ELECTRO-PNEUMATICS AND

SAFETY OF MACHINERY

NEW MACHINERY DIRECTIVE 2006/42/EC
STANDARDS EN/IEC 62061 - EN ISO 13849-1

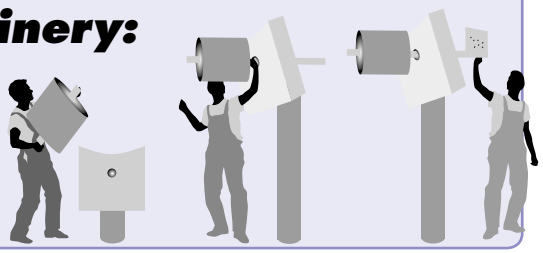
ASCO numatics™

EMERSON™
Industrial Automation

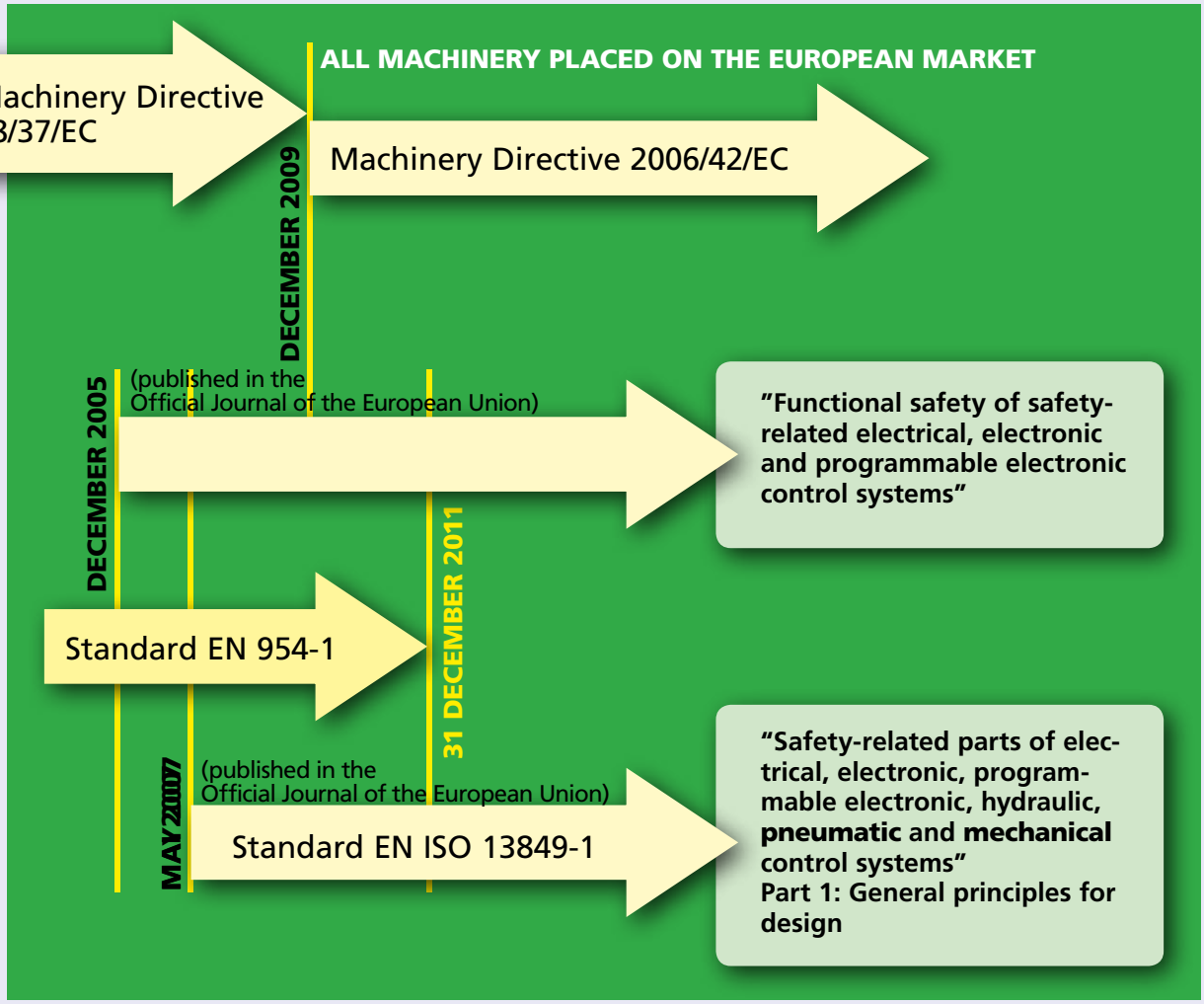
SAFETY OF MACHINERY

Principle of the safety of machinery:

To guarantee the safety and health of persons exposed to the installation, operation, adjustment and maintenance of machinery.



Development of the standards



Three key concepts for the design of machinery and their safety functions have emerged from the implementation of the new **Machinery Directive 2006/42/EC**:

- A **risk analysis** prior to design
- A particular consideration of the **quantitative aspect** of the safety functions in addition to the qualitative approach
- The use of **performance levels** (PL)

Risk evaluation:

The manufacturer or supplier of a machine must see to it that a risk evaluation is conducted to determine the health and safety requirements for persons involved in its operation. The machine must then be designed and constructed in accordance with the results of the risk evaluation.

RELIABILITY DATA

The products' reliability data (MTTF, $MTTF_d$, B_{10}, B_{10d}...) gained from reliability tests under standard conditions can be downloaded in the SISTEMA format from our website www.asconumatics.eu

Distribution function

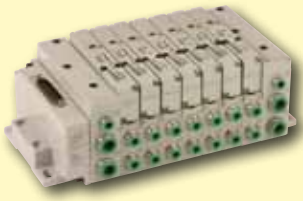
Spool valve series 551 552-553

0V1B

Stainless steel spool and sleeve valve series L1/L2

1V1A

Mini-valve series 519-520-521



Valve manifold series 2005-2012 & ISO 15407-2 26mm

0V1A
2V1

Valves to ISO 5599/1

Compact series

Pilot valve series 302-190-192

1V1B

Series 541-542-543

Pressure switch

0S1
2S1

Air preparation

Shut-off valve and slow start-up

Regulator

Fluid control solenoid valves

Actuator control

1S1

Position detector

2V3
2V2

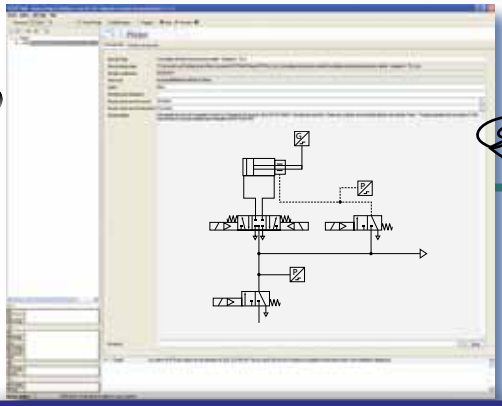
Stopper cylinder series 346 or NCPPG

Actuators (pneumatic cylinders) are not taken into consideration in the calculation of performance levels (PL). Since actuators are not an integral part of the control systems, they do not fall under EN ISO 13849-1 requirements. Manufacturers are, however, required to integrate the risks related to a failure of the actuator into their risk evaluation (EN ISO 14121 and EN ISO 12100).

Library of reliability data

ASCO numatics

Available for download at http://www.asconumatics.eu



CALCULATION → PL, SIL

SISTEMA
(Safety Integrity Software Tool for the Evaluation of Machine Applications)
SISTEMA software available for download at www.dguv.de/ifa/en

RISK EVALUATION

"Good engineering practice + probabilistic calculations"

Construction and risk evaluation of machines

EN ISO 12100
Safety of machinery
Basic concepts, general principles for design

EN 1050 (EN ISO 14121-1)
Safety of machinery
Risk assessment - Part 1: Principles

Functional and safety-relevant requirements for safety-related control systems

Functional description:

Electrical safety aspect

EN 60204-1
Safety of machinery. electrical equipment of machines - Part 1: General requirements

Design and construction of safety-related control systems for machines

EN/IEC 62061

Risk related to the hazardous event = Severity of damage S

Effects	Severity S	Class K = F + O + P				
		3-4	5-7	8-10	11-13	14-15
Death, loss of eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, loss of fingers	3			SIL 1	SIL 2	SIL 3
Reversible, medical treatment	2	Other measures			SIL 1	SIL 2
Reversible, first aid	1					SIL 1

Safety integrity levels SIL 1, 2, 3

Any architecture

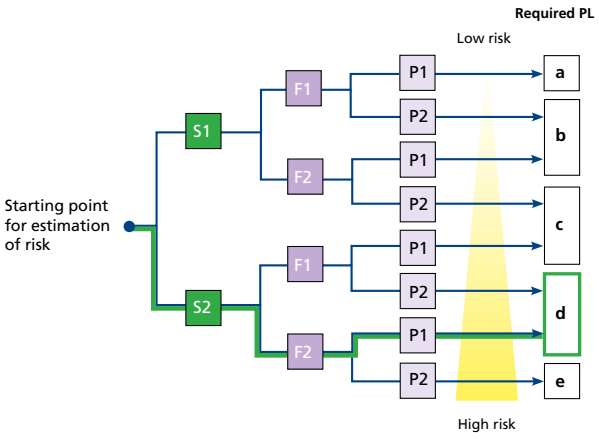
A → Series arrangement w/o diagnostic function
B → Parallel arrangement w/o diagnostic function
C → Series arrangement with diagnostic function
D → Parallel arrangement with diagnostic function

EN ISO 13849-1

et

- Frequency and/or duration of exposure F
- Probability of occurrence O
- Probability of avoidance P

→ Probability of damage



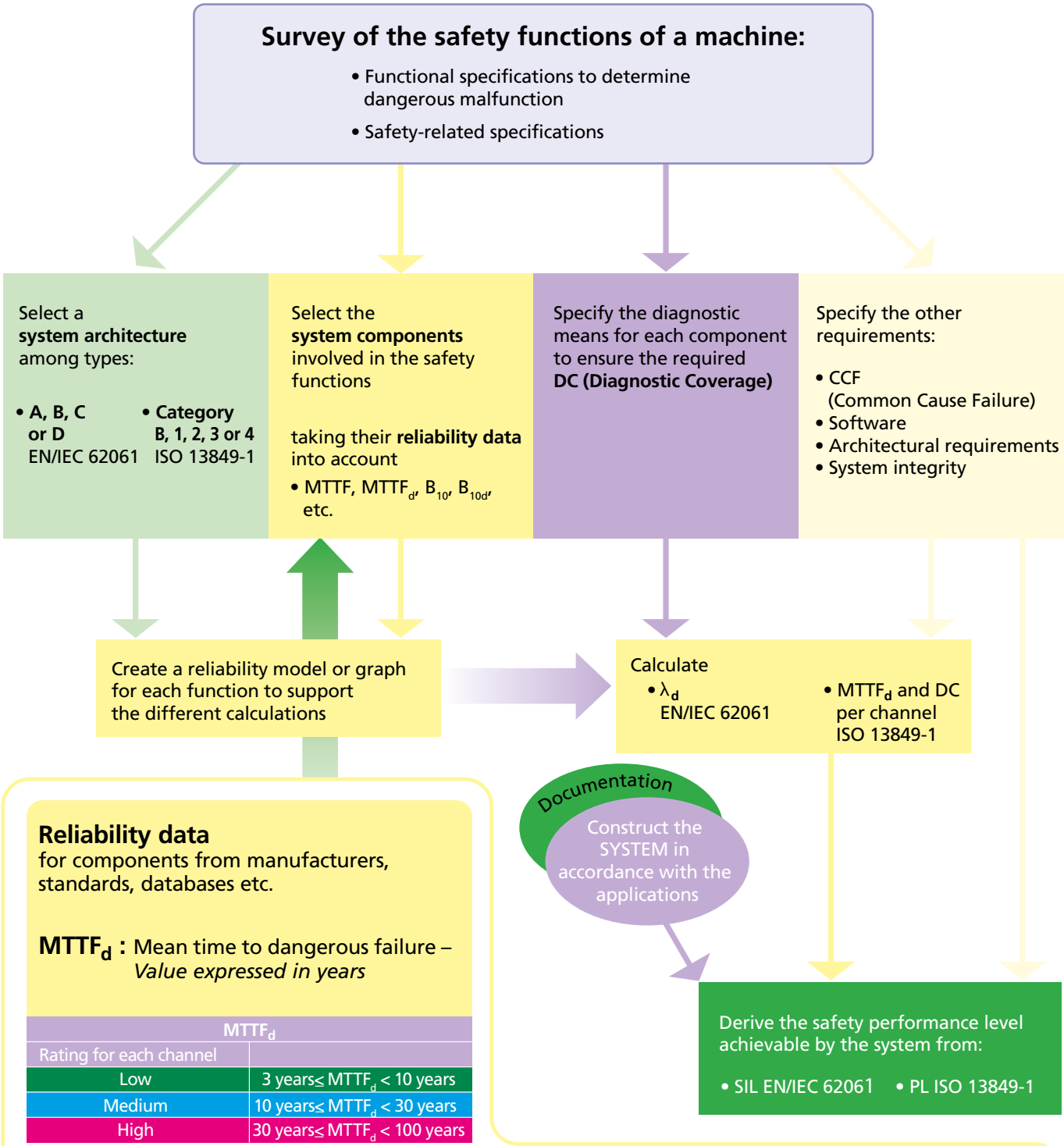
Performance levels PL a, b, c, d, e

Designated architecture (categories)

B, 1, → Series arrangement w/o diagnostic function
2 → Series arrangement with diagnostic function
3, 4 → Parallel arrangement with diagnostic function

DESIGN PROCESS

EN/IEC 62061 - EN ISO 13849-1



B_{10d} : Number of cycles after which 10 % of a random sample of wearing components fail dangerously – *Value expressed in number of cycles.*

DC : Diagnostic Coverage

Diagnostic coverage			
None	Low	Medium	High
DC < 60%	60% ≤ DC < 90%	90% ≤ DC < 99%	99% ≤ DC

CCF : Common Cause Failure. Measures to be taken to prevent a given cause (and its effect) from concurrently disabling the multiple channels of a safety circuit.

Mission time T_{10} : In line with "good engineering practice" as recommended in EN ISO 13849-1, components attaining this value must be replaced (precautionary principle).

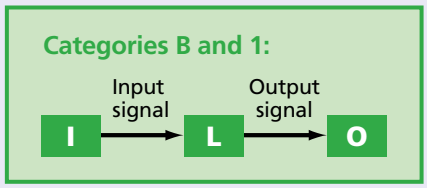
Only the pneumatic part is described in the form of a subsystem in these examples. Other safety-related components (e.g. protective devices, electrical logic elements) must be added to ensure the safety function is complete.

The examples shown here only relate to the stopping of hazardous movements. In pneumatics, safety measures concerning the interruption of energy sources, the evacuation of potential energy (pressure contained in a part of the circuit), and a "progressive" start-up after an unexpected shutdown should not be omitted.

To attain a PL = c, category 1 architecture

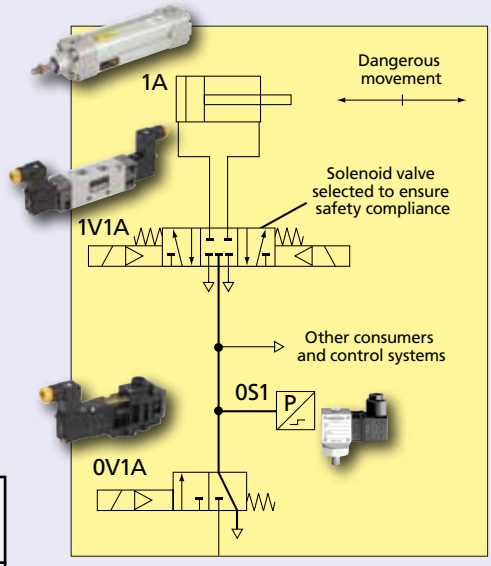
- **Safety function:** Stopping of the potentially hazardous movement of cylinder 1A.

- **Functional description:**



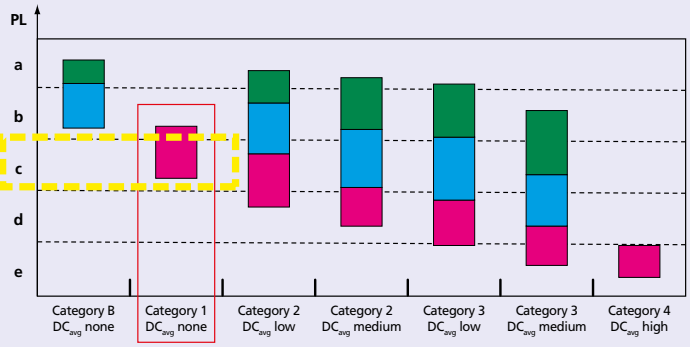
Input 'I': not represented, movable guard or light barrier, etc.

Logic element 'L': not represented, PLC



- **Calculation of the probability of dangerous failure:**

Safety function	Working hours / day	Working days / year	Cycles / year
1 cycle = 5 s	16h	240 days	2 764 800 cycles



B_{10d} (1V1A – series 520) = 130 000 000 cycles, i.e. an operating time of 47 years, $MTTF_d$=470 years "high"

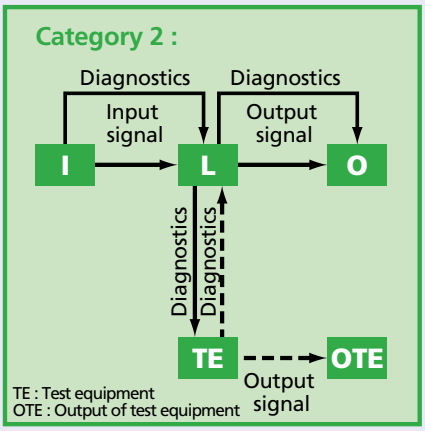
PL Performance levels
- $MTTF_d$ rating for each channel = low
- $MTTF_d$ rating for each channel = medium
- $MTTF_d$ rating for each channel = high

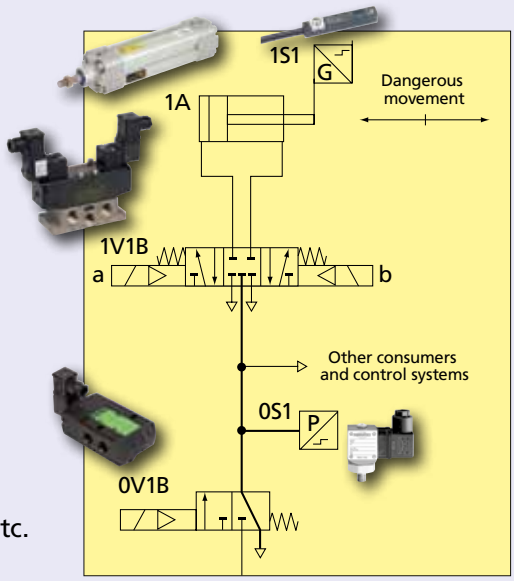
By limiting the valve's operating time to 47 years, this corresponds to a PL = c

To attain a PL = c, category 2 architecture

- **Safety function:** Stopping of the potentially hazardous movement of cylinder 1A.

- **Functional description:**





Input 'I': not represented, movable guard or light barrier, etc.

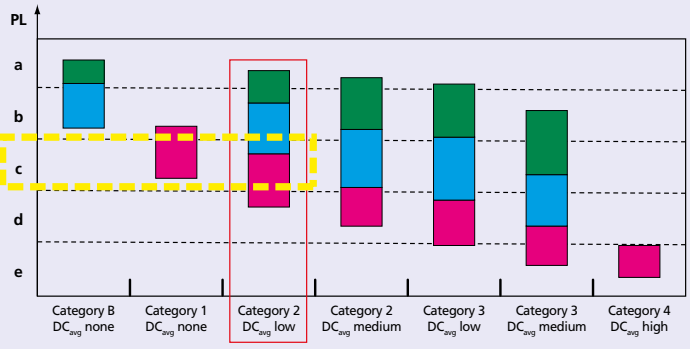
Logic element 'L': not represented, PLC

Stop of cylinder ensured by:	Diagnostics ensured by:
Output O: Valve 1V1B	Cross-monitoring in L1 of the supply status coherence of coils 1V1Ba and 1V1Bb and the limit switches 1S1

0V1: Energy isolating valve: ensures the system is exhausted in case of loop failure.

- **Calculation of the probability of dangerous failure:**

Safety function	Working hours / day	Working days / year	Cycles / year
1 cycle = 5 s	16h	240 days	2 764 800 cycles



B_{10d} (valve 1V1B - series 542) = 44 912 670 cycles, i.e. an operating time of 16.2 ans,
$MTTF_d$ = 162 years "high"

$MTTF_d$ (sensors 1S1) = 45 000 000 h, i.e. 11 718 years "high"

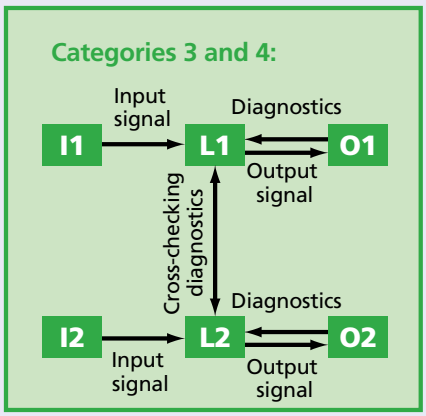
The case study shows:
DC (Diagnostic Coverage) = 60% "low".

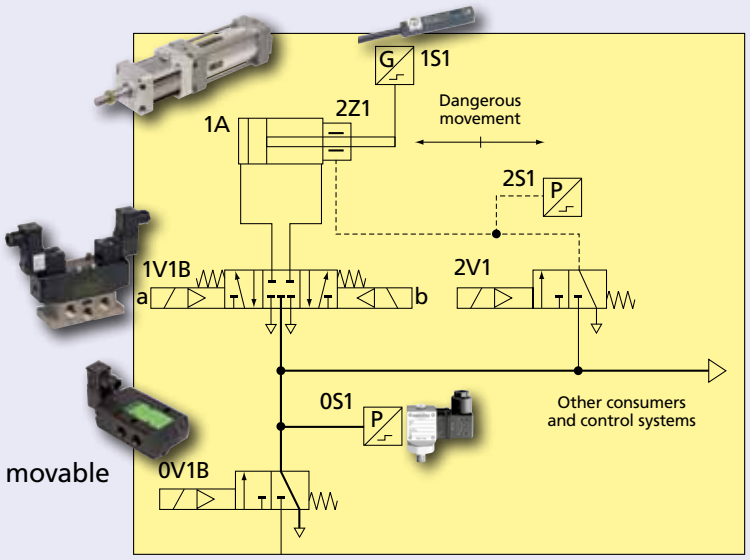
PL Performance levels
- $MTTF_d$ rating for each channel = low
- $MTTF_d$ rating for each channel = medium
- $MTTF_d$ rating for each channel = high

By limiting the valve's operating time to 16.2 years, this corresponds to a PL=c for the safety loop.

To attain a PL = d, category 3 architecture

- **Safety function:** Stopping of the potentially hazardous movement of cylinder 1A.
- **Functional description:**





Inputs 'I1' and 'I2': not represented, movable guard or light barrier, etc.
Logic elements 'L1' and 'L2': not represented, PLC

Stop of cylinder ensured by:		
Output O1: Valve 1V1B	Comparison in L1 of the supply status of coils 1V1Ba and 1V1Bb and the limit switches 1S1	Cross-monitoring of L1/L2 status coherence within the PLC
Output O2: Valve 2V1 controlling the rod lock 2Z1	Pressure switch 2S1 for transmission of signal to L2	

0V1B: Energy isolating valve: ensures the system is exhausted

- **Calculation of the probability of dangerous failure:**

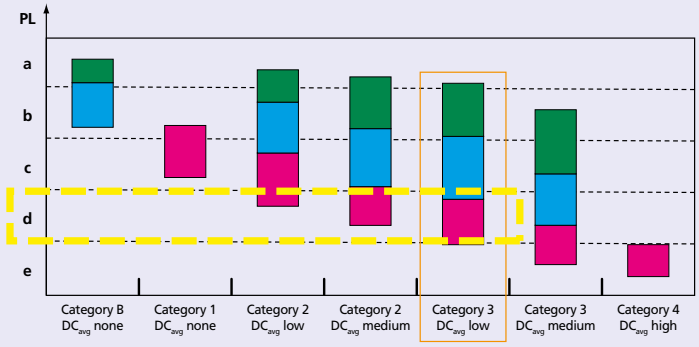
Safety function	Working hours / day	Working days / year	Cycles / year
1 cycle = 10 s	16h	240 days	1 382 400 cycles

B_{10d} (valve 1V1B - series 542) = 44 912 670 cycles, i.e. an operating time of 32.4 years, MTTFd = 324 years "high"

B_{10d} (valve 2V1 - series 520) = 20 000 000 cycles, i.e. an operating time of 14.5 years, $MTTF_d$ = 145 years "high"

B_{10d} (pressure switch 2S1, dynamic rod lock 2Z1) = 4 000 000 cycles, i.e. a mission time of T10 = 2.89 years, MTTFd = 28.9 years "medium"

$MTTF_d$ (sensors 1S1) = 45 000 000 h, i.e. 11 718 years "high"



By limiting the operating time of the pressure switch and rod lock to 2.89 years, this corresponds to a PL = d for the safety loop

The case study shows:

DC (1V1B) = 60% "low",
DC (2V1) = 99% "high", DC* (2Z1) = 75%

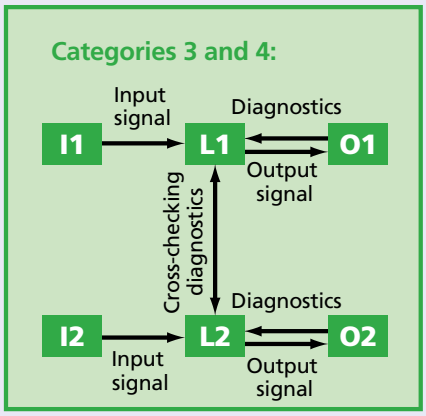
i.e. for channel O2, DC = 78% "low".

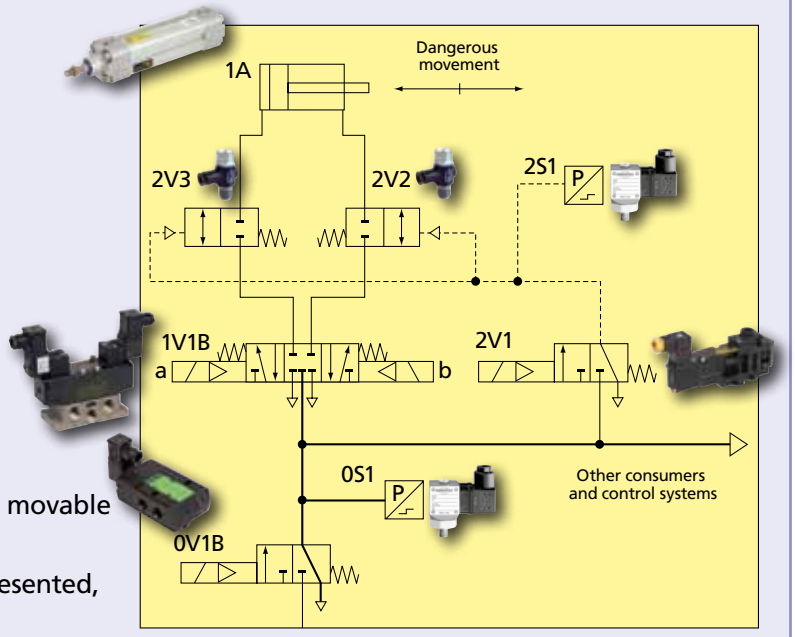
PL Performance levels
- $MTTF_d$ rating for each channel = low
- $MTTF_d$ rating for each channel = medium
- $MTTF_d$ rating for each channel = high

** "Good engineering practice" methods associate this type of component with a low-to-medium DC to cover any of the component's drift failures.*

To attain a PL = d, category 3 architecture

- **Safety function:** Stopping of the potentially hazardous movement of cylinder 1A.
- **Functional description:**





Inputs 'I1' and 'I2': not represented, movable guard or light barrier, etc.

Logic elements 'L1' and 'L2': not represented, PLC

Stop of cylinder ensured by:	Diagnostics ensured by:	
Output O1: Valve 1V1B	Comparison in L1 of the supply status of coils 1V1Ba and 1V1Bb and the limit switches 1S1	Cross-monitoring of L1/L2 status coherence within the PLC
Output O2: Valve 2V1 controlling the two 2/2 "cylinder stop" valves used as braking units	Pressure switch 2S1 for transmission of signal to L2	

0V1B: Energy isolating valve: ensures the system is exhausted.

- **Calculation of the probability of dangerous failure:**

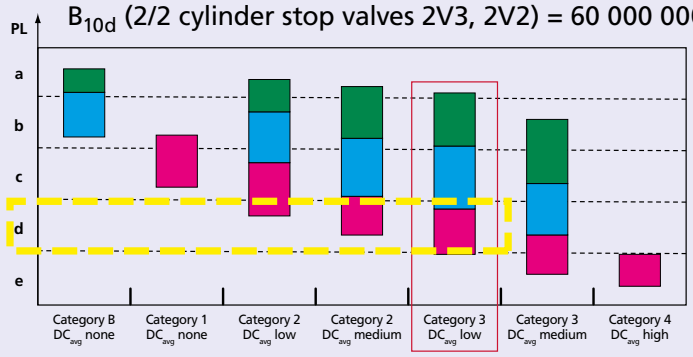
Safety function	Working hours / day	Working days / year	Cycles / year
1 cycle = 10 s	16h	240 days	1 382 400 cycles

B_{10d} (valve 1V1B - series 542) = 44 912 670 cycles, i.e. an operating time of 32.4 years, MTTFd = 324 years "high"

B_{10d} (valve 2V1 - series 520) = 20 000 000 cycles, i.e. an operating time of 14.5 years, $MTTF_d$ = 145 years "high"

B_{10d} (pressure switch 2S1) = 4 000 000 cycles, i.e. a mission time of T10 = 2.89 years, MTTFd = 28.9 years "medium"

B_{10d} (2/2 cylinder stop valves 2V3, 2V2) = 60 000 000 cycles, i.e. $MTTF_d$ = 434 years "high"



By limiting the operating time of the pressure switch to 2.89 years, this corresponds to a PL = d for the safety loop.

The case study shows:

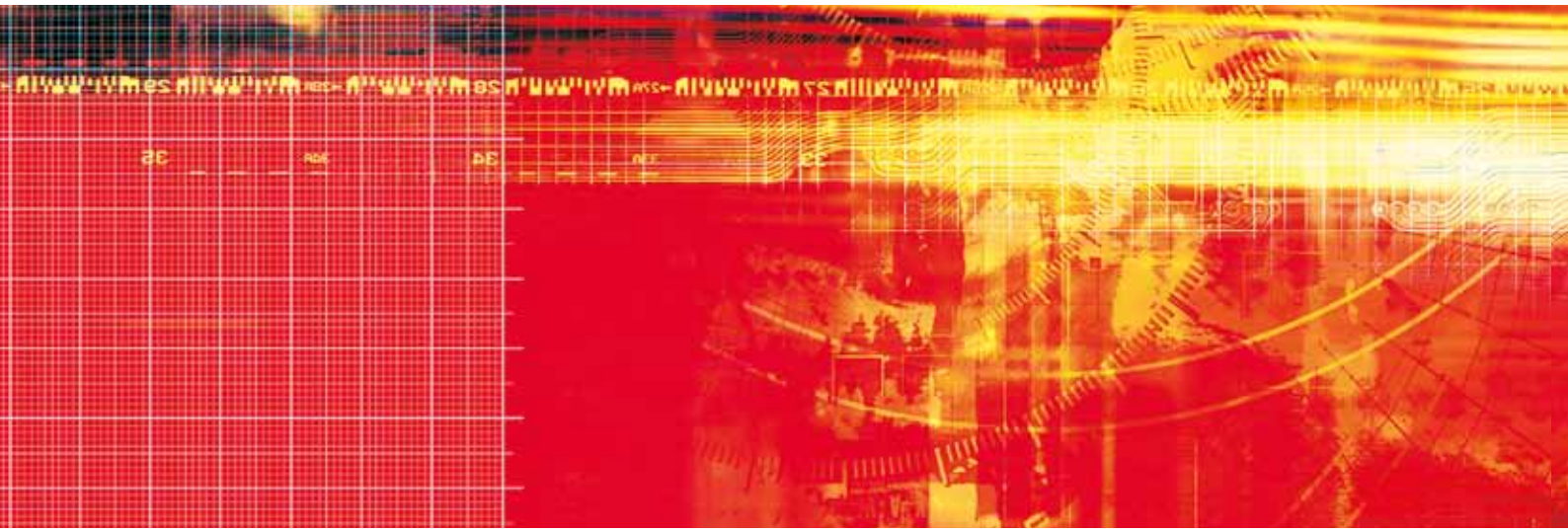
DC (1V1B)=60% "low",
DC (2V1)=99% "high", DC* (2V3, 2V2)=60%

i.e. for channel O2, DC = 78% "low".

PL Performance levels

- $MTTF_d$ rating for each channel = low
- $MTTF_d$ rating for each channel = medium
- $MTTF_d$ rating for each channel = high

** "Good engineering practice" methods associate this type of component with a low-to-medium DC to cover any of the component's drift failures.*



ASCO numatics™

www.asconumatics.eu

383 73 30 . 1M0911