



## Are your safeguards as safe as you think?

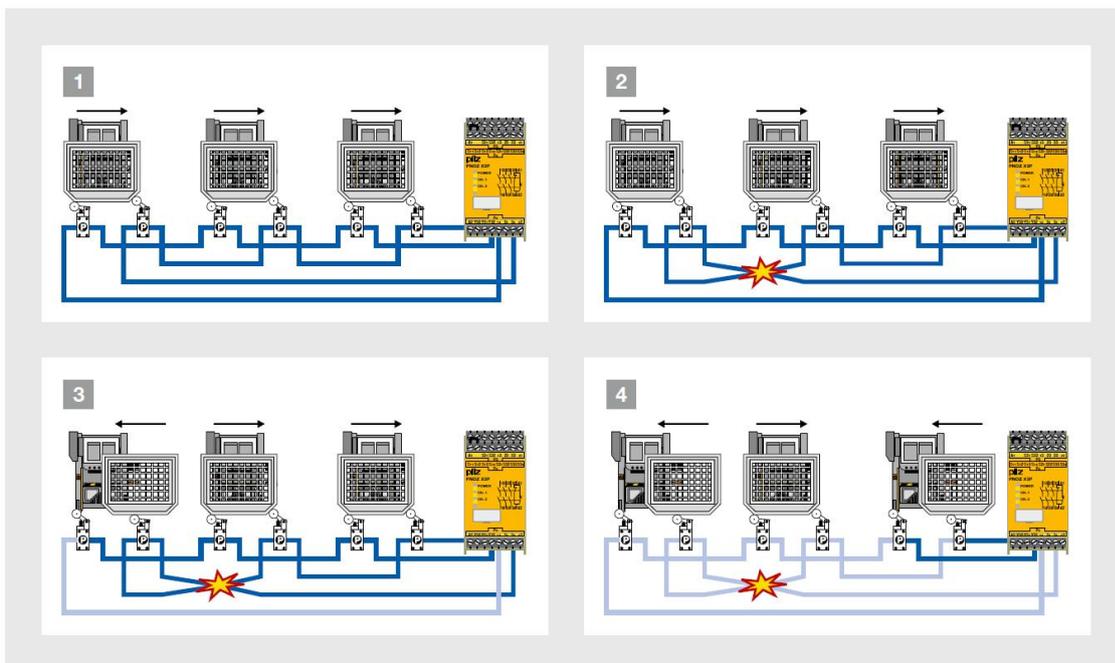
There are doubtless many machines in the UK fitted with multiple guards which are monitored in one circuit by series connected safety switches with dual channel wiring; does this sound like one of your machines? Can any of these guards be opened simultaneously? Then read on!

Historically the practise of series-wired safety switches has arisen because it saved money on cabling and safety relays, and because such dual channel wiring translated to Category of 3 of the now-withdrawn standard EN 954-1 (for more than one switch in series, EN 954-1 degraded Category 4 to Category 3). Category 3 lives on in the standard EN ISO 13849-1 in which clause 6.2.6 requires that for Category 3 to apply specific conditions must be met which include: a single fault must not lead to a loss of the safety function, that an accumulation of undetected faults can lead to the loss of the safety function, *and importantly as an addition over and above EN 954-1's requirements that **at least 60% of faults have to be detected in a diagnosis mechanism (DC = low)***.

On closer inspection the ability of a system to detect 60% of dangerous faults can be impacted by a phenomenon known as “fault masking” which can dramatically reduce the Diagnostic Coverage and consequently the Performance Level as will be explained below.

### Fault masking

The answer as to how many (if any) switches can be connected in series depends on the faults that can be anticipated (of which there is a list in the validation standard EN 13849-2). The following example of interlocked guards connected in series is intended to illustrate this point.



**1** The example shows three safety gates connected in series to an evaluation device. Initially all the safety gates are closed and the relay's outputs are “on”, i.e. the machine can be operated.

**2** On the left-hand safety gate, a short circuit occurs in the line to the switch with the N/C contact. At first the fault is not detected (because a demand has not yet been placed upon the safety function) and the machine can continue operating (because the guard is still closed).

**3** The left-hand safety gate is then opened, an event which the left switch signals to the relay. During feasibility comparison of the two switches the safety relay discovers an inconsistency and switches to a fault condition, i.e. once the safety gate is closed the machine cannot be restarted (but in this case the safety gate is left open).

**4** Now the right-hand safety gate is also opened. Via these signals the relay once again detects a normal condition. The fault condition is reset, the safety gates can once again be closed from left to right and the machine is ready to start up again.

This example illustrates an **undetected fault** in the safety circuit, which has built up as a result of the clearing of the fault by the simultaneous opening of two gates. An additional, subsequent fault could cause the whole interlocked guard system to fail to danger (e.g. another wiring fault occurs, a guard is opened and the machine *does not stop*). While this is in line with Category 3 (an accumulation of undetected faults can lead to a loss of the safety function) these and similar faults are described by the term **“fault masking”**. In the current standard EN ISO 13849-1, the maximum diagnostic coverage (DC) that the switch can achieve is restricted, depending on the masking probability.

In practice, a single switch pair that is evaluated by a safety relay can achieve a DC = 99%. Based on this premise, in the current draft of EN ISO 14119, the maximum DC for a group of interlinked switches is dependent upon the number of switches connected in series and their frequency of operation. Note at some point ISO 14119 will replace the current standard for interlocking, EN 1088.

As you can see in the table below, masking restricts the maximum achievable DC and PL.

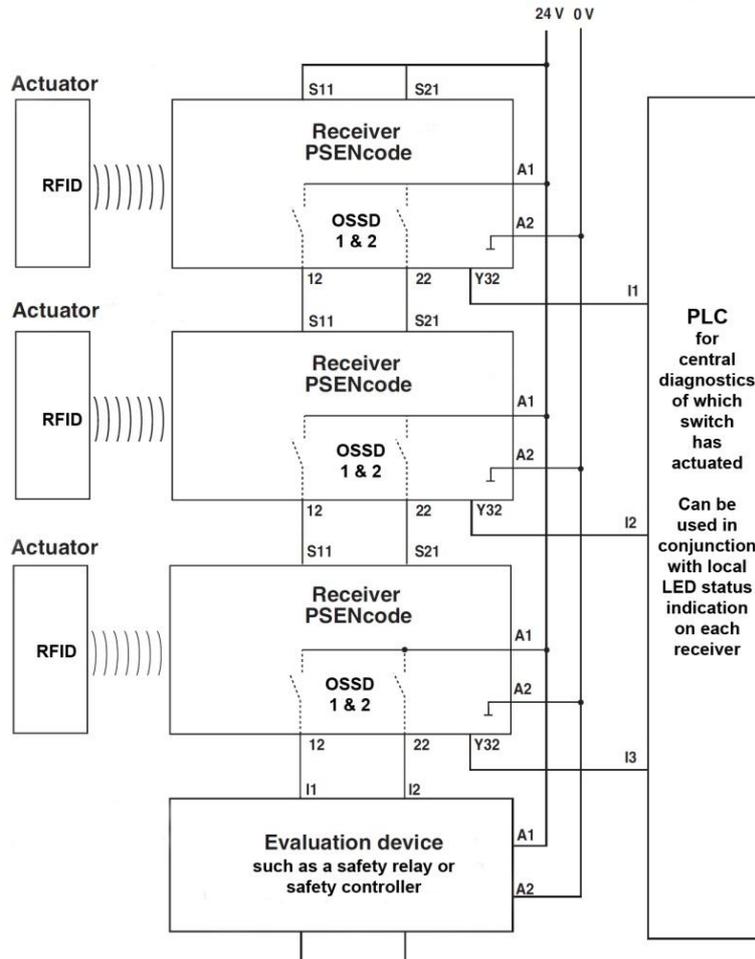
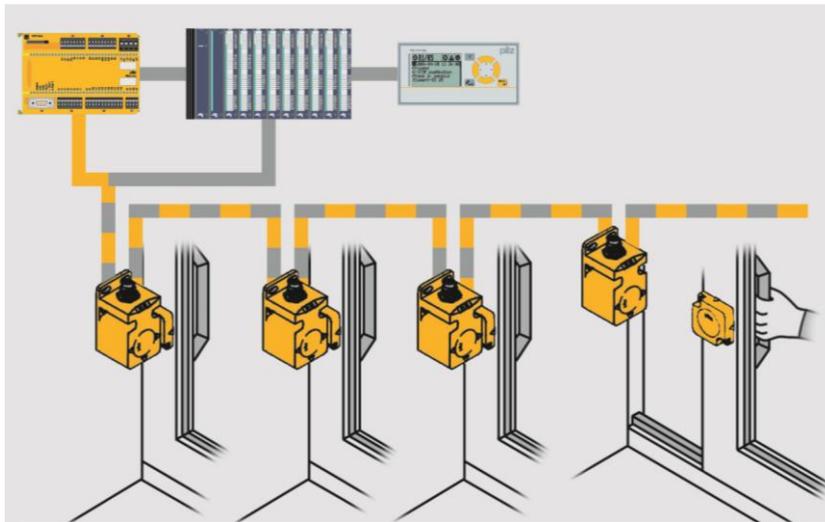
Number of frequently used movable guards <sup>1)</sup>		Number of additional movable guards	Masking probability	DC for guard limited to	Maximum achievable PL
1	+	1	Low	Low (≥ 60 %)	PL d
		2 to 4	Medium	Low (≥ 60 %)	PL d
		> 4	High	None (< 60 %)	PL c
> 1		-	High	None (< 60 %)	PL c

<sup>1)</sup> Switching frequency greater than once per hour

From the above, if you can show that no two guards are moved with a frequency of greater than once an hour, or there are no more than 4 of them in series, the statistical chance of a fault occurring and being masked is reduced; however the Diagnostic Coverage of the system is reduced from 99% to 60% (low), which in terms of EN ISO 13849-1 means the best PL achievable is PL d which also means you’ve met Category 3 – so no problem if your risk assessment required Category 3.

If you find that more than one guard can be moved with a frequency of greater than once an hour, or there are more than 4 of them in series, the statistical chance of a fault occurring and being masked is high and the result is that Diagnostic Coverage is reduced to less than 60% (according to EN ISO 13849-1 this is equivalent to no DC). Under these circumstances, according to EN ISO 13849-1, the best achievable PL is **PL c**, or Category 1 in old terms. If your original risk assessment required Category 3, under these circumstances your system is no longer compliant.

## Is there a cure for fault masking?



If a series of interlinked switches is required to meet PL e, a technical solution is required, using switches with integrated fault detection. As masking cannot occur in this case, it is possible to have interlinked switches without restricting the DC or PL. Only switches with internal diagnostics and an OSSD (Output Signal Switching Device) output, a solid state type as

commonly found on RFID based switches, are unaffected by this. Such devices are certified by the manufacturer with PL e (i.e. they are classed as a subsystem, not just a component) which means they have their own internal dual channel category 4 architecture, built in 99% DC, as well as the other internal characteristics allowing the series connection of switches (such as extremely low failure rates expressed as  $PFH_D$  in the magnitude of  $10^{-9}$  dangerous failures per hour). Diagnostics of which guard has been opened (not to be confused with Diagnostic Coverage, which is to do purely with detection of dangerous failures) is provided on the switch body by LED status, and also via signalling which can be taken to a standard PLC.

## Types of device with RFID coding and OSSD outputs

Some manufacturers of safety components, including Pilz, deploy this technology in their products. Other than the capability to avoid fault masking, RFID based non-contact switches also offer less troublesome switching (when compared to magnetic types) through various actuator approach angles, and better resistance to defeat through the use of varying degrees of coding (all the way to unique actuator/receive pairs), and better protection against ingress (when compared to mechanically actuated switches). Pilz has adopted this technology in to a wide range of its devices.

[PSENcode switches](#) (RFID guard position monitoring devices with self-monitoring OSSDs)



[PSENslock](#) (solenoid locks with built in RFID guard position monitoring with self-monitoring OSSDs)



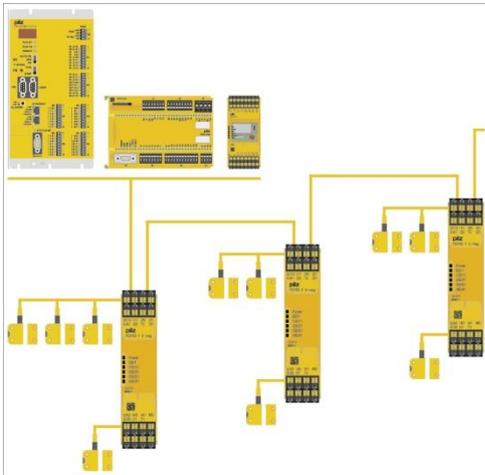
[PSENsgate](#) (solenoid locking, command to release, E-stop, escape from inside the hazard area, and RFID guard position monitoring system with self-monitoring OSSDs)



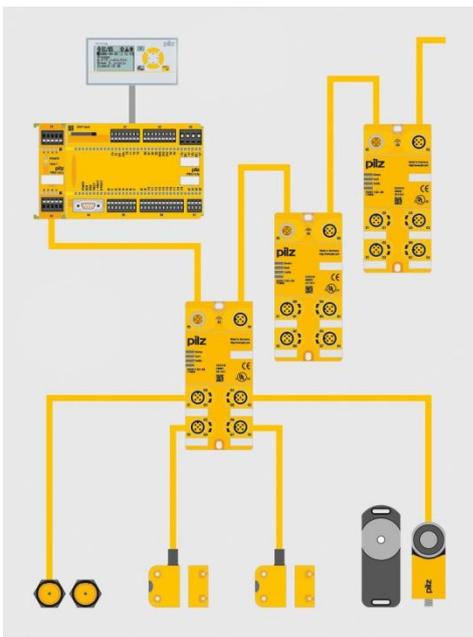
[PSENini](#) (inductive safety sensors for safe position monitoring e.g. robot home position, with self-monitoring OSSD outputs)



## An alternative or complementary solution – the use of distributed I/O



Other than replacing designs using series, volt-free switches with RFID / OSSD-based technology, there are other options based upon improved wiring management through “zoning”. Normal volt-free contact-based switches are wired individually, but in low numbers, back to local IP20 I/O modules in small control boxes (such as [Pilz PDP20 F mag](#)), which in turn can be cascaded across the machine back to a main panel using the OSSD outputs of the PDP20 F mag modules to provide 99% DC throughout the system.



Where the luxury of enclosures for IP20 I/O modules is non-existent, I/O modules can be conveniently placed directly on-machine (such as [Pilz PDP67 F 4 Code](#) and [PDP67 F 8DI ION](#), illustrated) because they are IP67 rated (epoxy encapsulated, available with stainless steel M12 threaded connectors for long term resistance to washdown cleaning). These modules can be cascaded across a machine on one multicore cable back to the main control panel without degradation of DC or PL through use of coding or test pulses.

Pilz has developed a SafeLink protocol for use with its PNOZmulti safety controller and PDP67 F 8DI ION modules; up to four SafeLink modules (PNOZm12p) can be connected to a PNOZmulti controller and up to four PDP67 modules connected to each SafeLink module. Up to four

dual channel devices can be connected to each PDP67 modules. Therefore it is possible to connect up to 64 (4 x 4 x 4) dual channel remote switches back to one PNOZmulti.

## E-stops in series?

It is worthy of note that series connection of Emergency stop devices is unlikely to incur a loss of Diagnostic Coverage, based upon the fair assumption that it's unlikely that any two E-stops will be actuated simultaneously or as frequently as once an hour. Therefore it is reasonable to wire such devices in series. That said, it is generally inadvisable to require E-stops to perform to PL e simply because they're not intended as primary protective devices; if a hazard requires a safety related control function to perform to PL e other primary means of safeguarding should be used.

**Conclusion:**

Fault masking is a real issue even if you don't refer to current or future standards and you just apply basic engineering logic. Designers of safety guards and associated circuits on new machines, and those responsible for existent machines in use should review whatever safety guard circuits they have where safety switches are connected in series. You need to ensure that the ugly head of masked faults can't, sometime in the future, rise up and bite unsuspecting victims. The technology is available to help reduce on-machine cabling and, critically, the possibility of fault masking.

**For more information please visit <http://www.pilz.co.uk>**

PSENCs webcode: 5184

PSENIini webcode: 6256

PSENSlock webcode: 5193

PSENsgate webcode: 6474

PDP67 webcode: 6557

PNOZmulti webcode: 5245

*Article written by David Collier at Pilz Automation Technology.*