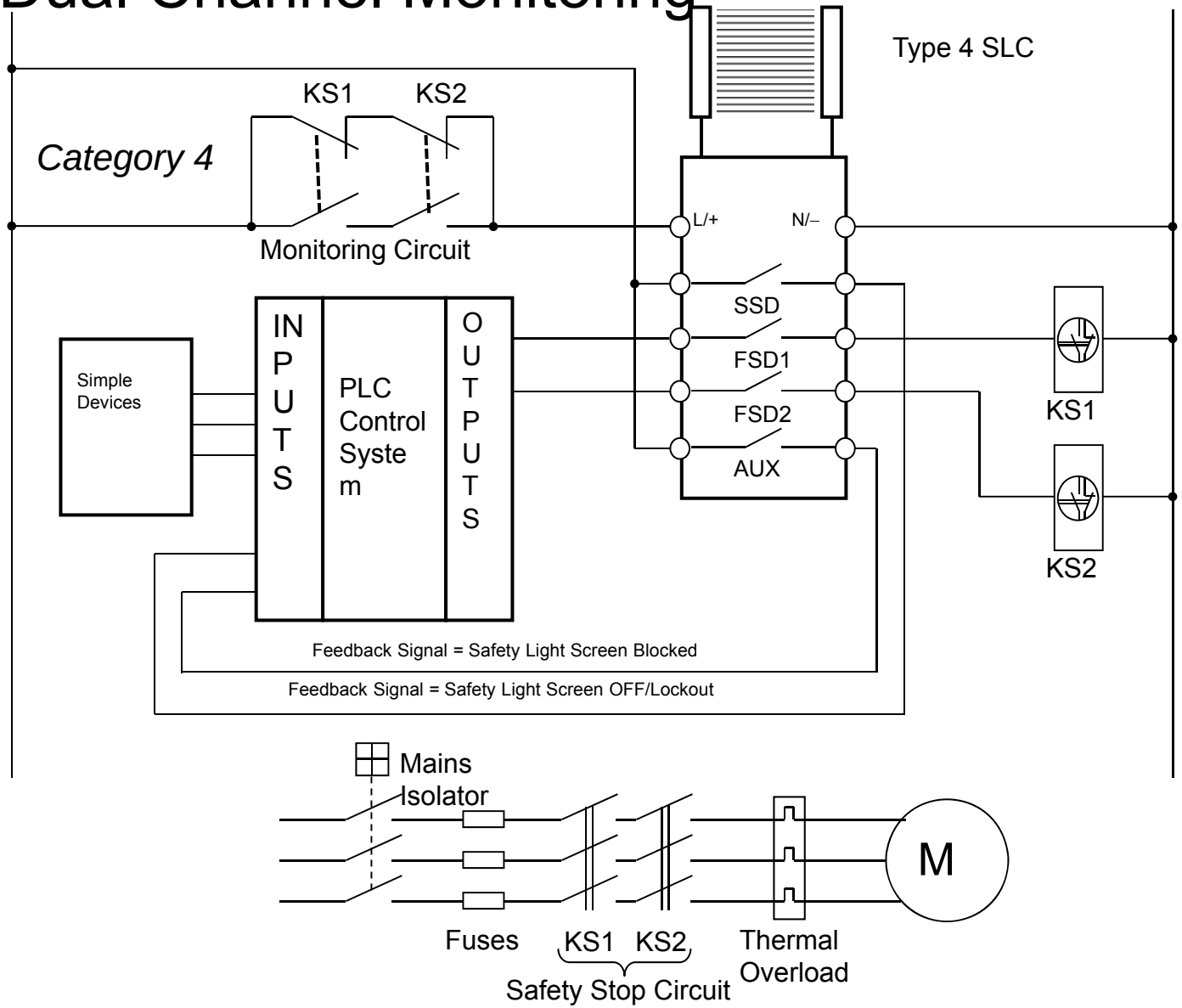
Safety Function:	**While the E-stop is in the depressed state, the power to the hazardous portion of the machine remains off.** **When the E-stop is reset, the hazardous portion of the machine does not automatically restart.**
Faults to Consider:	**None to consider.**
Fault Exclusion:	**Welded E-stop contacts can be excluded since direct opening action contacts are used.** **The NO contacts of the monitoring safety relay failing shorted can be excluded because they are redundant and cross monitored.** **A short across the reset contacts or a stuck reset button is excluded because the safety interface relay is looking for a change of state.** **Catastrophic failure of the E-stop device can be excluded if designed and installed per ISO 13850 and tested at periodic intervals.**
Safety Principles:	**At a minimum, the E-stop device should be designed and installed per ISO 13850 and tested at periodic intervals. If the E-stop contact block falls off the panel, the circuit does not lose the safety function.**



Category 4

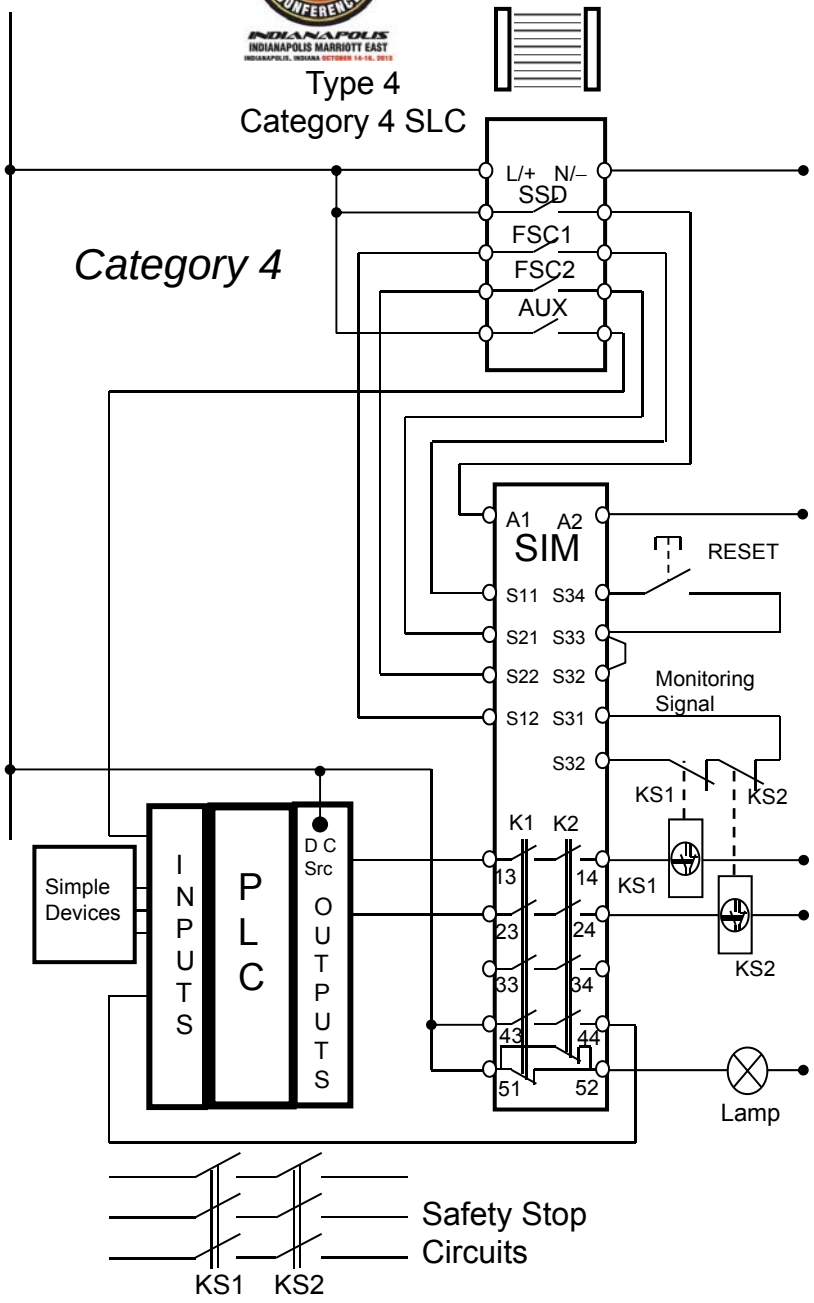
- A category 4 SIM is used to monitor the Estop contacts, and the MPCE
- The SIM is capable of
  - Detecting wire to wire and wire to power source shorts
    - Typically only on solid state outputs which can be pulsed
    - Typically only on isolated contact inputs which are tested with a pulse from the SIM
    - NOTE: This capability is product specific, verify with data specification sheet
  - The reset is monitored to prevent automatic reset of the safety output
- Loss of physical contact of Estop operator with contact block is detected
  - The method shown is diagrammatic as implementation mechanism is vendor specific

Dual Channel Monitoring



Total dual channel with monitoring
Cat 4

KS1 and KS2 force guided relays are monitored for the same state in series/parallel connection.
SLC controller power supply must internally bridge the momentary loss of power during contactor transfer
Use of over-lapping contacts, which in other applications could be used to bridge the contactor switching gap is not permissible.



Dual Channel Monitoring

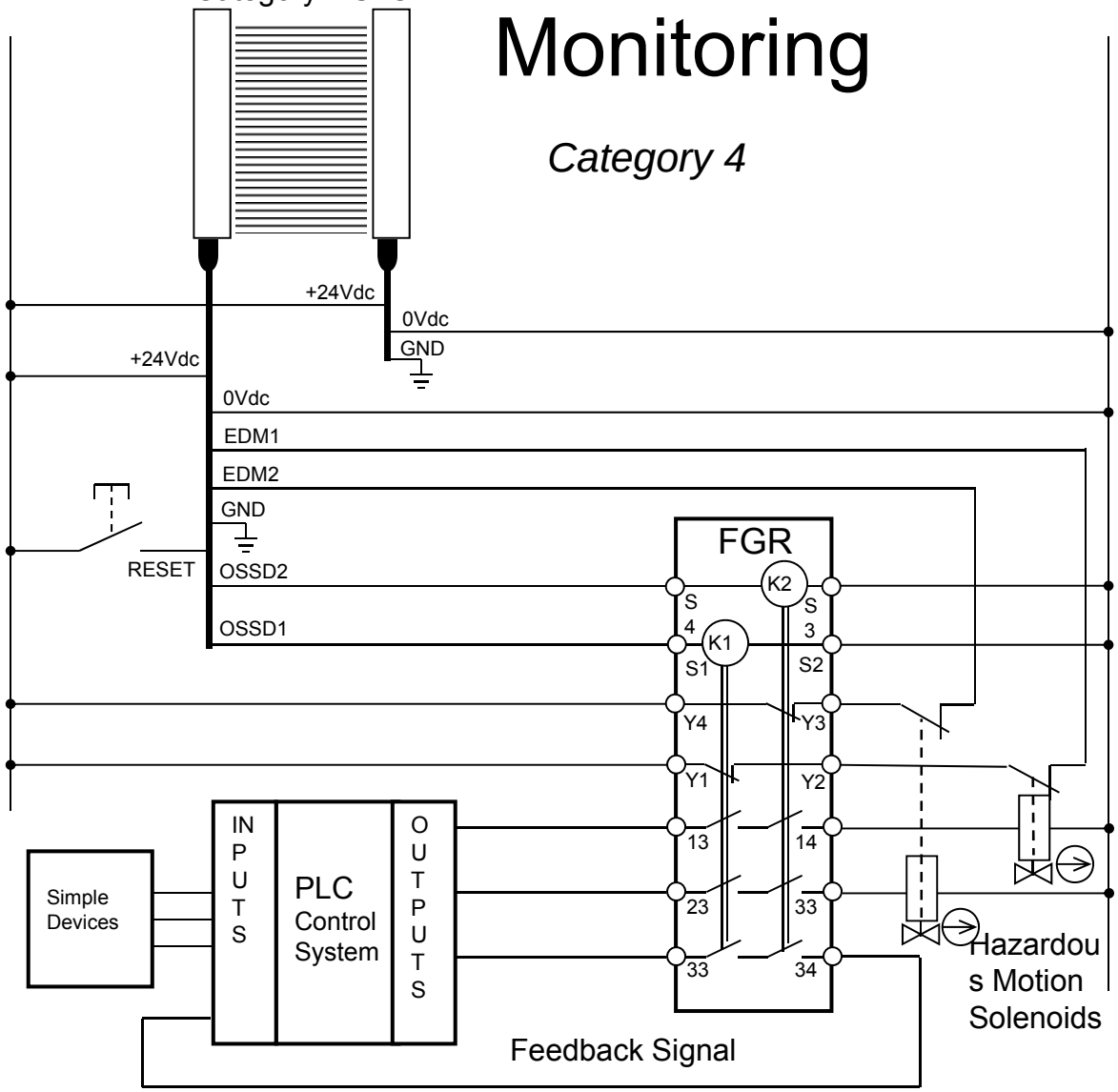
- Do all safety circuit applications require a safety interface module to monitor safeguarding devices?
  - NO, NOT IF the Safeguarding device has:
    - Self monitoring Force Guided relay or OSSD Output
    - Wire shorts are detected or excluded
    - Has EDM to monitor expansion relay or load

- In this example, the safety light curtain does NOT have an EDM function nor output wiring short detection and the KS1 and KS2 monitoring is accomplished by the safety interface module. It also serves to increase the fan-out without adding undetected failure modes

- Note: This type of monitoring with a safety interface module is often required by the " Two Component" Safety Light Curtains if
  - They do not have the monitoring EDM input, thus requiring a third component to perform the safety function.
  - A safety interface module or expansion relay may also be required if the safeguarding device has OSSD outputs which are not be internally checked for cycle or connection to an external power source

Dual Channel Monitoring

Category 4

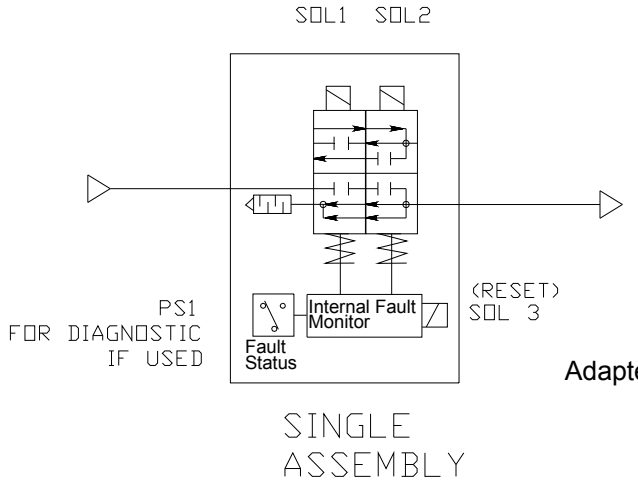


- A simple Force Guided Relay module which is an active input extension module may be used because the SLC
  - Has internal monitoring of the OSSD against internal failure and external wiring shorts
  - Has a separate external device monitoring, EDM, capability to detect failure of either of the two relays or the valves
- Without on-board EDM or output monitoring on the SLC a separate safety interface module would be needed to perform the monitoring functions
-

A closer look at the Outputs for Cat 3,4

- There must be two means of eliminating the hazard
  - Each capable of individually eliminating the hazard, regardless of the status of the other
- Final Switching device which controls the power flow to the hazard
  - Machine Primary Control Element (MPCE)
  - Each individually able to control power to the hazard
  - Removal of the CONTROL signal from the MPCE does **NOT GUARANTEE** that the power has been removed from the hazardous device
- The failure to danger of one output or MPCE, if left undetected, reduces the circuit to a single channel Cat B or 1
- Therefore, EACH must be monitored, for its state that removes power, on <u>each cycle of the safety function</u>

Cat 4 Pneumatic Integral Safety Valve

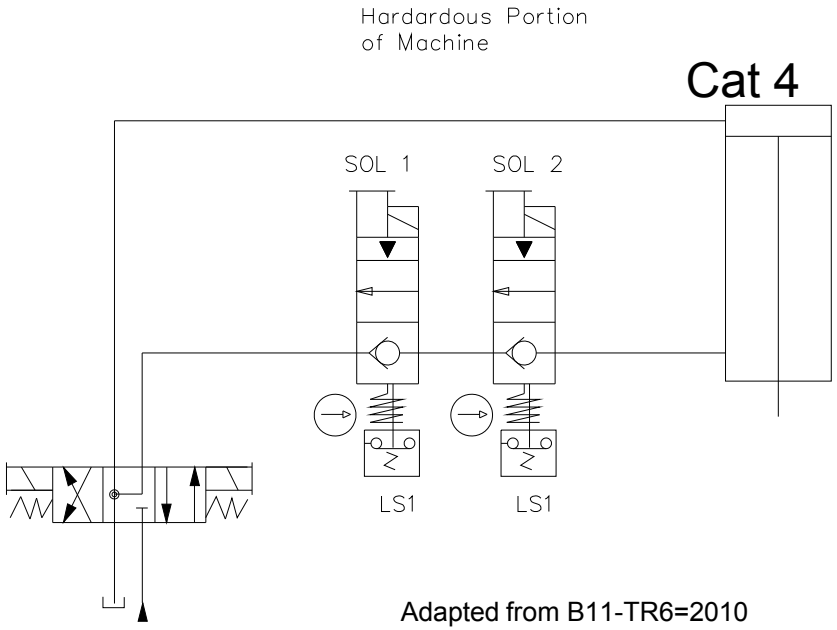


Adapted from B11-TR6=2010

- The valve is a double power spool, each individually capable of venting the load and blocking the supply.
- Internal porting prevents one spool from passing air if, after release of the solenoids, either of the spools has failed to block and vent and therefore the valve itself creates the monitored dual channel.
- An electrical contact is provided to indicate that an internal fault has locked the valve in the blocking mode.
- Failure of this contact arrangement does not compromise the spool safety function
- Each Solenoid is driven by a separate safety output,
- Fault reset may be automatic, manual, or as shown, electrical input
- Other configurations provide spool position of the two power spools electrically for shift to blocking and are monitored in the EDM part of the safety circuit

Hydraulic circuit

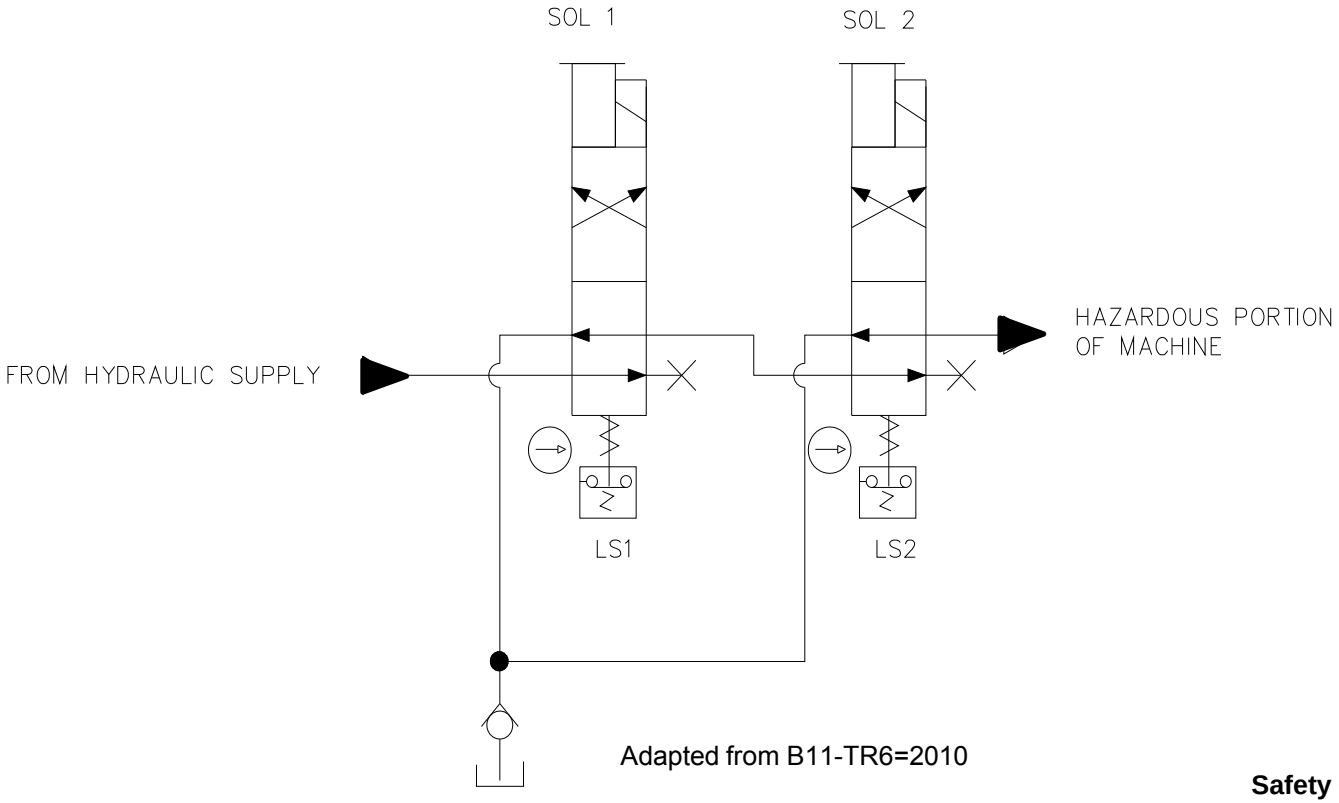
- In this choice of hydraulic valves, the drain of the cylinder in the advance direction is prevented by two individual blocking valves providing a hydraulic lock.
- The rod advance constitutes the hazard, the retract is not hazardous
- Each solenoid is driven by a separate safety output
- To maintain the Category 4 for the system, both MPCE LS1 and LS2 must be monitored in the SRP/CS's EDM
- Note: To prevent pressure intensification, the "advance" position of the directional valve should not be activated with the drain valve(s) closed.
- This arrangement has an additional feature which allows a special manual function to raise but not lower the ram under the safety stop condition by flow through the check valves



Adapted from B11-TR6=2010

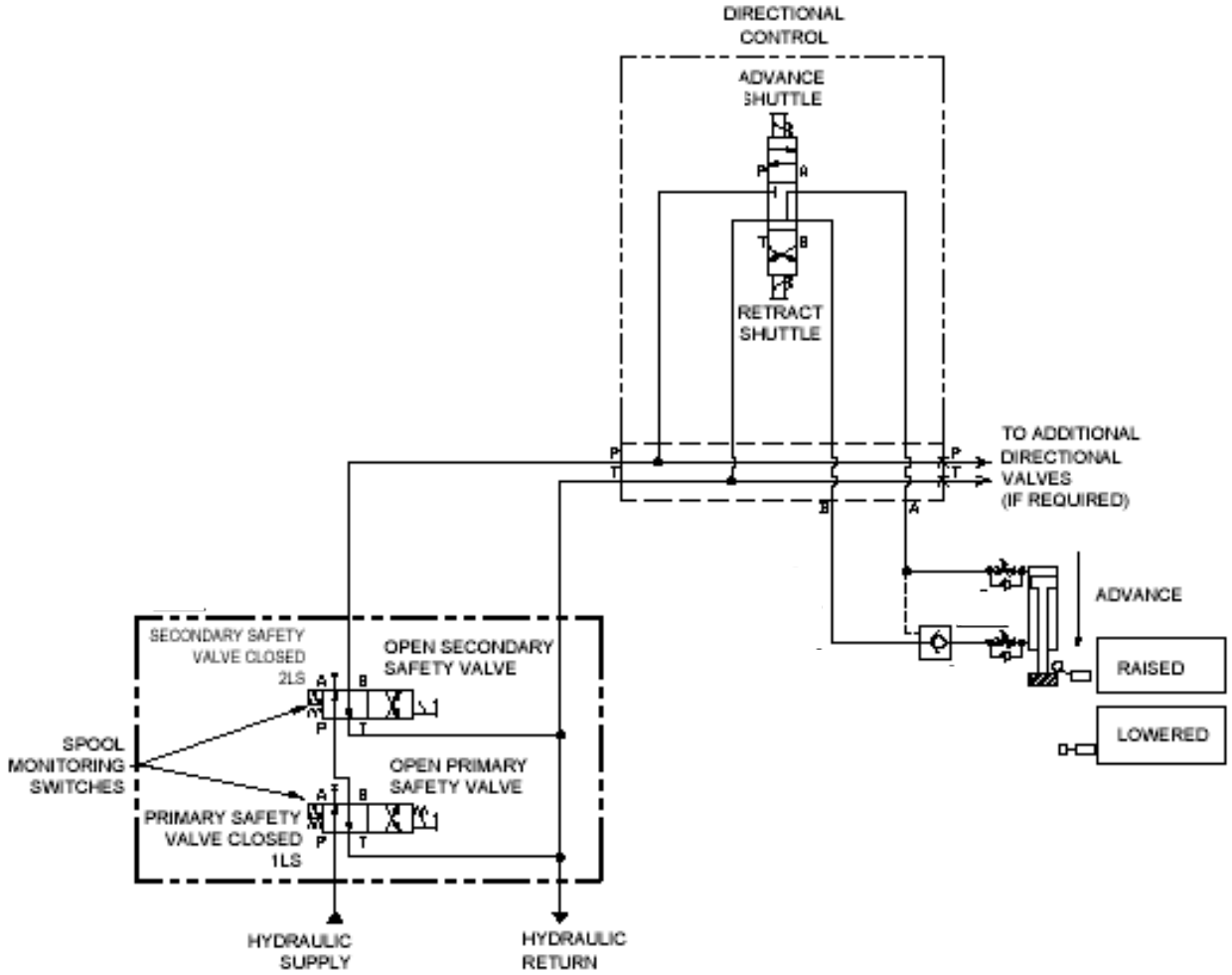
Hydraulic Cat 4 System

- This valving may be used to supply multiple directional valve system
  - Individual components may be needed to hold up gravity advance loads due to the drain connections of all lines.
- MPCE Sol 1 and Sol 2 are driven by individual safety outputs
- MPCE LS1 and LS2 are monitored in the SRP/CS's EDM



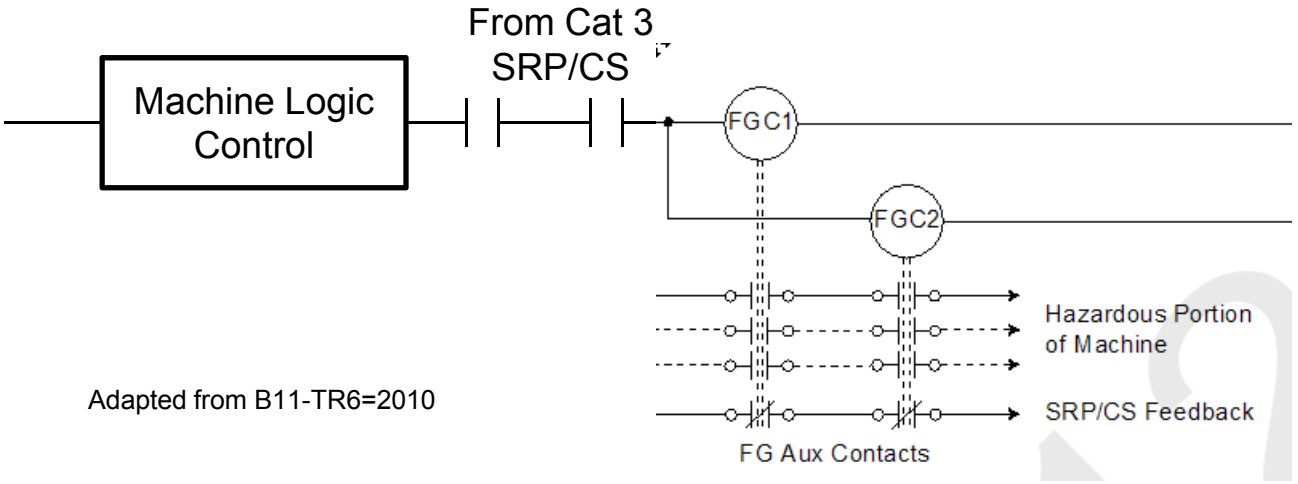
Adapted from B11-TR6=2010

Dual Channel with Monitoring Hydraulic



- Two pressure supply valves are used, each energized by separate channels of the safety interface relay. Valve performance is monitored by spool sensors connected to their own dual channel Cat 4 safety interface module's EDM

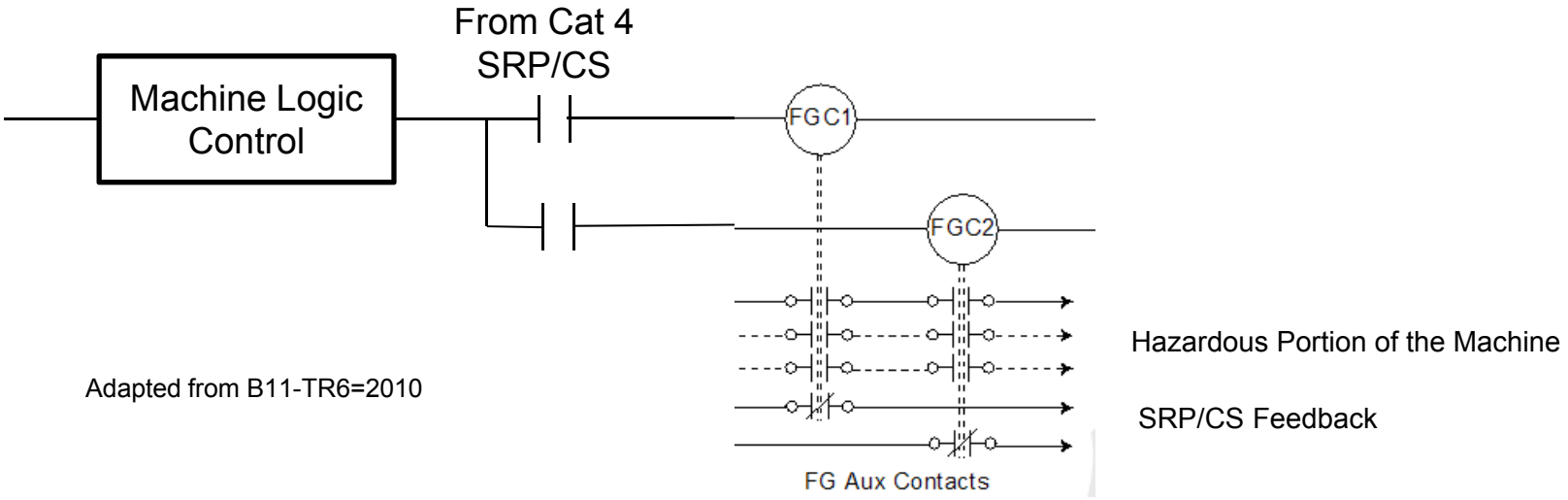
Category 3 Output



Adapted from B11-TR6=2010

- When contacts from Cat 3 SRP/CS go low contactors FGC1 and FGC2 drop removing power from the hazardous portion of the machine
- Contactors are monitored by the SRP/CS
- Care must be taken to prevent feedback from shorting to a power source
- The common feed to FGC1 and FGC2 is a single point of failure
  - Short to a common supply must be excluded

Category 4 Output



Adapted from B11-TR6=2010

- When contacts from Cat 3 SRP/CS go low contactors FGC1 and FGC2 drop removing power from the hazardous portion of the machine
- Contactors are individually monitored by the SRP/CS
  - If individual monitoring is not possible, the contacts may be wired in series, but the wires must be protected from shorts so that shorts to another supply may be excluded
    - This can also be accomplished by assuring that the contacts cycle with each cycle of the safety function

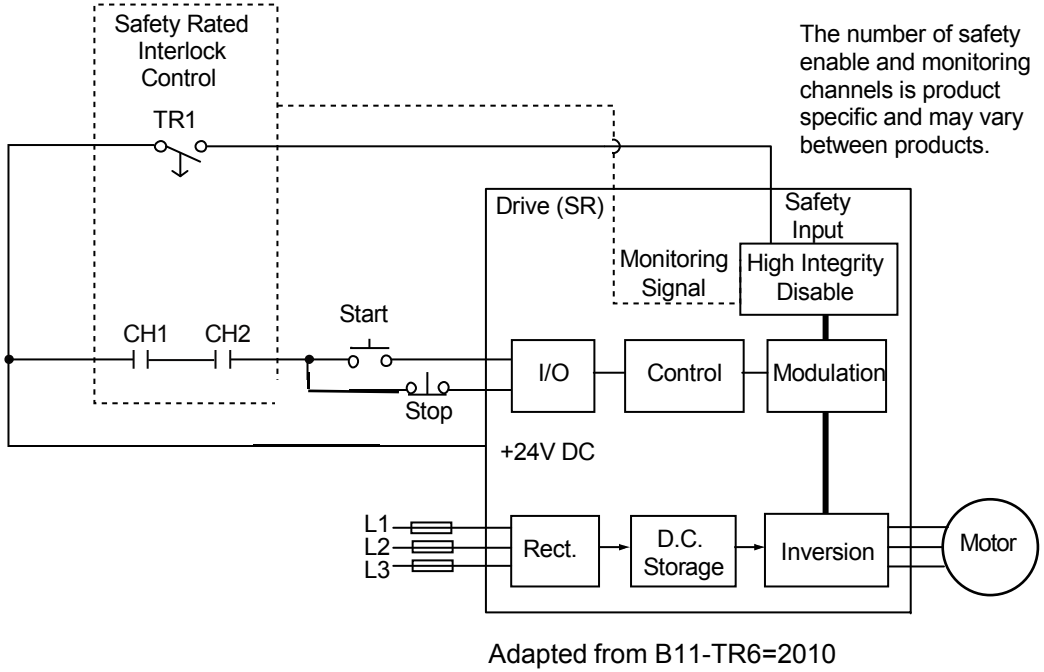
Smart Drives

- Smart Drives
  - Variable Frequency Drives
  - Servo Drives
  - Industrial Robots
- Control Safety Performance Capability
  - Varies with Drive Type, Vendor, and Feature Set Options
    - Safety capability typically up to Cat 3 PLd
      - Now permitted in NFPA 79 and ISO 10218-1,2
      - Now have Safety Rated controller options
        - » Stop, Hold, Speed, Torque
        - » Robots may have controller Restricted Space which is safety rated
- Interface controls with drive
  - Design features of the Safety Function as with any other control of an MPCE using appropriate risk reduction design
  - If safety capability of drive is equal or greater than risk reduction performance required, connect directly to controller
    - Verify with manufacturer
    - Consult drives manual on capability and function specific functions, names will vary between manufacturers for the same features
  - If controller safety rating is lower than what is required by the risk assessment, add additional MPCE devices to enhance capability

Safety Features of Smart Drives

- Features are OPTIONAL
  - Review need before purchasing as retrofit may not be possible
- May have varying safety rating, typically PLd
- Features include but not limited to
  - Safe Off
  - Safe Stop 0 (NFPA 79 Stop category 0)
  - Safe Stop 1 (NFPA 79 Stop category 1)
  - Safe Hold (NFPA 79 Stop category 2)
  - Safe Torque Off
  - Safely Limited Torque
  - Safely Limited Speed
  - Safely Limited Position (Safe Cam)
    - In Robot may be used to set Limited Space
    - May be Inclusive or Exclusive

Safety Rated Drives



Adapted from B11-TR6=2010

Note: **Stop Categories are not safety ratings**

They determine the state of power on the motor at the end of the stopping function and is defined by NFPA 79

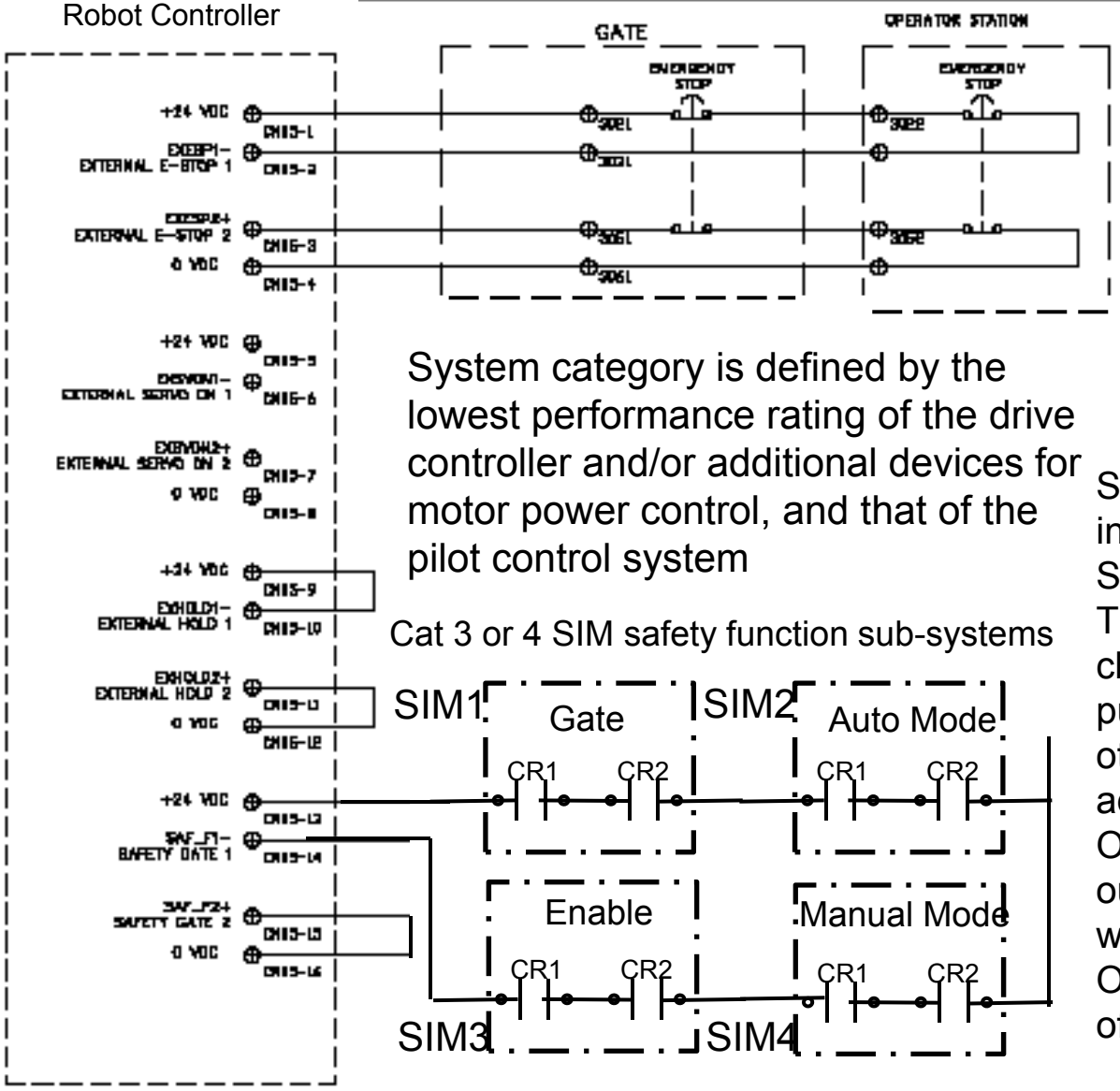
Cat 0: power off at the stop command

Cat 1: Controlled power to bring to stop, then power off

Cat 2: Controlled power to stop, power maintained to provide additional function capability such as torque for holding up a load

- Variable Frequency and Servo Drives, as well as Robot Controllers, are now available with on-board safety rated control capability.
  - The pilot control must have at least the same safety performance capability as the drive, to maintain the performance for the system

Representative Robot Controller



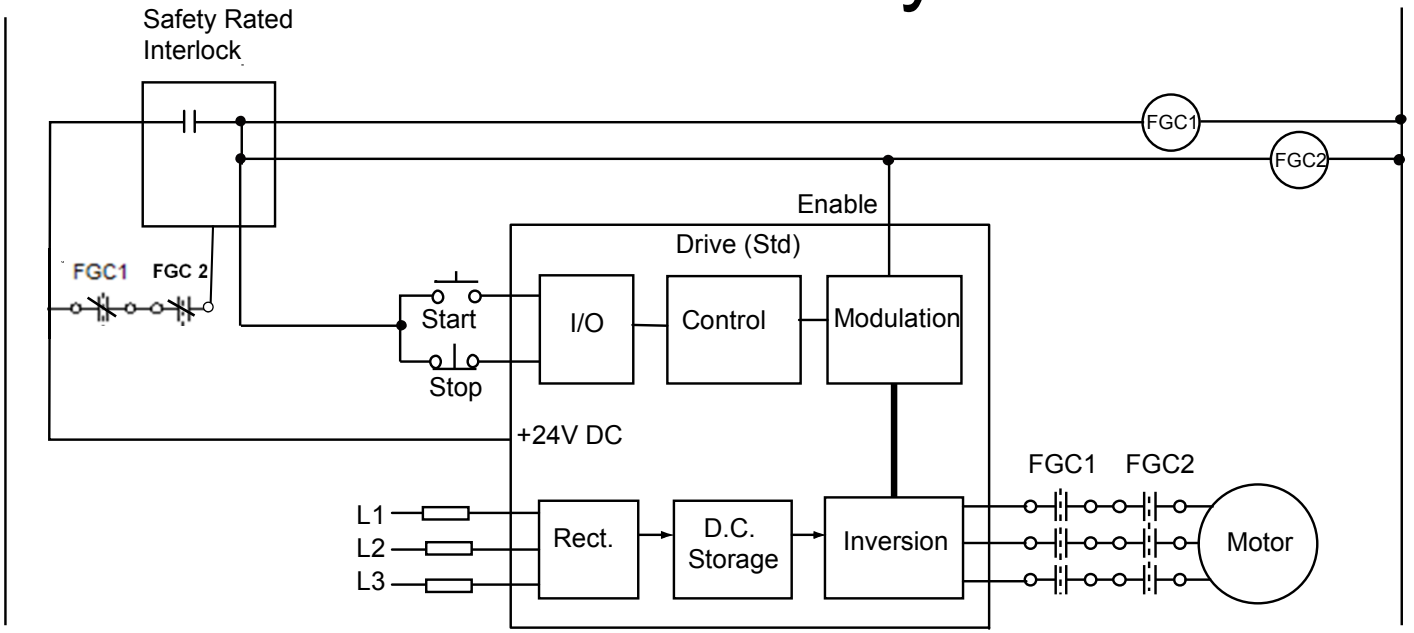
Depending on the risk and/or the Robot Controller safety performance on this input, the Estop contacts may be taken directly to the controller or first monitored by an SIM

System category is defined by the lowest performance rating of the drive controller and/or additional devices for motor power control, and that of the pilot control system

Cat 3 or 4 SIM safety function sub-systems

Safety logic may be developed by interconnection of SIMs or in a Safety Rated Controller or PLC. This Robot controller is single channel input. If its 24VDC is pulsed and monitored, short to other supply need not be addressed. If not, a SIM with OSSD which detects shorts on output may be required. Check with vendor on impact of SIM OSSD test pulses and connection of DC common

Cat 4 on a non-safety rated drive

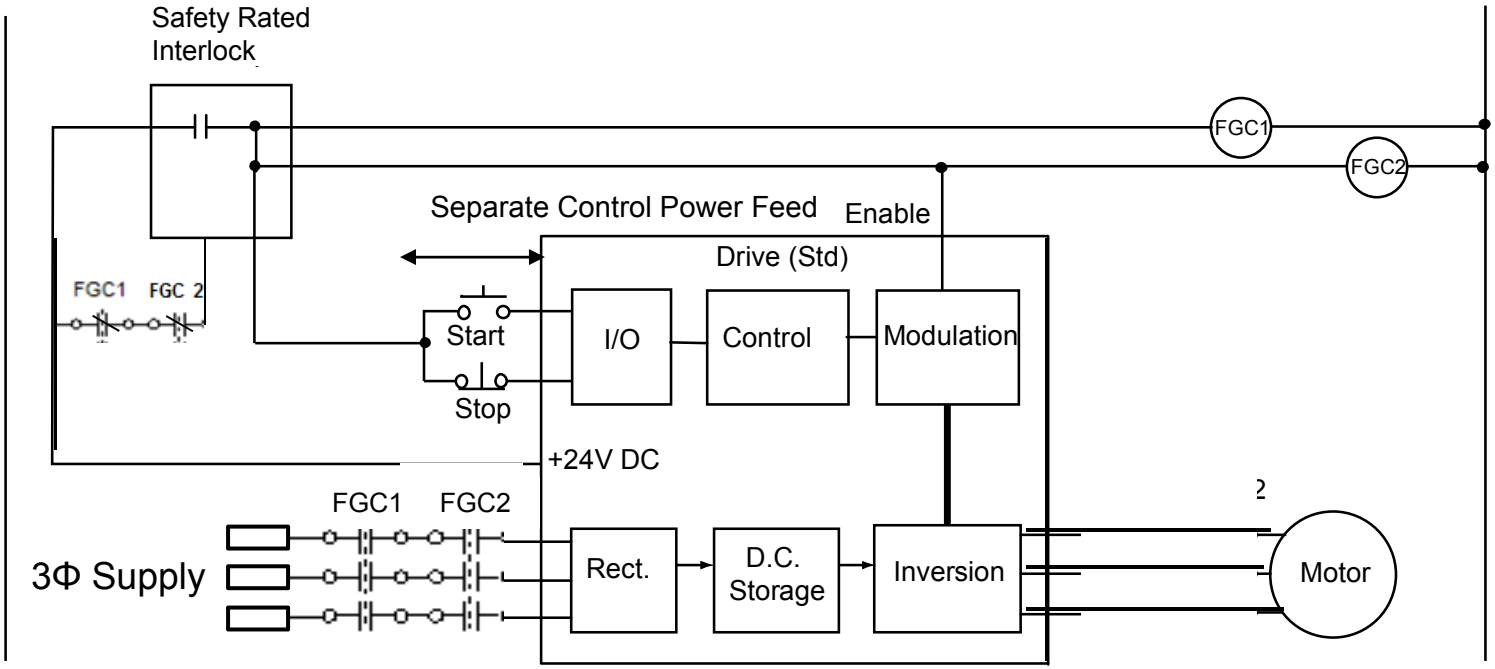


Adapted from B11-TR6=2010

- To meet Cat 4, dual monitored contactors may be used as with simple squirrel cage induction motors
- A single monitored contactor may be used to augment the Cat 3 motor safety controller

Note that although the contactors are shown here between the drive and the motor, this may not be acceptable for a specific drive manufacturer. For those, it is typically possible to add the contactor(s) on the power side of the drive while keeping power on the logic section to prevent re-start issues

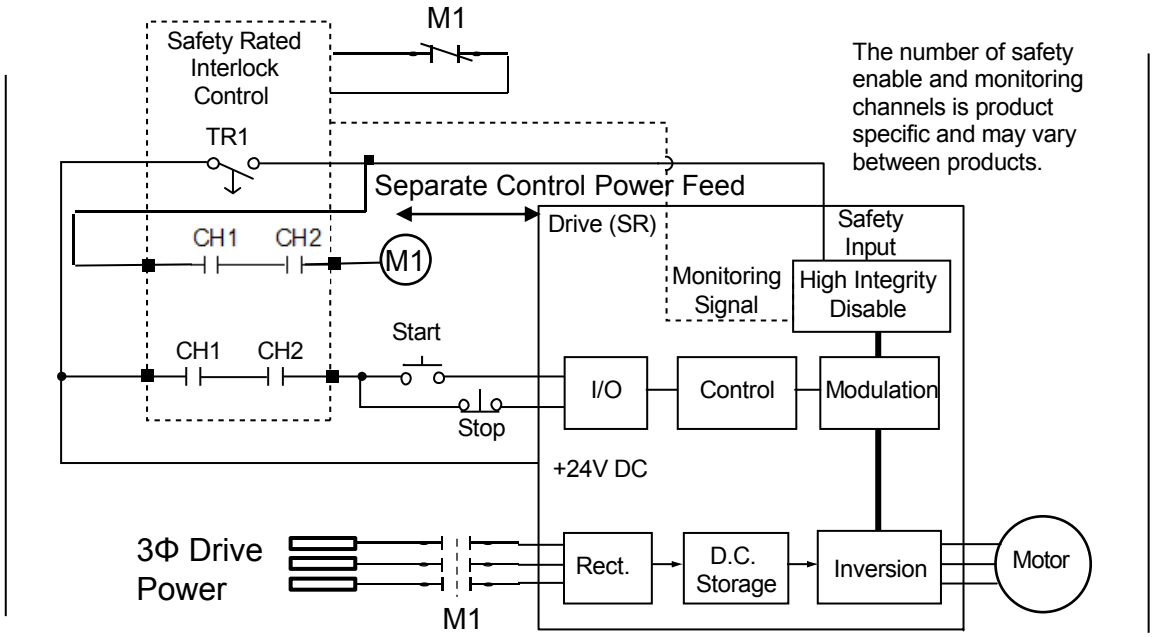
Cat 4 with Isolated Power and Control Feed



Adapted from B11-TR6=2010

The logic and control power is fed from a separate control voltage drop, which permits the isolation of the Inverter power without loss of the controls which typically requires a re-zero of the control function

Use of a Cat 3 Safety Rated drive with separate failure mode contactor to build Cat 4 performance system



Adapted from B11-TR6=2010

- The Cat 3 safety capability of the Drive is used for one of the two channel required for the Cat 4 system.
- Drive power module had separate 3Φ drop from control power, therefore may be isolated from supply to provide second means of power shut-off
- M1 is controlled with separate output and monitored to provide common cause failure isolation and monitoring

Access Gate Interlocking

- Robot cells require an enclosure around the robotic system
- Detecting entry into a safeguarded space through the monitoring of the status of a physical gate

Mechanical Limit Switch Door Interlocks

- Cat 3 One Switch
  1. Positive Mounted
  2. Direct acting
  3. Dual channel monitoring
  4. **Assure that limit is mechanically protected from door impact**
  5. With one switch mechanical operation failure is either

     Excluded or Accepted as an acceptable risk
  6. May wire switches from other doors in series
     - Operationally should have a low probability that multiple doors are opened together

Mechanical Limit Switch Door Interlocks

- Cat 4 Two Switches
  - Items 1 through 4 above plus wire short detection
    - Second limit may be negative mount as CCF solution
    - Not connected in series unless there is a low probability of simultaneous operation of multiple doors
  - Why the second limit switch
    - Standard design limit switches, although direct acting, may reasonably be expected to fail mechanically
    - Mechanical Failure Fault exclusion is typically not indicated for most limit switches for Cat 4 when alternatives are available
  - Alternative
    - Special heavy duty switch designs are available which have been certified by 3d party NRTL as meeting the over-design requirements for mechanical devices which permit the exclusion of mechanical failure
      - **Must be mounted and applied per manufacturer's direction for use**

Non-Contact Door Interlocks Cat 3 and 4

- Magnetic Reed
  - Use multiple reed switches and multiple magnet target
    - Difficult to defeat with standard magnets due to unknown orientations
    - SIM controllers typically add maximum time between transfer of one reed switch and another to hinder manipulation
  - Require low load interface
    - SIMs provide low inrush and inductance to prevent reed contact arcing and subsequent failure to re-open
  - May be capable of Cat 4 with one sensor

Non-Contact Door Interlocks Cat 3 and 4

- Cat 4 devices, typically may be wired in series and retain Cat 4
  - RF - Transmit power from emitter to receiver
    - Difficult to defeat as RF power flow chain must be retained
    - Require control box for output
    - Some reduction of system response with multiple sensor start up in series
  - RFID - Require target with special code
    - Permits use of unique code to reduce circumvention of interlock with “spare” target
    - Typically have OSSD output which may be wired in series
      - No significant impact on system response with multiple devices
      - Have individual output monitoring as part of unit
      - May have non-safety auxiliary output for functional monitoring in HMI or controller

Designing with SIMs

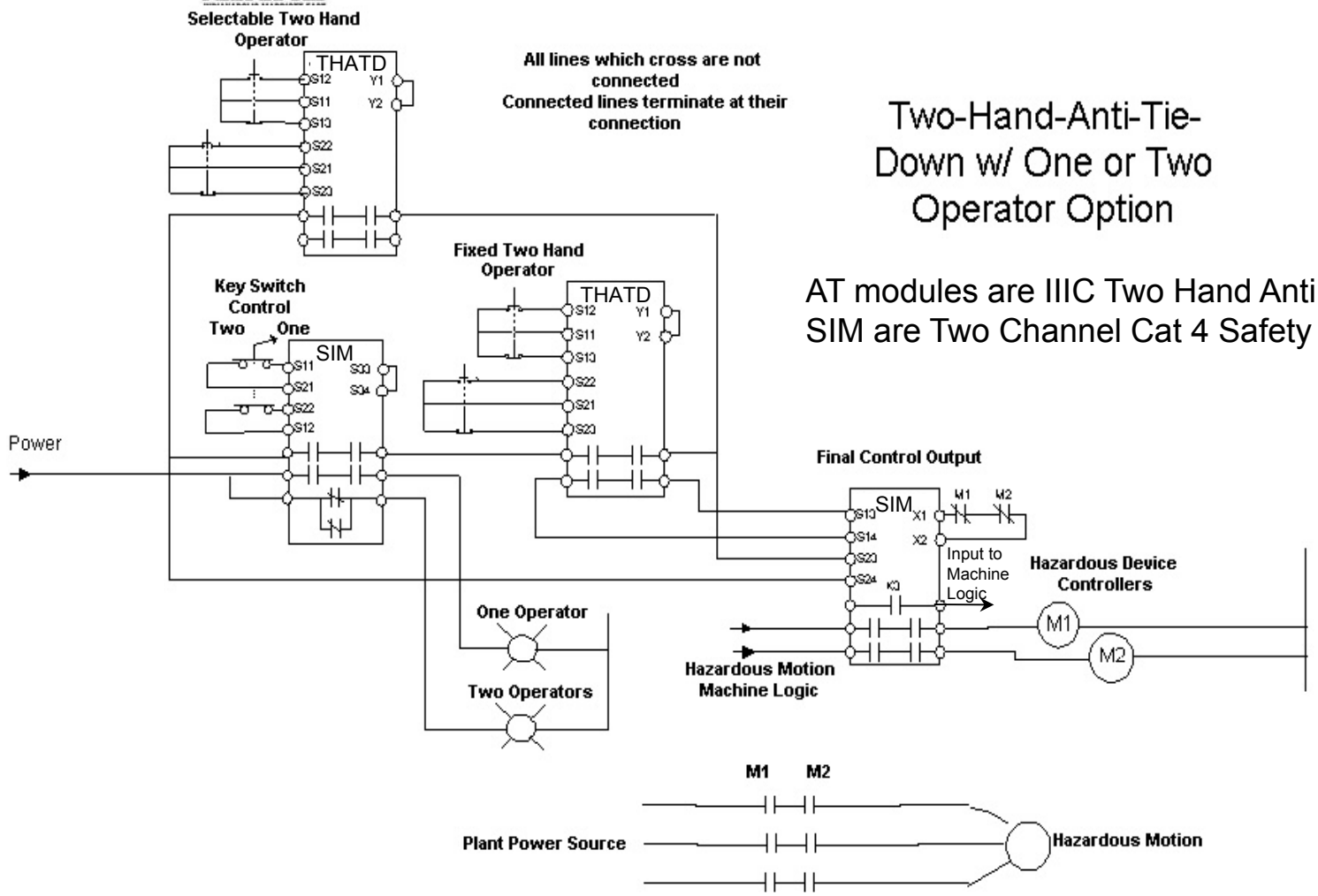
- Safety Interface modules are not binary devices as ordinary relays, but tertiary
  - Output is ON when inputs are true
  - Output is OFF when inputs are not true
  - Output is OFF when there is a fault in the input, output or the device itself
- A single SIM may be used to monitor a two stage input device only if the input OFF state represents a safety state situation.
  - Use of a single SIM to monitor multiple position selector switches is limited

Designing with SIMs

- For that reason, the N.C. contacts of a SIM used with monitoring of two state input channels are seldom used
  - Consider the “safe” monitoring of a dual contact selector switch for position “1” and “2”
    - In position “1” both input channels are true and the SIM outputs are HIGH
    - In position “2” both channels are low, and the SIM outputs are LOW
    - BUT if the SIM detects a failure
      - The SIM output ALSO goes LOW defaulting to a Position “2” output state.
    - If this default to Position “2” output at a failure is acceptable, the system as designed may be retained,
    - If however, the **default** state is **not acceptable**, a second SIM must be employed
      - Each SIM monitors the valid position of its respective selector switch contacts

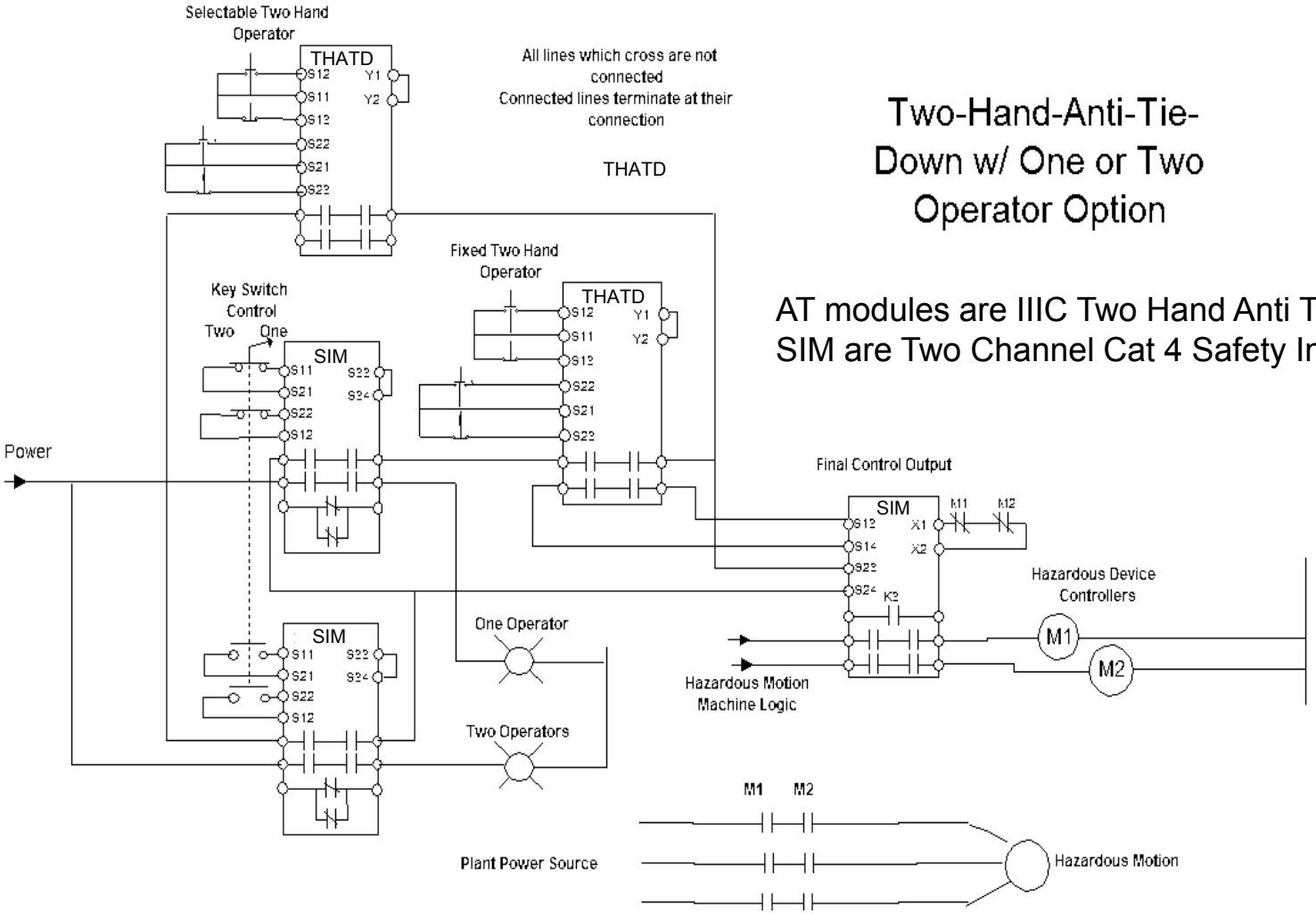
Two-Hand-Anti-Tie-Down w/ One or Two Operator Option

AT modules are IIIC Two Hand Anti Tie Down
SIM are Two Channel Cat 4 Safety Interface Modules



Since the loss of a safety interface module output may be due to a failure rather than the alternate state of the dual channel input, NC contacts are usually not used in permissive logic. Here the selection to two positions or a failure of the input or the relay causes the system to default to two station operation, the safe function. If this DEFAULT is not acceptable, a second safety interface module is used to monitor the ON state of the selector switch contacts in Two station mode**. Supplemental guarding, which may require interlocking, may be required at the hazard access utilized by position 2 when not selected for hand loading**
Additional logic may be required by specific standards which require indication of active output on the Two Hand operators

Two-Hand-Anti-Tie-Down w/ One or Two Operator Option



AT modules are IIIC Two Hand Anti Tie Down
SIM are Two Channel Cat 4 Safety Interface Modules

Failure of the selector switch will disable both modes of operation. Additional logic may be required by specific standards which require indication of active output of the Two Hand operators

In addition, supplemental guarding, which may require interlocking, may be required at the hazard access utilized by position 2 when not selected for hand loading Additional logic may be required by specific standards which require indication of active output on the Two Hand operators

Muting

- The AUTOMATIC suspension of the MONITORING OF THE STATE of a safeguarding device
- The safety performance of the muting function must be equal to or greater than that required by the safety function to be muted
- Muting function must be difficult to initiate manually so that it is not over-ridden
- Failure of the muting function to reset or its inappropriate initiation is a failure to danger of the safety function
- Muting may be called only:
  - When the safeguarding device is clear
    - Ex The Safety Light Curtain must be clear in order to be muted

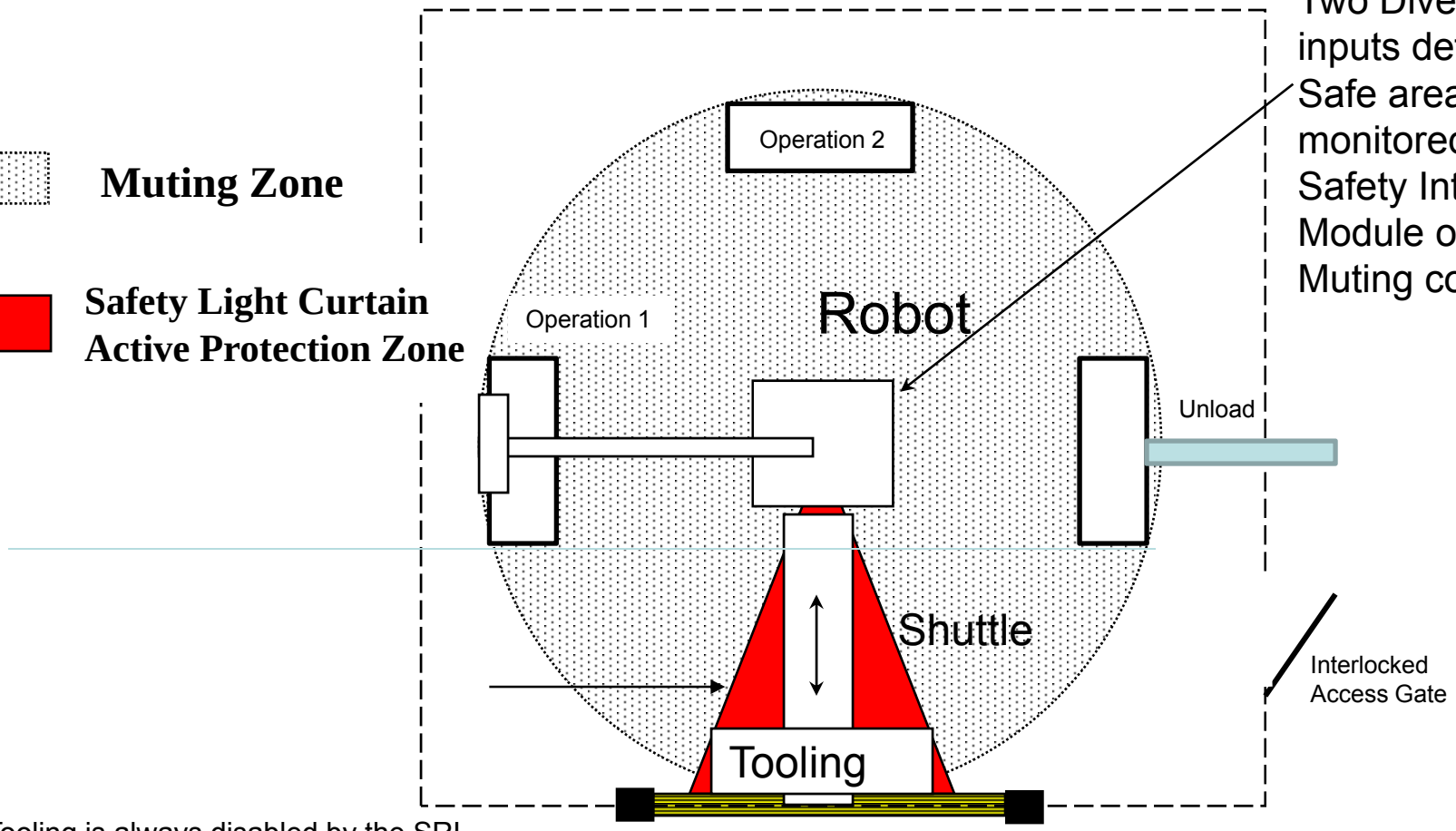
      AND
  - When there is no hazard
    - Ex Upstroke of the ram of a punch press with no other hazards

      OR
  - When some other device performs the risk reduction function
    - Ex A shipping pallet enters the opening of a safeguarded space monitored by a Safety Light Curtain and blocks all entry

Muting

Muting Zone

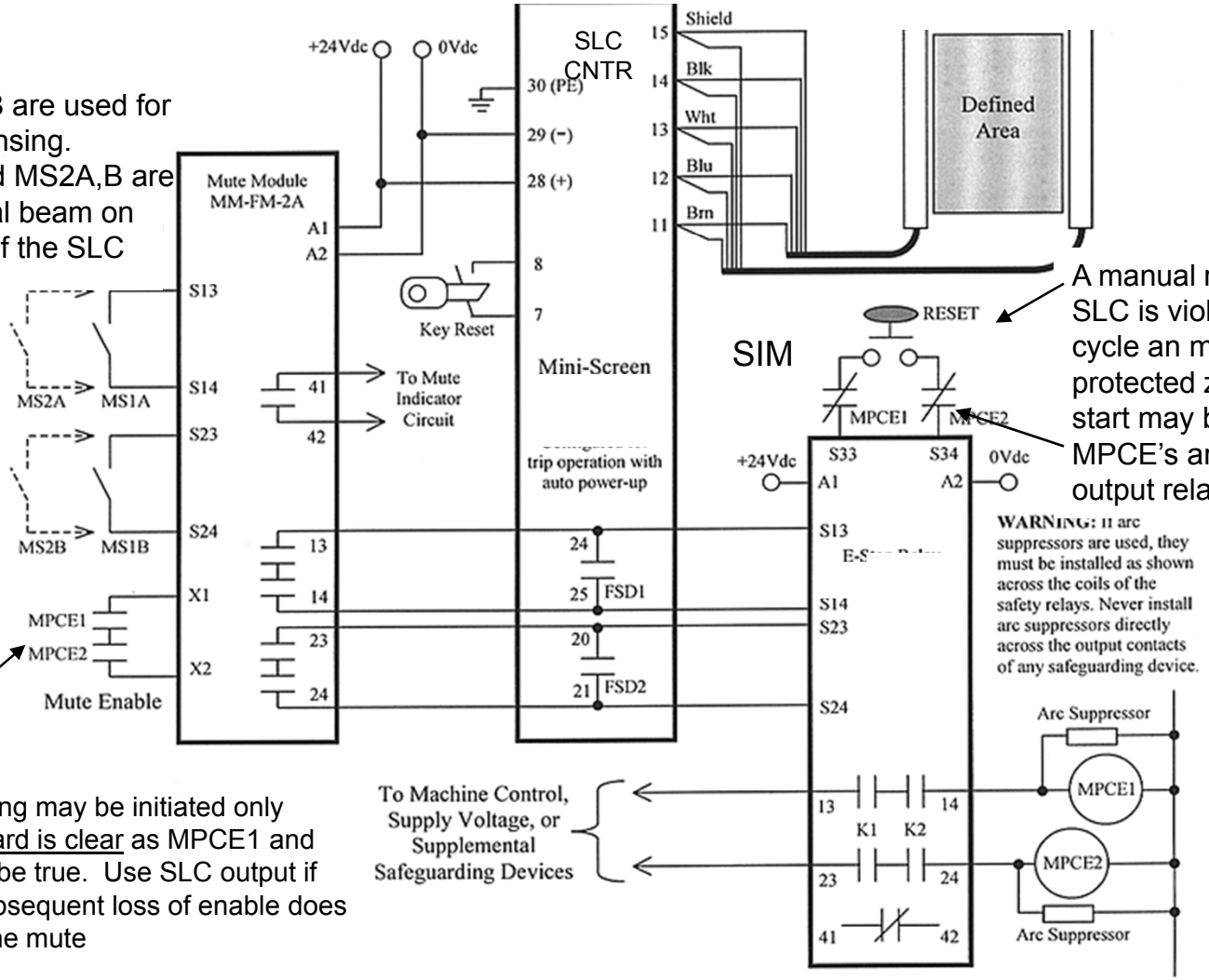
Safety Light Curtain Active Protection Zone



Clamp Tooling is always disabled by the SRL
Robot is disabled if Operator is in the SRL and the Robot is in the Danger Zone. MPCE are monitored each cycle
Robot MPCE are monitored each time there is intrusion without muting function being high
Note: the SLC is used once in its normal state for tooling safeguarding and once muted for the robot interface

Combinational Logic using Muting Module and Emergency Stop Relay

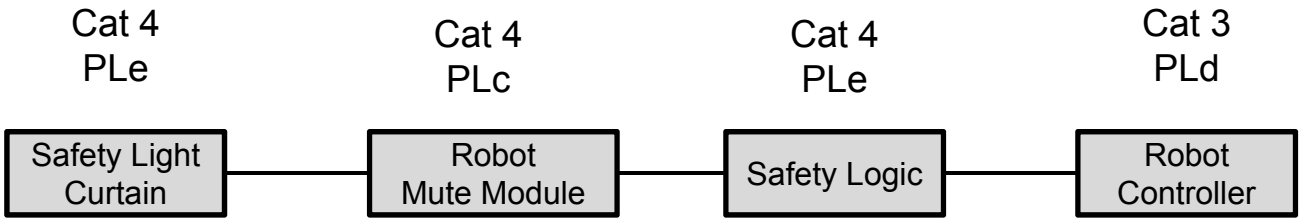
MS1A and B are used for "X" mute sensing. MS1A,B and MS2A,B are used for dual beam on either side of the SLC



A manual reset is required when the SLC is violated during a non muting cycle an manual clearing of the protected zone is required before re-start may be given.
MPCE's are monitored by the safety output relay.

Note that muting may be initiated only when the hazard is clear as MPCE1 and MPCE2 must be true. Use SLC output if available. Subsequent loss of enable does not interrupt the mute

Safety Function Block Diagram
Robot Muting



Even though the electrical connection of the Robot Muting Module is in Parallel, it is a SERIES safety function

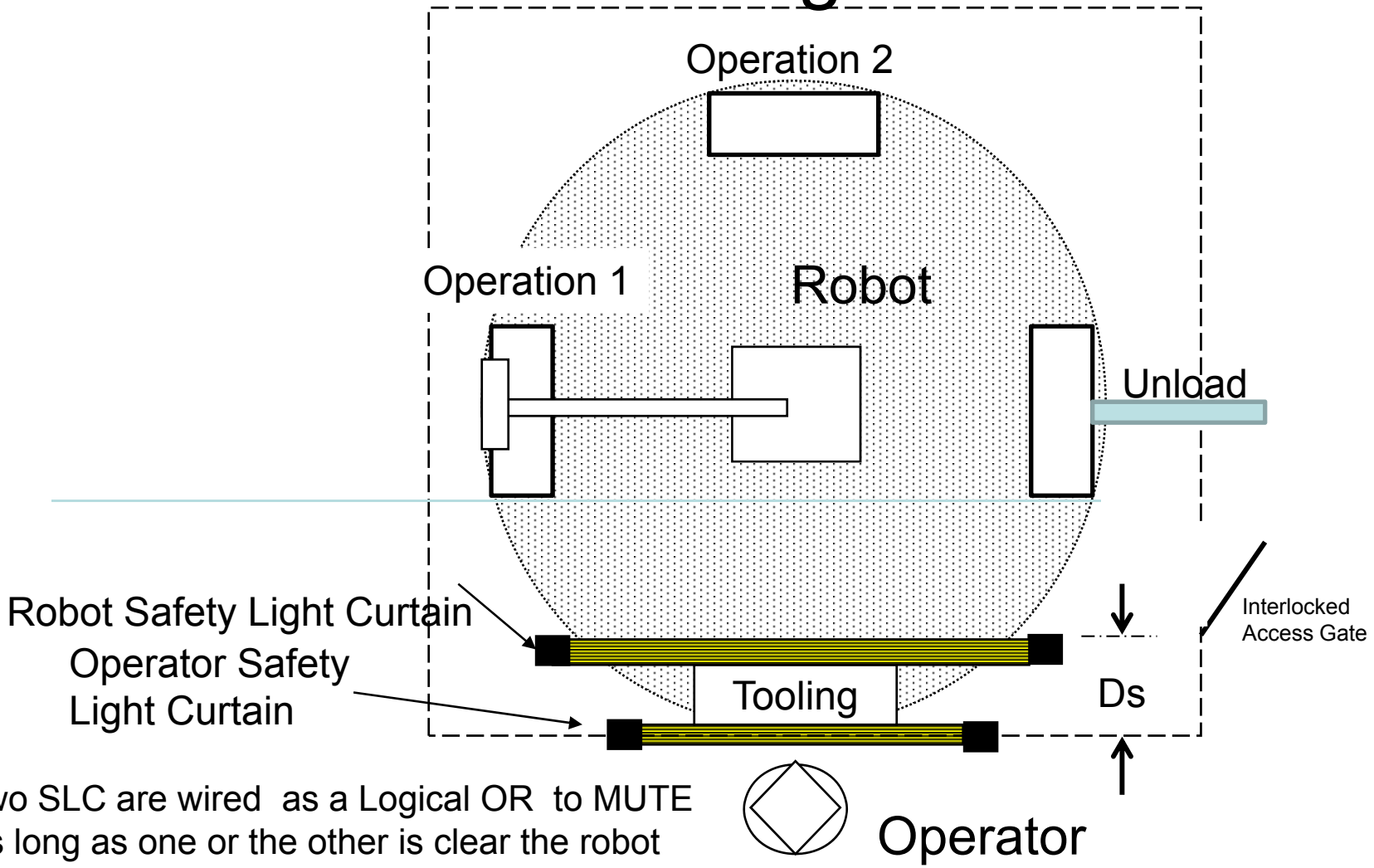
Failure to the ON state is a failure to danger

Failure to mute is NOT a failure to danger

Probability of failure and ability to detect muting input for the mute module is calculated based on its ON state failure mode.

In this example the total performance of the SRP/CS could not exceed PLc unless the muting function performance was increased to a PLd or PLe

Muting

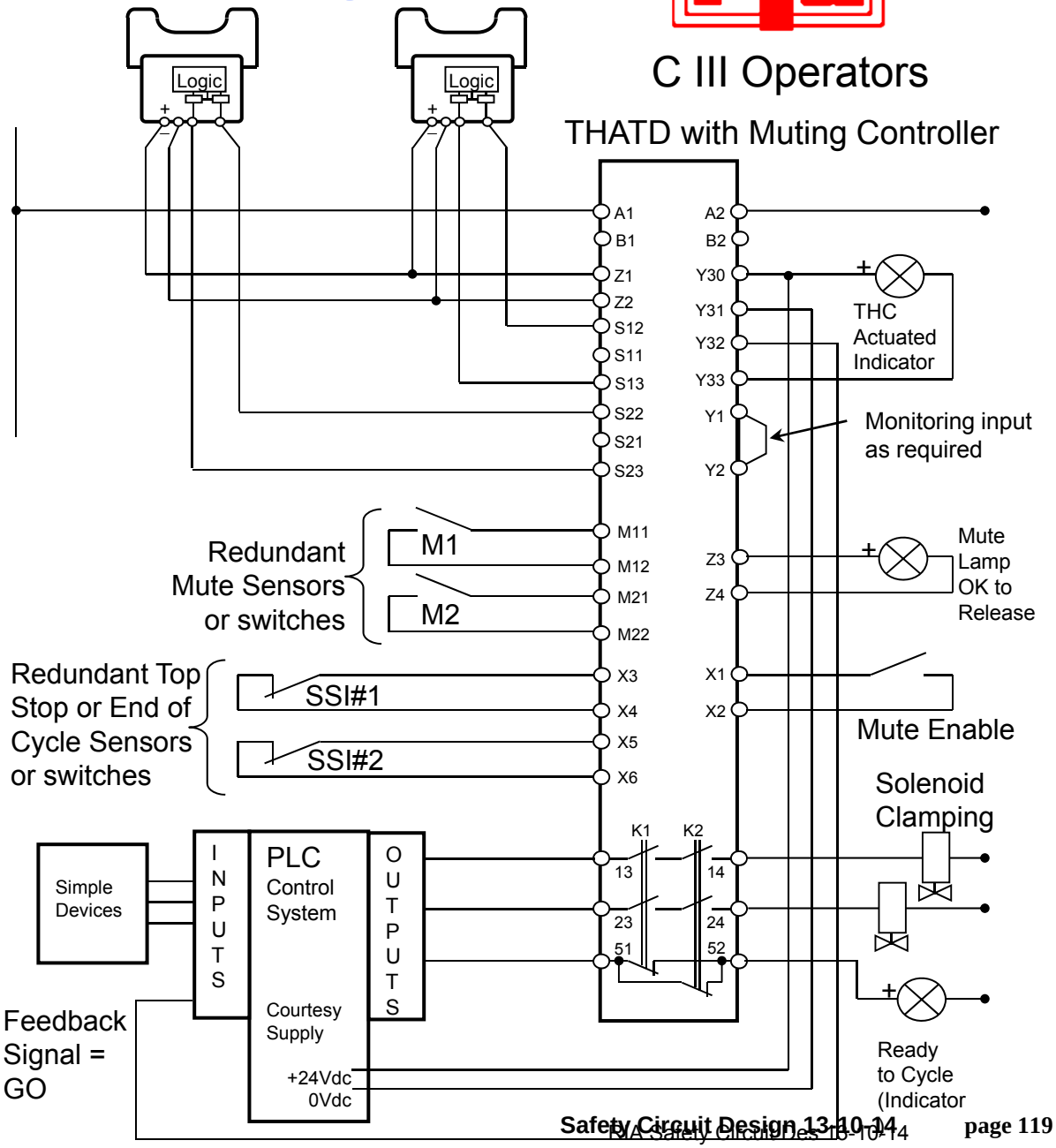


Two SLC are wired as a Logical OR to MUTE
As long as one or the other is clear the robot may operate. If both are blocked, the robot is safety stopped. The operator SLC also provides risk reduction from tool hazards

Two Hand Anti-Tie-Down w/ Dual Channel with Monitoring and Muting

Category 2, up to Cat 4 if reliable valve monitoring is added

- The muting function of the module provides control reliable circuitry to assure that a muting system failure does not produce muting of the THATD function
- Muting can be initiated only when both P.B. are operated due to module logic.
- This type of circuit is appropriate where the hazardous situation is terminated before the end of the actual cycle. This allows the operator to release the push buttons when the hazard has been eliminated but the non hazardous portion of the cycle is to continue
- Can be designed as single cycle
- Overall performance of the safety function is determined by the additional ability to monitor the valves controlling the hazard

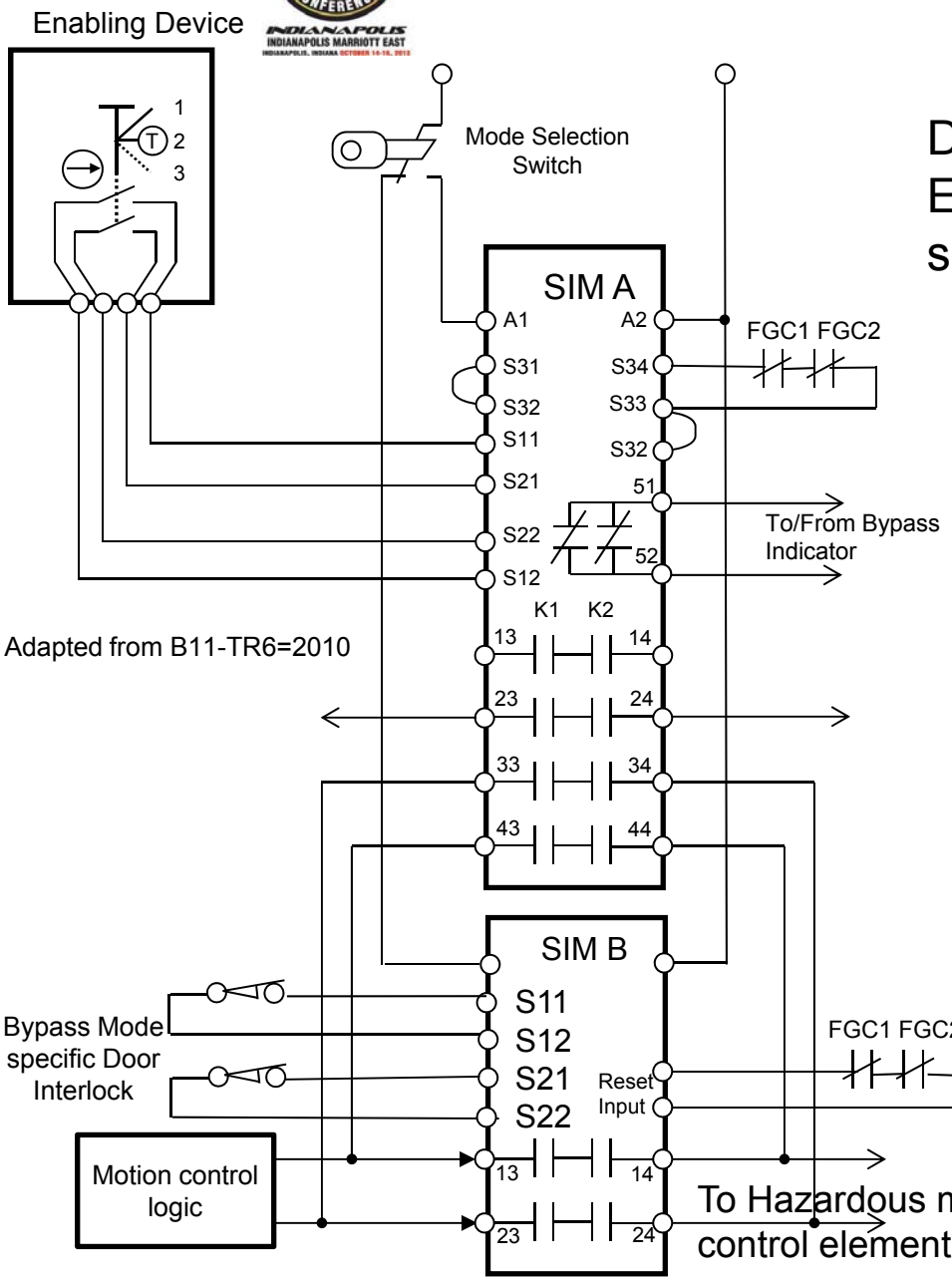


Bypassing

- The MANUALLY INITIATED suspension of the MONITORING OF THE STATE of a safety device
- The safety performance of the bypass function must be equal to or greater than that required by the safety function to be bypassed
- Failure of the bypass function to reset or its inappropriate initiation is a failure to danger of the safety function
- Is selected by a mode selector which may be supervised
- Calls other complementary safeguarding devices to activate the hazard or to reduce the risk
  - Enabling device
  - Run-to-hold control
  - Additional guarding
    - Interlocked with mode selection
  - Slow speed
    - To reduce risk by enhancing ability to avoid harm
- Other hazards, not directly associated with the manual task, must be put into a safe state
  - Ex: Robot teach mode selection with an enable operator as part of the teach pendant.

    End effector clamps are on manual operation

    The conveyor supplying or removing parts is halted



Dual Channel with Interlock Monitoring and Enabling Device Bypass of a dual channel safety device

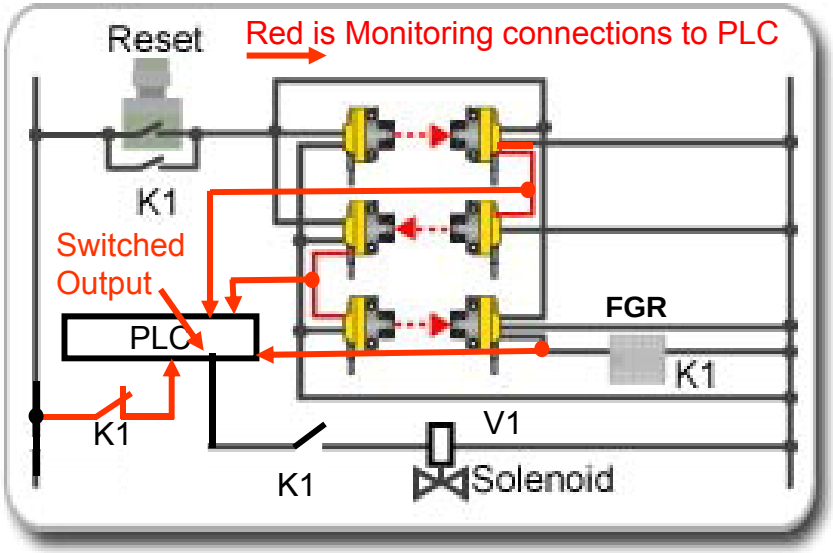
- The enabling device provides Bypassing function of the safe guarding device when the operator handle is held in the center position and the safety interface module A is enabled by the key switch

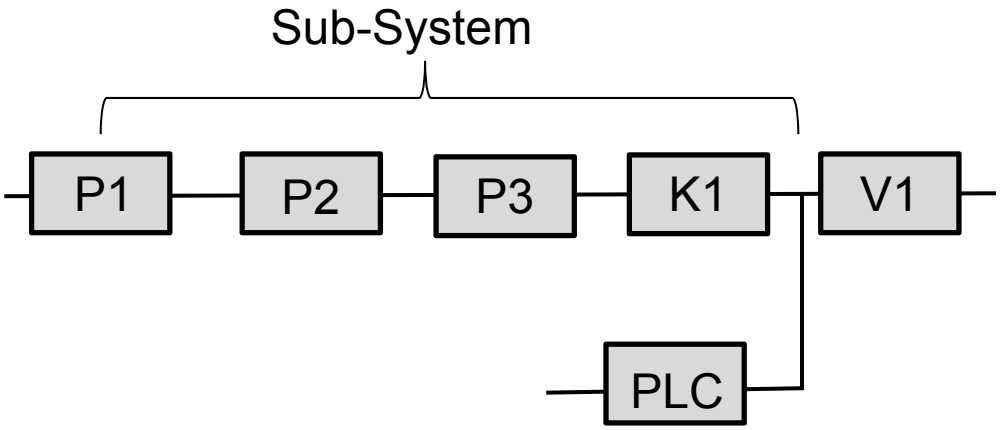
- The key lock provides two functions
  - Supervised access to the Bypass enabled function
  - By removing power form the safe guarding device B, assures that its indicators do not give false indication of the safety state of the equipment when in enabling device mode

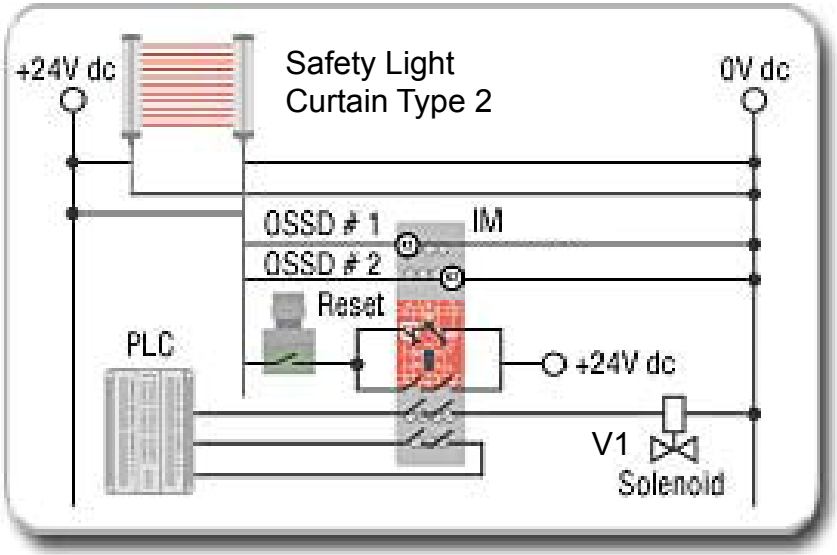
- Each safety device must be reset to activate its specific function. If so equipped, the auto reset at power up function on SIM B to be disabled

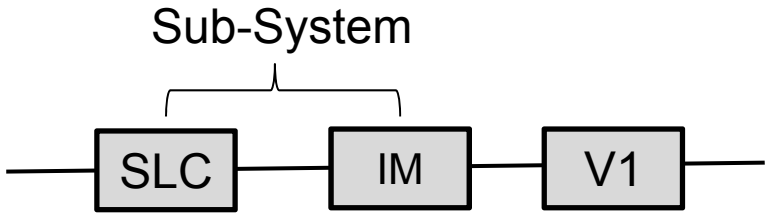
Possible up to Cat 4 with correct SIM and reliable MPCE monitoring

Note: SPR/CS performance limited by un-monitored valve

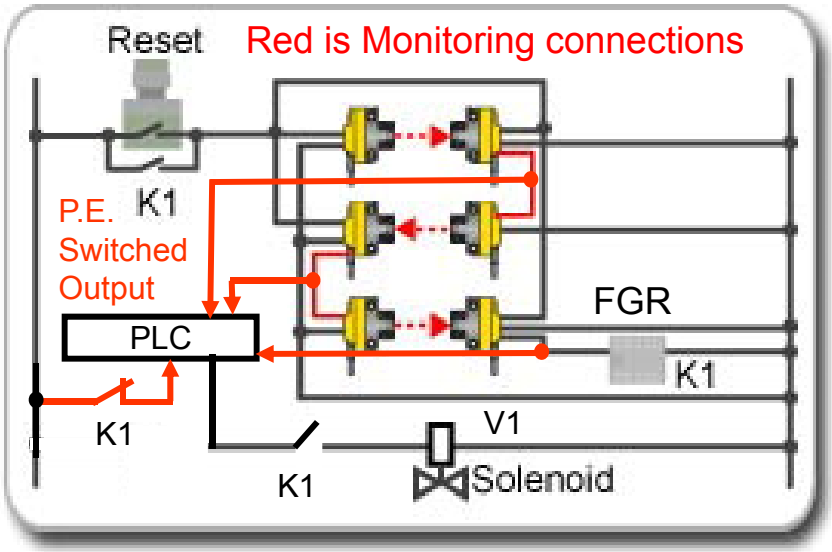


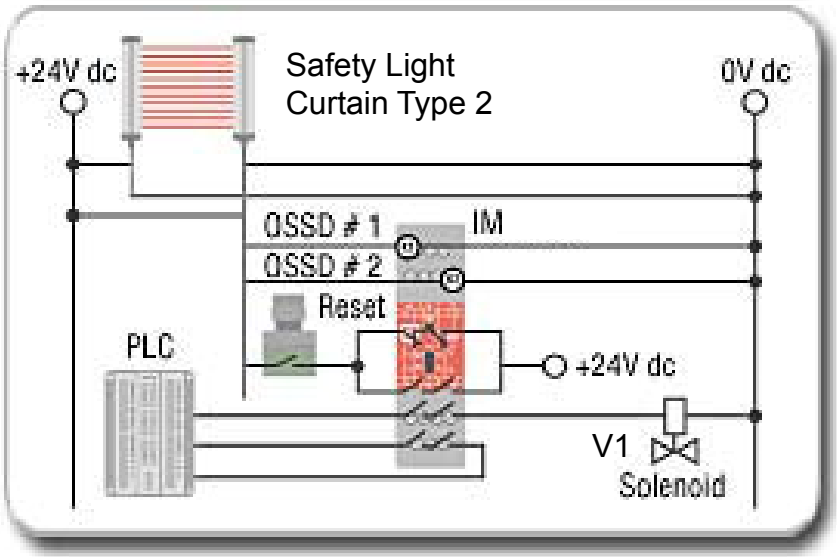






Example of the "spectrum" within a given category





- The dedicated standard PLC monitors the function of the three photoelectric sensors and the follower relay K1
- The PLC is not a Serial device in the Safety Logic Block Diagram, i.e. its failure does not result in the loss of the safety function, therefore its $MTTF_d$ is not included in the safety channel calculation
- $MTTF_d$ of the PLC is 50 years and is >1/2x the $MTTF_d$ of the system being monitored, and meets the minimum requirement for a test component for this system
- The Type 2 Safety Light Curtain is certified by a Third Party Test Laboratory to meet the required standards of Cat 2 and has a PLd
- The Interface Module is a pre-wired set of FGR, monitored by the SLC
- The solenoid valve is a Well Tried hydraulic component with a $MTTF_d$ of 150 years at this operation rate
- Both systems' performance is limited by V1 because it is not monitored
- **For a Mission Live of 20 years, the PE circuit has a 44% chance of Failure To Danger while the Type 2 has a 21%.**