

**SMC – meeting tomorrow's  
machine safety standards today**



## SMC – meeting tomorrow's machine safety standards today

**As leading experts in pneumatics and specialists in factory automation, the development of high quality, innovative products which offer excellent performance and provide maximum operator safety has always been at the front of our minds.**

This simple premise has helped SMC grow into the global organization it is today, with over 15.300 employees and sales offices in 78 countries around the world.

With the rapid advances in manufacturing and machine technology, safety in engineering is becoming increasingly important and the protection of people working in close proximity to both machines and systems is of paramount importance.

With the introduction of the new Machinery Directive 2006/42/EC, which came into force from the end of December 2009, mechanical engineers in Europe and throughout the world, will have to consider new harmonised standards and their subsequent requirements when designing and developing safe machines.





### **A change in the standards:**

The Machinery Directive (MD) 2006/42/EC defines the safety requirements which a machine must meet in order for it to be sold and used in Europe.

EN ISO 13849-1 and EN 62061 are standards which relate specifically to operational safety. The official Journal of the EU defines which standards are harmonised and give a presumption of conformity with the MD.

### **An overview:**

#### **Machinery Directive (MD) 2006/42/EC**

Replacing the existing 98/37/EC Machinery Directive, the new MD 2006/42/EC is universally applicable for machinery, safety components, partly completed machinery and other specific equipment.

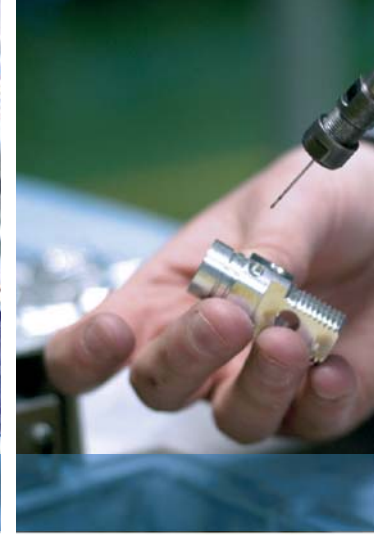
The manufacturer of machinery has to meet the safety requirements of the MD and confirm this by attaching a CE mark to the machine.

#### **EN ISO 13849-1 and EN 62061**

**EN ISO 13849-1:** provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems including the design of software. For safety-related parts of control systems, it specifies characteristics that include the performance level required for carrying out safety functions.

It applies to safety-related parts of control systems regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.), for all kinds of machinery.

**EN ISO 62061:** specifically addresses the operational safety of safety-related electrical, electronic and programmable electronic control systems.

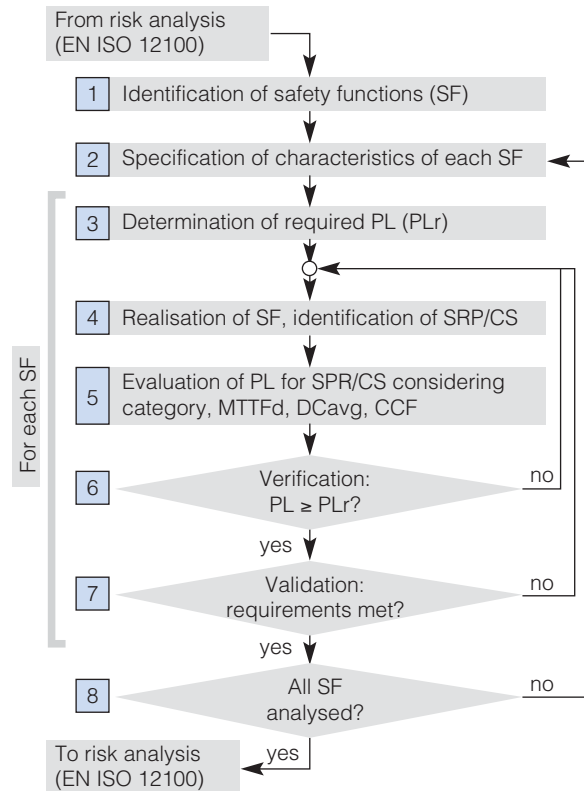


## How does it affect you?

Under EN ISO 13849-1, the consideration of safety starts with the risks associated with the machine, its function and its operation. Machine designers are obliged to eliminate risks before considering further measures to reduce or control risks (EN ISO 12100).

The risks of the machine must be quantified by the machine designer and if the risks are considered high, the designer is obliged to employ systems that reduce the risks to acceptable levels. Once the risks have been reduced to acceptable levels by means of an inherent safe design, then protective devices will be required. At that point, safety functions (SF) must be defined and satisfied by the machine design.

EN ISO13849-1 uses an interactive process for the design of the safety-related parts of control systems, as follows:



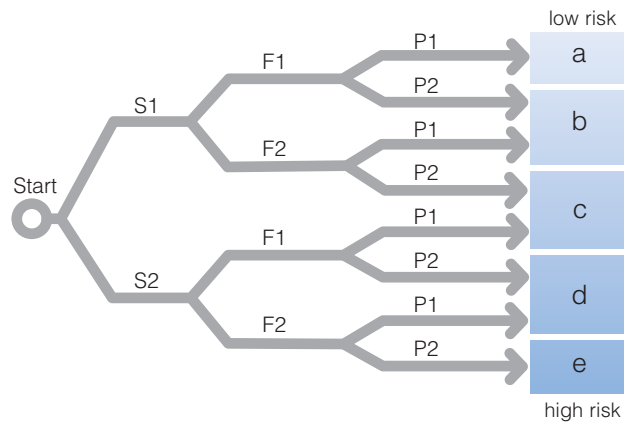
Iterative process for design of the safety-related parts of control systems; SF = safety function; PL = performance level; PLr = required performance level; SRP/CS = safety-related parts of control systems; MTTFd = mean time of dangerous failure; DCavg = average diagnostic coverage; CCF = common cause failure

- A required **performance level “PLr”** (target value) must be specified for each intended safety function
- The safety function requirements are derived from the necessary risk reduction
- ISO 14121-2 describes methods for determining the necessary level of risk reduction
- EN ISO 13849-1 employs one of these methods where the following parameters are evaluated: S – Severity of injury, F – Frequency and time of exposure to the hazard and P – Possibility of avoiding the hazard or limiting the harm.



There are five performance levels: **a, b, c, d, e**, with “a” being low risk and “e” representing the highest risk.

Each of these five performance levels corresponds to a further parameter scale, based on the probability of a dangerous failure per hour.



Once the safety function (SF) and the required risk reduction PLr have been defined, the actual design of the SRP/CS can begin - as suitable protective measures have to be used to match the performance levels.

The following elements define the performance level or PL:

1. The architecture categories of the safety system
2. The reliability of the safety system (MTTFd)
3. How easily faults can be detected (DCavg)
4. How vulnerable the system is to failure (CCF)

Once the design of the safety control systems has been completed and the PLs have been determined, a verification and validation process should be completed in accordance with EN ISO13849-2.

Severity:	PL defined statistically
S1 slight,	Average probability of dangerous failures per hour, h <sup>-1</sup>
S2 serious	
Exposure frequency:	
F1 not often,	a
F2 frequent	b
Avoidance possibility:	c
P1 possible,	d
P2 scarcely possible	e

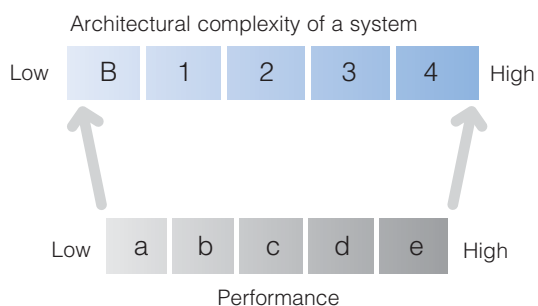


## Architecture categories of the safety system

The architecture categories help to classify the safety-related parts of a control system (SRP/CS) in relation to their resistance to faults and their subsequent behavior in the fault condition, based upon the reliability and/or the structural arrangement of the parts.

For defining the probability of failure and the PL, the architecture categories provide the major definition, completed by the component reliability (MTTFd), the diagnostic coverage (DCavg), and the resistance to common cause failures (CCF) information.

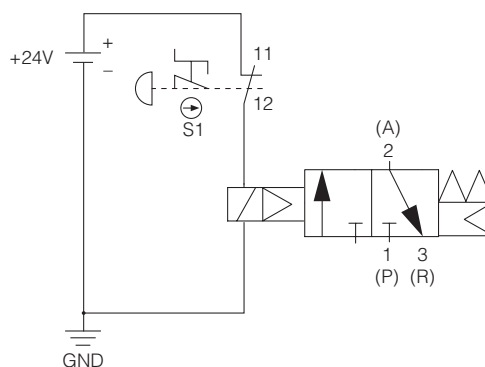
There are five Architecture categories: B, 1, 2, 3, 4.



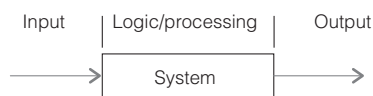
### Architecture categories - B and 1

In categories B and 1, the resistance to faults is achieved primarily by the selection and use of suitable components. Category 1 has a greater resistance than category B because of the use of special components and principles which are considered well-ried and tested in a safety context.

A typical application:



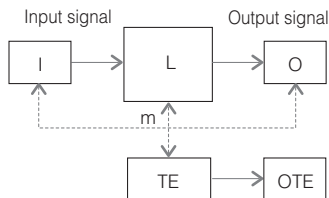
The simple system to remove supply pressure possibly suitable for low risk application which is PL 'a'



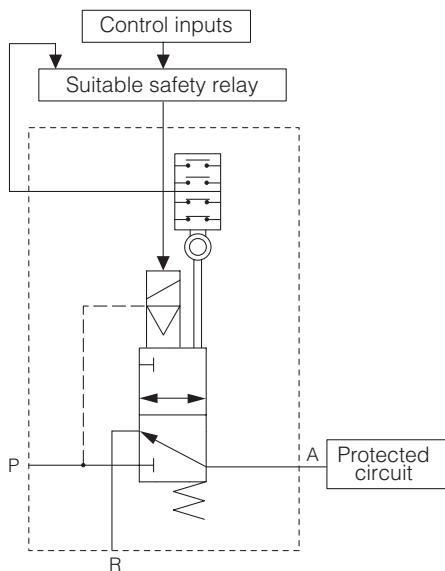


### Architecture - category 2

Category 2 combines all of the requirements of architecture B & 1, plus the system/s are checked for faults affecting the safety function. These checks are made at regular intervals, e.g. at start-up, or before the next demand on the safety function. By using an appropriate selection of test intervals, a suitable risk reduction can be attained.



System for use with SMC Products:



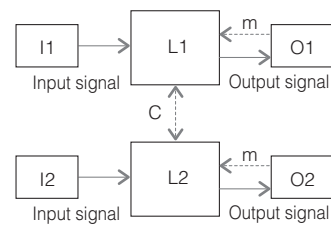
SMC special product: - in this example the product is our series: VG342-□-X91

### Architecture categories - 3 and 4

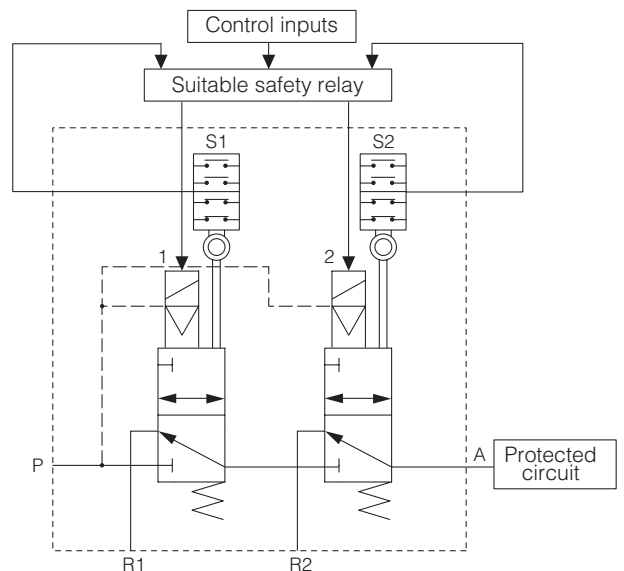
In categories 3 and 4, the occurrence of a single fault does not result in the loss of the safety function.

In category 4, and whenever reasonably practical in category 3, such faults are detected automatically.

In category 4, if single fault detection is not possible, accumulation of faults will not lead to a loss of the safety function.



System for use with SMC Products



SMC special product - in this example the product being tested is our series VG342-□-X87/X89 (including soft-start valve)



## The reliability of a safety system

The reliability of a system has to be quantified as part of the Performance level (PL).

Reliability is expressed as the Mean Time to Dangerous Failure (MTTFd) which is measured in hours. The MTTFd should be determined from the component manufacturer's data.

However, as this is application-specific, the components MTTFd cannot be quoted in isolation as the manufacturer is not aware of the exact machine application.

**As the world leading experts in pneumatics we will provide estimated MTTF or B10 values, to help support our customers. However, we (SMC) will not accept liability for the use of these components in safety systems beyond our normal warranty terms.**

MTTF or B10 are defined respectively as mean time to failure or number of cycles until 10% of the components has exceeded fixed limits under defined conditions, such as response time, leakage, or switching pressure.

### Finding the MTTFd-Value of a pneumatic component with B10-Value according to EN ISO 13849-1

Input parameter:

- B10: Number of cycles, until 10% of the components fails
- hOP: Mean operation [hours/day]
- dOP: Mean operation [days/year]
- TCycle: Mean time between the beginning of two successive cycles of the component [s/cycle]

Output parameter:

- nOP: Mean number of annual operations
- B10d: Number of cycles, until 10% of the components fails dangerously
- MTTFd: Mean time to dangerous failure

Typical procedure (in certain circumstances):

$$B_{10d} = 2 \times B_{10}$$

$$nOP = \frac{dOP \times hOP \times 3600[s/h]}{TCycle}$$

$$MTTFd = \frac{B_{10d}}{0.1 \times nOP}$$





### Finding the MTTFd-Values of a component which combines both electronic and pneumatic parts

The dependency of the probability of failure related to time (electronic) as well as cycles (pneumatic component) is an indication of such a combined system (combined fluid and electric systems).

The total MTTFd-value of the combined system will be determined from the B10d value of the pneumatic component and the MTTFd-value of the electronic components.

### DC (Diagnostic Coverage)

A factor called **DC (Diagnostic Coverage)** is a measure of how effectively failures can be detected by monitoring systems.

Sensors can be used to detect faults when monitored by a logic / processing device.

EN ISO 13849-1 provides the means of estimating **DC** which is then used as part of the determination of **PL**.

Diagnostic Coverage is defined as the measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures; so 0% ~ no dangerous faults are detected and approaching 100% ~most faults detected (but =100% is impossible because diagnostics are not considered to be completely reliable).

Diagnostic coverage categories:

Category	Range
None	DC < 60%
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

Diagnostic coverage estimated:

Measure	Diagnostic coverage
Monitoring of outputs by one channel without dynamic test.	0% to 99% depending on how often a signal change is done by the application.
Cross monitoring of outputs without dynamic test.	0% to 99% depending on how often a signal change is done by the application.
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90%
Cross monitoring of output signals and intermediate results within the logic and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99%
Redundant shut-off path with no monitoring of the actuator	0%
Redundant shut-off with monitoring of one of the actuators either by logic or by test equipment	90%
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99%
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90% to 99%, depending on the application
Fault detection by the process	0% to 99%, depending on the application; this measure alone is not sufficient for the required performance level 'e'
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99%



## Common Cause Failure (CCF)

It is necessary to consider how single failures might affect safety systems when there is redundancy in the system. A redundancy can be compromised if both channels fail simultaneously due to the same cause. This factor is called **CCF (Common Cause Failure)**.

EN ISO 13849-1 provides a score for **CCF**, which is used to determine the Performance level **PL**.

For this score, EN ISO13849-1 defines a checklist of eight important countermeasures, which are evaluated as follows:

- Physical separation between the signal paths of different channels (15 points)
- Diversity in the technology, the design or the physical principles of the channels (20 points)
- Protection against possible overloading (15 points) and the use of well-tried components (5 points)
- Failure mode and effects analysis during development for the identification of potential common cause failures (5 points)
- Training of designer/maintainers in CCF and its avoidance (5 points)
- Protection against common cause failures triggered by contamination (mechanical and fluidic system) and electromagnetic interference (electrical system) (25 points)
- Protection about common cause failures triggered by unfavorable environmental conditions (10 points)

A maximum score of 100 points can be obtained, but even for categories 2, 3 and 4, EN ISO13849-1 requires only a minimum total of 65 points.

Note: CCF is always system-dependent and application-specific. The system integrator will need data from the manufacturers of the component parts.

After these four essential quantitative parameters have been determined, EN ISO 13849-1 proposes a simple graphical method for determining the achieved PL for the SRP/CS.

The combination of requirements to achieve PL

		Category						
PL	B	1	2		3		4	
a	MTTFd Low		MTTFd Low		MTTFd Low			
b	Med	MTTFd	MTTFd Med	Low	MTTFd Med	Low	MTTFd	
c		High	High Med	Low	High Med	Med	Low	
d				High Med	High Med	High Med	MTTFd	
e						High	High	
DCavg =		None	None	Low	Med	Low	Med	High
CCF =		Not relevant		65% or better				

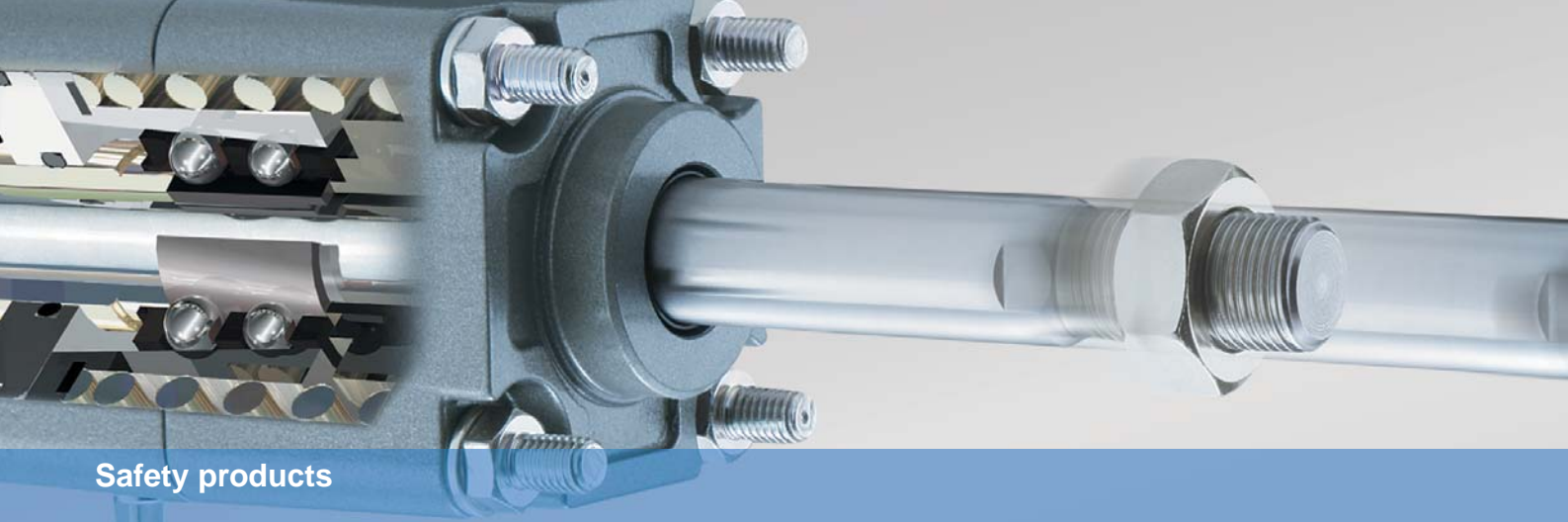


### Operational and safety components

The EU has produced guidance about the difference between these components as stated below:

*“Many machinery components are critical for the health and safety of persons. However purely operational components are not considered as safety components. Safety components are components intended by the component manufacturer to be fitted to machinery specifically to fulfill a protective role. Components placed independently on the market that are intended by the component manufacturer for functions that are both safety and operational functions, or that are intended by the component manufacturer to be considered as safety components.”*

SMC clearly states which components are intended for safety functions and are hence “safety components”. SMC does not intend operational components to be used for safety functions.

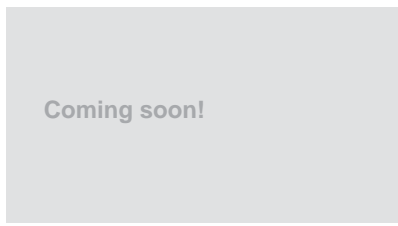


Safety products

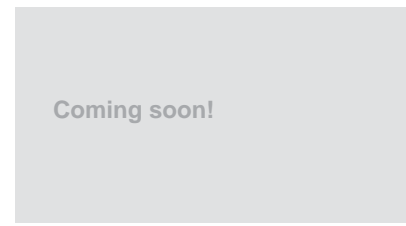
**Two hand control valve  
Series VR51**



**Single dump valve  
Series VG342-□-X91**

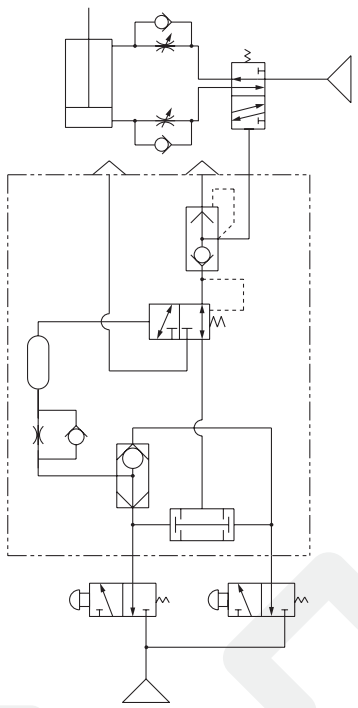


**Double dump valve  
(including soft-start valve)  
Series VG342-□-X87/X89**



- **Certified to type IIIA of EN574.**
- When starting an operation, accidents such as fingers being caught can be prevented, by requiring both hands to be used to operate push button valves.

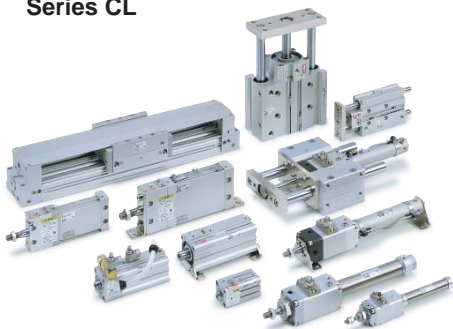
Possible circuit for the control of extension of a cylinder:





## Operational products \*

### Cylinders with lock Series CL



- **Suitable for emergency stops.**
- Since the mechanism locks when air pressure is exhausted, safe operation is possible even when there is a failure in the air supply or power system.

### Cylinders with end lock Series CB

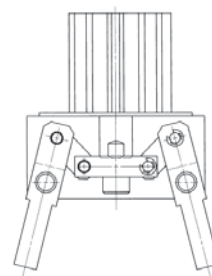


- **Holds a cylinder position even when the air supply is cut off.**
- Can prevent unexpected movement by locking when the air is exhausted at the stroke end position.

### Angular style air gripper toggle type Series MHT2



- A large holding moment in the vicinity of the support point is achieved through a toggle construction.
- **The workpiece can be held in place even when there is no supply of compressed air.**
- Robust simple construction.
- Over centre toggle action.
- Holds load even if air fails.
- Drive actuator can be replaced or re-sealed.
- Very high holding forces.



\* Operational products not certified as safety components.

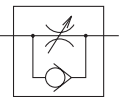
## Operational products \*

### Tamper proof speed controller Series AS□□□1F



Elbow Type/Universal Type

- Tamper resistant adjustment.
- **Prevents accidental loss** of needle.

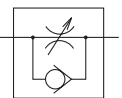


### Tamper proof speed controller Series AS□□□1F



Elbow Type/Universal Type

- Tamper resistant adjustment.
- **Prevents accidental loss** of needle.

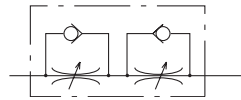


### Tamper proof speed controller Series ASD□□□1F



Dual speed controller/Universal Type

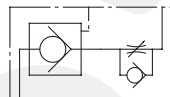
- Tamper resistant adjustment.
- Prevents accidental loss of needle.
- Ideal for single acting cylinders with low speed in both directions.
- **Lurch prevention**



### Speed controller with pilot check valve Series ASP



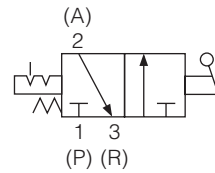
- Drop Prevention.
- The speed controller with pilot check valve is used to **stop the cylinder in mid stroke for extended periods of time** when air is cut-off.



### Residual pressure relief 3 port hand valve Series VHS



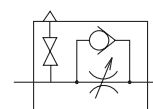
- **Isolates** supply and **exhausts** residual pressure.
- Open/closed indicator.

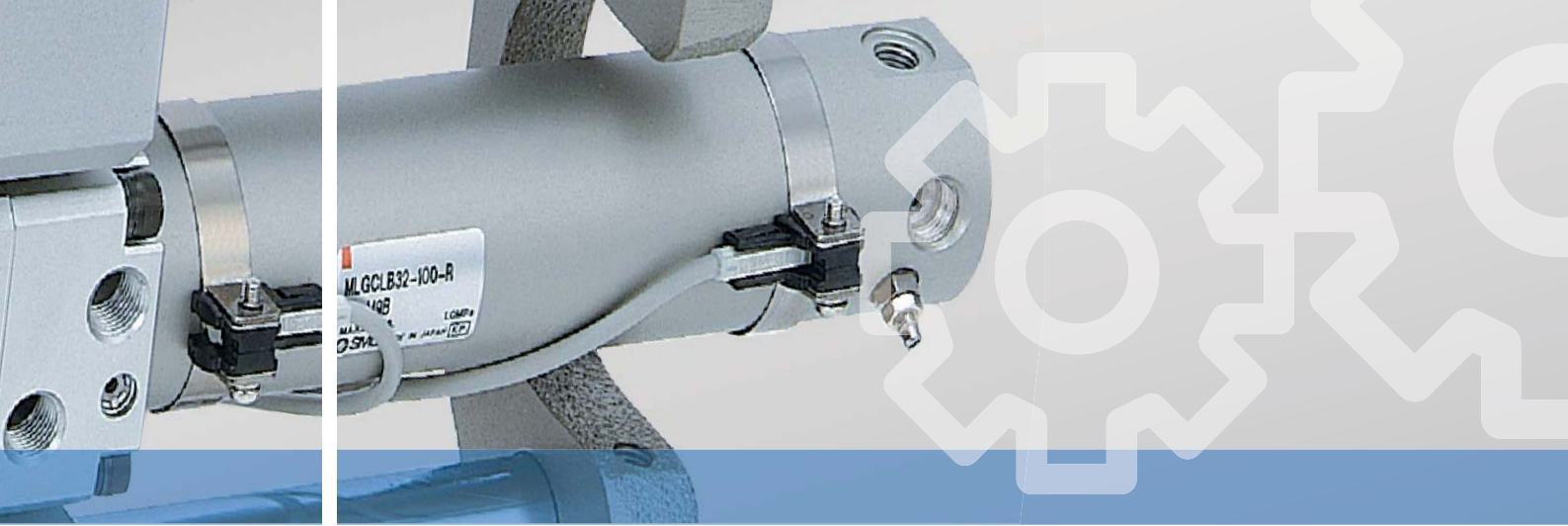


### Speed controller with residual pressure release valve Series AS□□□FE



- **Residual pressure easily released with one push of button.**
- Red colour release button.
- One-touch fitting as standard.
- Meter in and meter out flow styles.

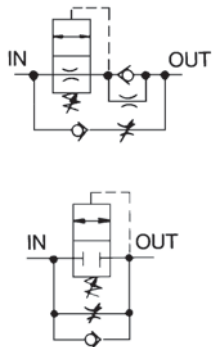




**Speed control valve  
Series ASS**



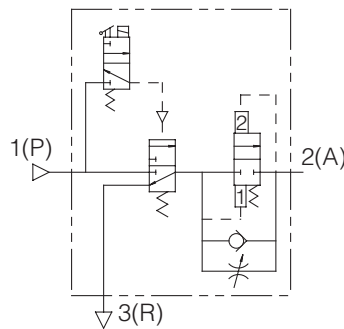
- Meter out type - a control valve with **cylinder speed control, fixed throttle and rapid air supply function**.
- Meter in type - a control valve with **cylinder speed control function and rapid air supply function**.



**Soft start up valve  
Series EAV**



- **Soft start up valve.**
- Integrated pressure release function.
- Adjustable fill bleed orifice.
- Pressure gauge can be fitted.
- Low power consumption.
- Connectable with modular type FRL combination unit.
- Large Cv factor.
- **High relief capacity.**



**3 Port Solenoid Valve  
Series VP300/500/700**



- **Reduced power consumption.**
- Port size G 1/4", G 3/8", G 1/2".
- Body ported type.
- Simple conversion to functions N.C. or N.O.
- Pilot-operated poppet valve for superior flow capacity.
- Pilot air model for vacuum.

**3 Port Pilot Poppet Solenoid Valve  
Series VG342**



- Light Weight: 1.1 kg
- Large Flow Capacity
- Low Power Consumption
- No lubrication required
- Possible to use in vacuum or under low pressures.
- Changeable actuation: N.C., N.O. or External pilot
- **Can be used as a selector or divider valve (External pilot)**

\* Operational products not certified as safety components.



### SMC Corporation (Europe)

<b>Austria</b>	☎ +43 2262622800	www.smc.at	office@smc.at	<b>Lithuania</b>	☎ +370 5 2308118	www.smclt.lt	info@smclt.lt
<b>Belgium</b>	☎ +32 (0)33551464	www.smc-pneumatics.be	info@smc-pneumatics.be	<b>Netherlands</b>	☎ +31 (0)205318888	www.smc-pneumatics.nl	info@smc-pneumatics.nl
<b>Bulgaria</b>	☎ +359 29744492	www.smc.bg	office@smc.bg	<b>Norway</b>	☎ +47 67129020	www.smc-norge.no	post@smc-norge.no
<b>Croatia</b>	☎ +385 13776674	www.smc.hr	office@smc.hr	<b>Poland</b>	☎ +48 222119600	www.smc.pl	office@smc.pl
<b>Czech Republic</b>	☎ +420 541424611	www.smc.cz	office@smc.cz	<b>Portugal</b>	☎ +351 226166570	www.smc.eu	postpt@smc.smces.es
<b>Denmark</b>	☎ +45 70252900	www.smc.dk.com	smc@smc.dk.com	<b>Romania</b>	☎ +40 213205111	www.smcromania.ro	smcromania@smcromania.ro
<b>Estonia</b>	☎ +372 6510370	www.smc-pneumatics.ee	smc@smc-pneumatics.ee	<b>Russia</b>	☎ +7 8127185445	www.smc-pneumatik.ru	info@smc-pneumatik.ru
<b>Finland</b>	☎ +358 207513513	www.smc.fi	smc@smc.fi	<b>Slovakia</b>	☎ +421 413213212	www.smc.sk	office@smc.sk
<b>France</b>	☎ +33 (0)164761000	www.smc-france.fr	contact@smc-france.fr	<b>Slovenia</b>	☎ +386 73885412	www.smc.si	office@smc.si
<b>Germany</b>	☎ +49 (0)61034020	www.smc-pneumatik.de	info@smc-pneumatik.de	<b>Spain</b>	☎ +34 945184100	www.smc.eu	post@smc.smces.es
<b>Greece</b>	☎ +30 210 2717265	www.smchellas.gr	sales@smchellas.gr	<b>Sweden</b>	☎ +46 (0)86031200	www.smc.nu	post@smc-pneumatics.se
<b>Hungary</b>	☎ +36 23511390	www.smc.hu	office@smc.hu	<b>Switzerland</b>	☎ +41 (0)523963131	www.smc.ch	info@smc.ch
<b>Ireland</b>	☎ +353 (0)14039000	www.smc-pneumatics.ie	sales@smc-pneumatics.ie	<b>Turkey</b>	☎ +90 (0)2124440762	www.entek.com.tr	smc@entek.com.tr
<b>Italy</b>	☎ +39 (0)292711	www.smcitalia.it	mailbox@smcitalia.it	<b>UK</b>	☎ +44 (0)8451215122	www.smc-pneumatics.co.uk	sales@smc-pneumatics.co.uk
<b>Latvia</b>	☎ +371 67817700	www.smclv.lv	info@smclv.lv				