SAFETY GALA 2013
SAFETY BY CHOICE NOT BY CHANCE

Automation and the Machine Directive





Alfonso de Victoria
Machinery Safety Expert

e-mail: adevictoria@chilworthglobal.com

Athens, May 2013

Contents

- Two key changes in 2006/42/EC directive;
- Safety functions based on electro mechanic and/or electronic components;
- Concentrated Vs. spread safety functions;
- Safety functions available in safety-related power drive systems;
- How to select the safety functions needed for a production line;
- How to validate the safety functions in a production line.

The two most important changes in machinery directive

With no doubt:

Accepting software for safety functions;

AND

The set of definitions, mainly manufacturer's.

Essential Health and Safety Requirement (EHSR) 1.2.1

Safety and reliability of control systems

Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that:

— they can withstand the intended operating stresses and external influences,

— a fault in the hardware or the software of the control system does not lead to

hazardous situations,

Definitions- Manufacturer

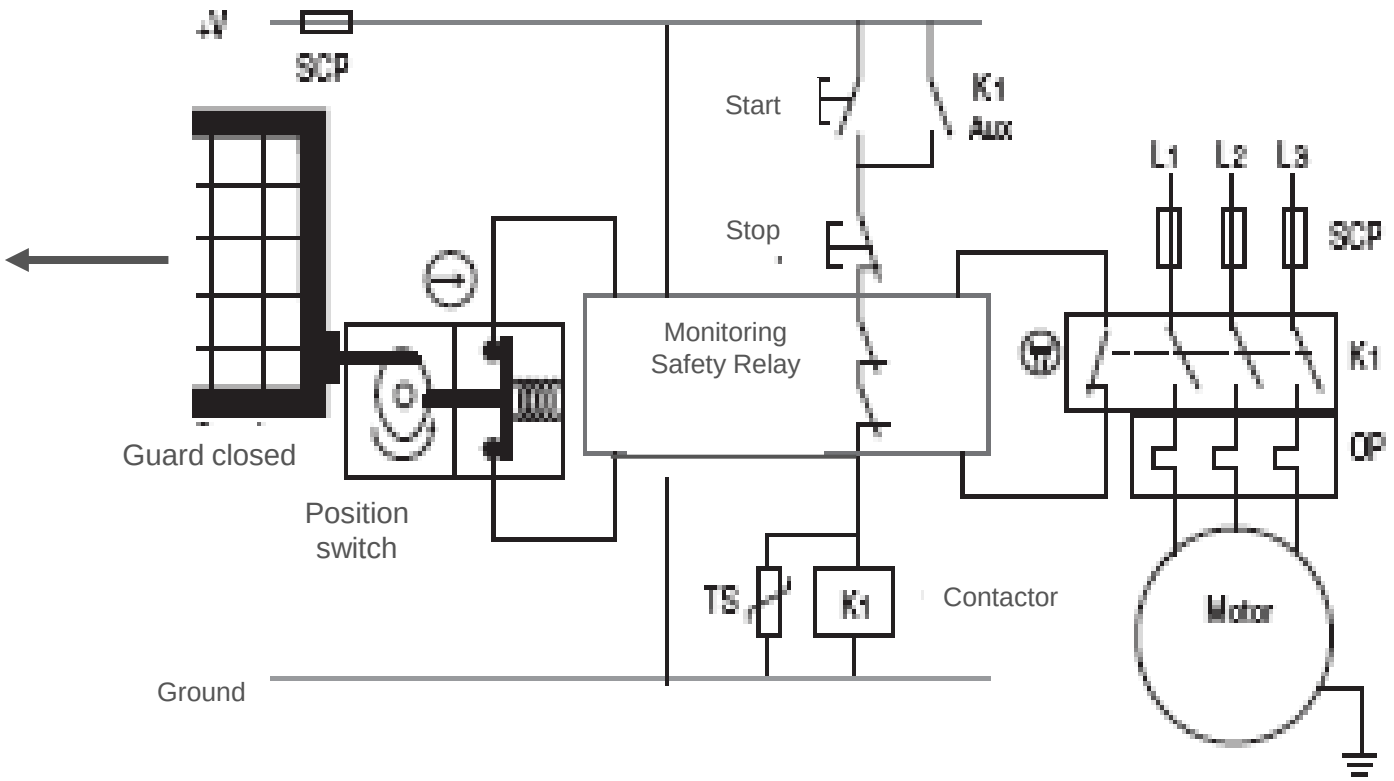
(i) ‘manufacturer’ means any natural or legal person who designs and/or manufactures machinery or partly completed machinery covered by this Directive and is responsible for the conformity of the machinery or the partly completed machinery with this Directive with a view to its being placed on the market, under his own name or trademark or for his own use.

(ii) In the absence of a manufacturer as defined above, any natural or legal person who places on the market or puts into service machinery or partly completed machinery covered by this Directive shall be considered a manufacturer;

Definitions- 4th defininition for Machinery

Assemblies of machinery referred to in the first, second and third indents or partly completed machinery referred to in point (g) which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole,

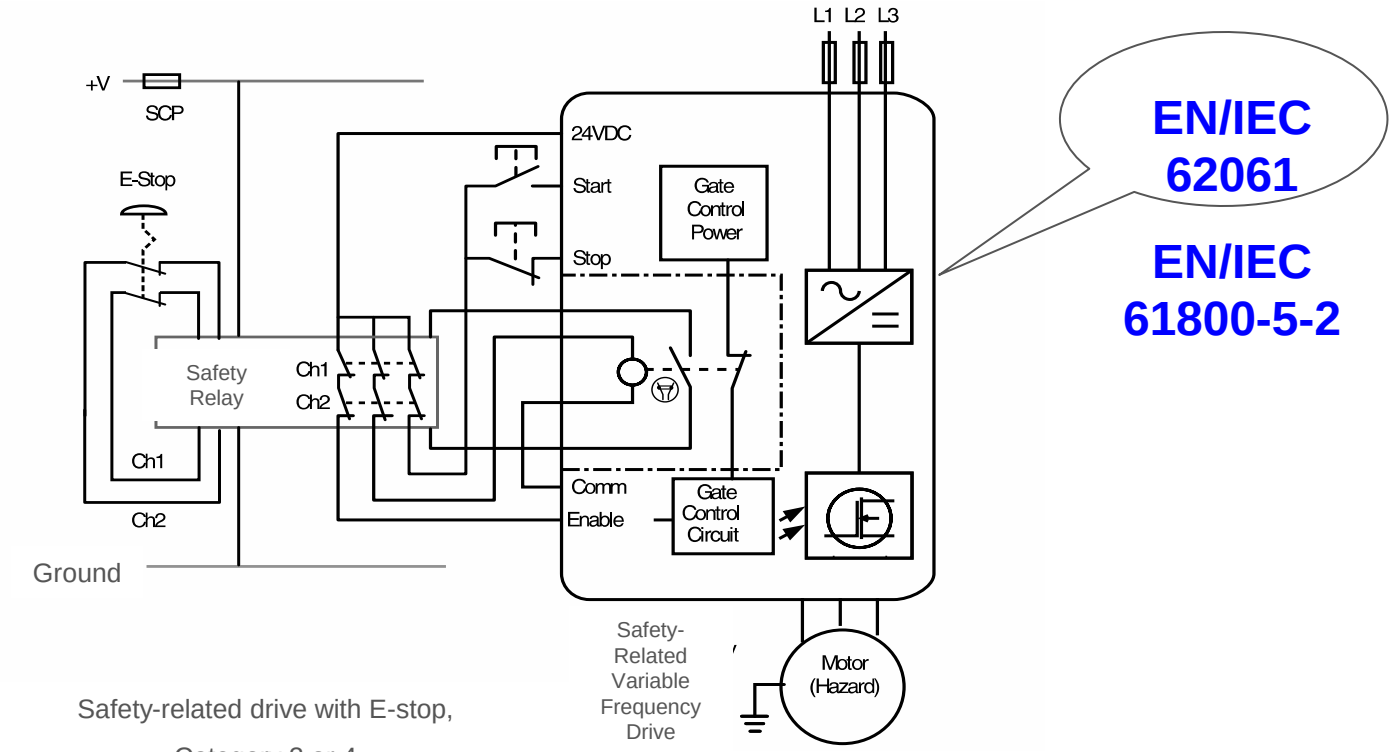
Sample design of a “classic” safety function



Safety contactors in a “classic” safety function

- Normally closed (NC), mechanically linked, are used to feed back the condition to the safety-related control unit.
- Normally closed (NC) and normally opened (NO) contacts cannot be closed at the same time.
- According to IEC 60947-5-1 standard, the mechanically linked contacts must fulfil the following requirements:
  - If normally opened (NO) contacts become welded, NC contacts remain opened at least 0,5 mm.
  - On the other side, if NC contacts are welded, the normally opened (NO) contacts stay opened.

Sample design of a safety function based on a safety-related variable speed drive



Safety-related drive with E-stop,

Category 3 or 4

Don’t mix up

A classic variable frequency (speed) drive with a safety-related one.

- With the first one, there is **no way** of monitoring any fails;
- In a safety-related one, its **condition is constantly checked** by the monitoring device.

Reliability items of data provided by the Safety-Related Power Drive System PDS (SR) manufacturer

SIL (Safety Integrity Level), according to EN IEC 62061 standard;

PL (Performance Level), according to EN ISO 13849-1 standard;

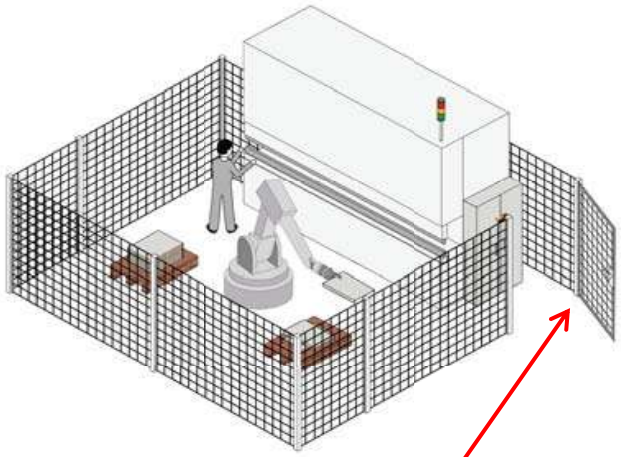
PFH (Probability of failure in one hour), y

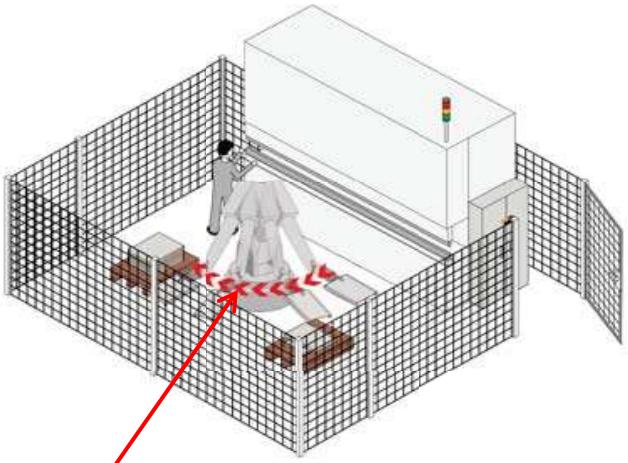
$MTTF_d$: Mean time to failure (dangerous), in years .

Why to use a PDS (SR)?

By using the available Safety Functions (SF) in a PDS (SR):

From static safety ➔ To dynamic safety





Independent from machine condition

Robot speed = f (persons)

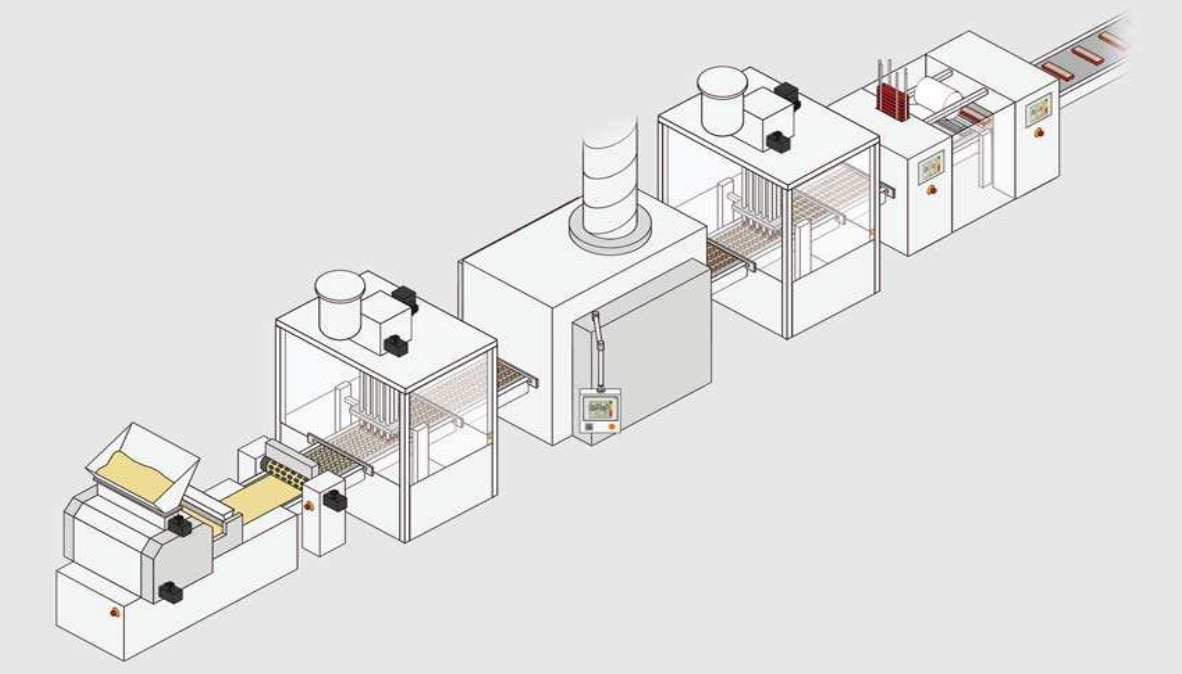
ASSESSED RELIABILITY

What a PDS (SR) is like

Like a closed box with two significant items:

Safe power shut off
Safe monitoring of: • Stop; • Speed; • Brake; • Movement direction; • Permitted distance…

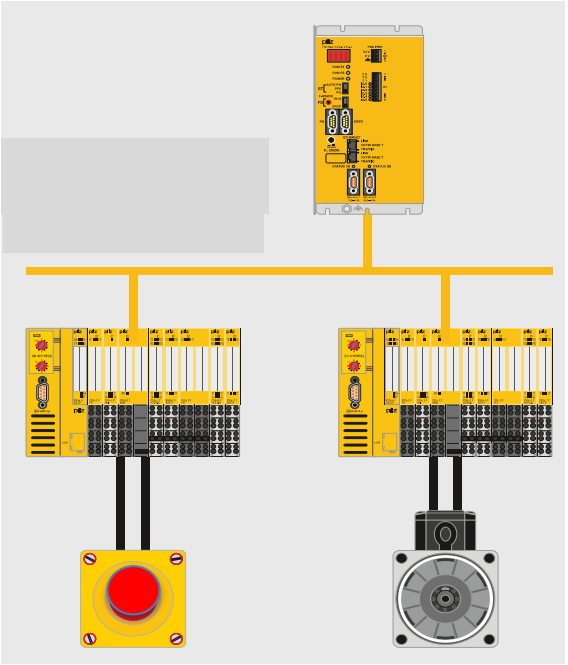
Assemblies of machinery

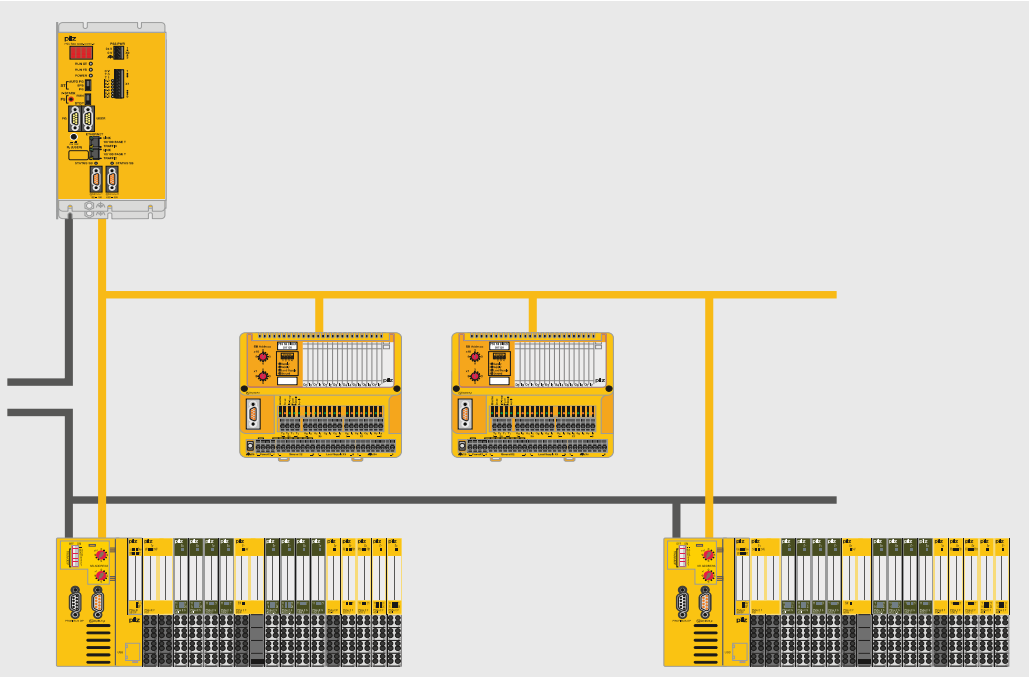


Decentralised safety technology

Data transmision among safety components.

Copper, wireless, light or fibre-optic based.





A robot cell with decentralised safety functions



Safety functions in EN 61800-5-2 standard

3 classes, related to:

- Safe stop;
- Safe monitoring of kinematic variables; and
- Safe break.

STO (Safe Torque Off)

The power is safely removed and no further movement is possible, and **unexpected start-up is prevented**.

It corresponds to a category 0 stop (uncontrolled stop) in EN 60204-1 standard.

MACHINE TOOL PROTECTED BY A LIGHT CURTAIN

SS1 (Safe Stop 1)

The braking ramp or time are controlled by the safety function. When the motor is at standstill, the **STO** function is triggered.

It corresponds to a category 1 stop (controlled stop) in EN 60204-1 standard.

CAR BODY MUTING

SS2 (Safe Stop 2)

The braking ramp or time are also controlled by the safety function; power is not removed. When the motor is at standstill, the safe operating stop (**SOS)** function is triggered.

It corresponds to a category 2 stop (controlled stop) in EN 60204-1 standard.

SOS (Safe Operating Stop)

Safe operational stop, the stopping referred to in ESHR 1.2.4.2 in the directive. The energy supply to the actuators is maintained, so the stop condition must be monitored and maintained.

It corresponds to a category 2 stop (controlled stop) in EN 60204-1 standard.

This SF monitors the standstill position.

SLS (Safely Limited Speed)

To safely limit the speed.

Very complicated without drive integrated safety functions.

Tipical use: dangereous moving parts motion with a guard removed or a protective device disabled.

SLI (Safely Limited Increment)

The moving part is allowed to travel a permitted distance.

Encoder systems.

SLT (Safely Limited Torque)

Reduced torque or force.

Usually executed by measuring the motor current.

SLP (Safely Limited Position)

Ensures that the moving part does not exceed a preset position limit.

Tipical use: robot cells

SBC (Safe Brake Control)

Safe signal to drive a mechanical brake.

Safety brakes must be used.

Tipical use: brakes for axes with suspended loads

How to select the SF needed for an assembly of machinery

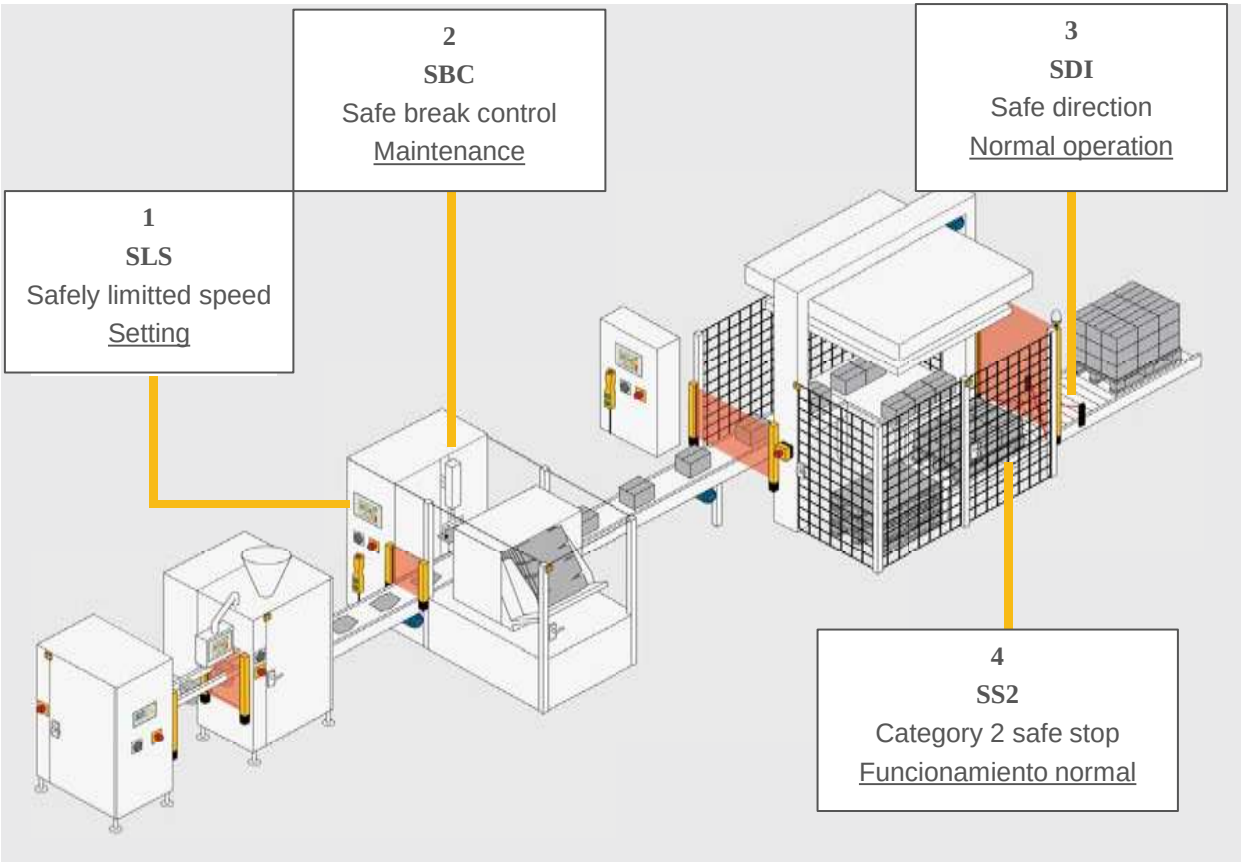
As usual for Machinery Directive

Starting rom the identification and assessment of dangerous situations

Dangerous situations found

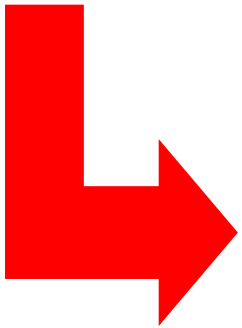
Danger	Zone (shown in figure)	Life phase	Cause	Safety Function
Mechanic	1	Setting	Speed too high	**SLS** Safely limited speed
Mechanic	2	Maintenance	Suspended moving part fall	**SBC** Safe break control
Mechanic	3	Normal operation	Error in power phases sequence	**SDI** Safe direction
Mechanic	4	Normal operation	Operator intervention due to malfunction	**SS2** Category 2 safe stop

Safety functions to be implemented



How to assess the safety function

By means of a harmonised standard



EN ISO 13849

And last but not least…

Thanks for your patience