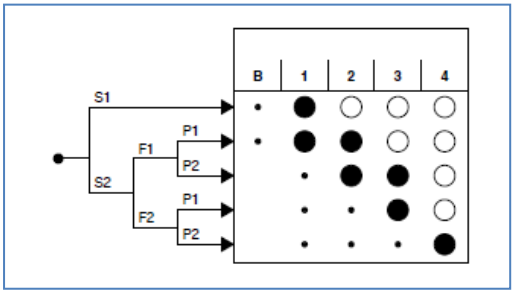
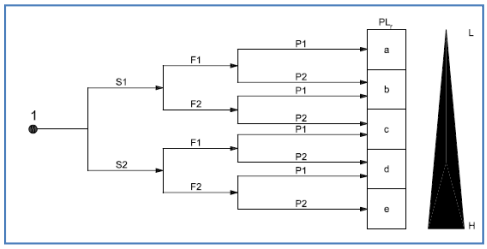
Designers of safety circuits on guards with a PLd might be tempted to use Category 2 architecture to reduce cost, but are they ready for the test requirements?

Up until recently the Category of the control system, as per EN 954-1 (scheduled for withdrawal at end 2011) has been used as the basis for construction of safety-related control functions. With increasing uptake of EN ISO 13849-1, however, the term “Category” has been taken over by “Performance Level (PL)”. In addition to Category, PL also considers the reliability (MTTFd) of the individual components and combination of components in a safety-related control system to evaluate the availability of a safety function over time, but the behaviour of the safety function in the presence of faults is still dictated by the Category, now also referred to as architecture or structure.



In the past, designers using the risk graph in EN 954-1 may have arrived at a Category 3 requirement based upon known severity, frequency of exposure and possibility of avoidance parameters. The designer would then have designed a dual channel system, one with redundancy or hardware fault tolerance (HFT= 1), providing a behaviour that a single fault in the system would not give rise to a loss of the safety function.



These same parameters used with the similar risk graph in EN ISO 13849-1 would most likely lead to the PLd.

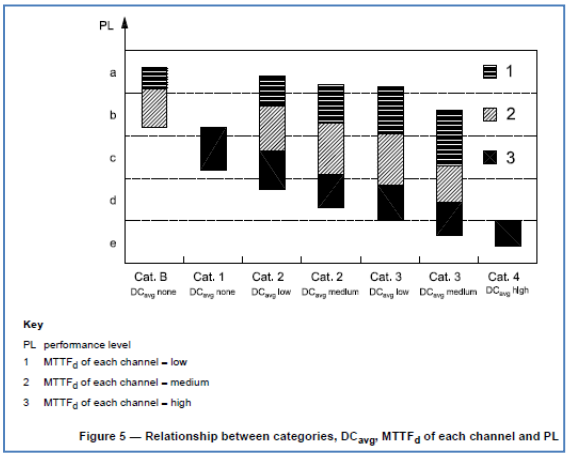


Figure 5 — Relationship between categories, DC_{avg}, $MTTF_d$ of each channel and PL

Testing

In EN ISO 13849-1, PL is achieved by a combination of Category, MTTFd (mean time to dangerous failure) and diagnostic coverage (DC). According to figure 5 in the standard, PLd is still achievable using Category 3 architecture but also using Category 2 (so long as the MTTFd is high and there is at least a low level of diagnostic coverage). It may be very tempting to try to use Category 2, single channel architecture to achieve PLd – to save component cost and panel space. A central factor in Category 2 is checking the safety function (not increased reliability), where an increased check frequency will decrease the probability of a dangerous situation – in other words testing reduces the probability of continued operation in the presence of a fault. Within the simplified procedure in EN ISO 13849-1 the check in Category 2 must occur at start up and then periodically, and there is an assumption that the frequency equates to at least one hundred tests to every demand on the safety function (clause 4.5.4 of EN ISO 13849-1, where for Category 2 “demand rate $\leq$1/100 test rate”). This test rate is an additional quantitative factor to that given in the old EN 954-1. In other words, if you try to claim PLd using Category 2 architecture,

you are assuming that the safety function will be tested at least 100 times between demands upon the safety function! This warrants closer inspection.

BGIA (now IFA) has worked out the Markov reliability model of EN ISO 13849-1 designated architecture category 2 as a single-channel circuit with this high test frequency, based on the findings of a European working group trying to map EN 954-1 categories to the SILs of IEC 61508/IEC 62061. This is a challenge within the machine industry where safety functions are considered to be high demand *versus* the process industry where the demand placed upon safety functions is low or continuous.

It's difficult to see how users are going to manage this test frequency in machine applications on anything other than a dynamically tested OSSD (solid state safety output) on a light curtain, or in very low demand applications such as infrequently used emergency stops. For electromechanical devices on guards (such as tongue interlock switches, limit switches, magnetic safety switches) testing will mean actuation (i.e. opening and closing the guard) at least 100 times between the functional need to open the guard. This may at least prove inconvenient because it would impede productivity, or even impossible due to the high demand already placed upon the safety function. Imagine having to test a guard door 100 times within a two minute production cycle – not practical! Lastly, consider the implication of frequent testing of electromechanical devices in terms of component wear and tear. MTTFd for an electromechanical component (like a safety interlock switch or contactor) is dependent upon its B10d (failure rate data normally available from the manufacturer, otherwise generic data is available in EN ISO 13849-1 in table C.1) and the number of operations in a year (n_{op}). The stress placed upon the components would be a hundred times greater for the tests as that placed upon them due to the demand of the safety function, and the increased number of operations would at least reduce MTTFd (and potentially the PL), and at worst destroy the components very early in the guard's life causing lost production and expense.

$$\mathrm{MTTF_d} = \frac{B_{10d}}{0{,}1 \times n_{op}}$$

where

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\ \mathrm{s/h}}{t_{cycle}}$$

It is, therefore, more practical and common-place to achieve PLd using Category 3 or 4, dual channel architectures, because they improve reliability through hardware fault tolerance (without a highly frequent periodic test cycle) as well as "automatic" diagnostic coverage within the system.

Single failure point

On balance, there is an argument against Category 3 in PLd systems in the case where a single component, such as an interlock or limit switch containing two contacts is employed to monitor a guard. Such a device has one potential point of failure: a failure of a limit switch plunger mechanism (say due to excessive force, contamination or corrosion) is a single failure point affecting both contacts, and both channels. In this case, what is ostensibly a Category 3 architecture can be considered to be a Category 1, because a single failure can cause a loss of the safety function. With a single device containing two channels needing to achieve PLd, it's necessary to declare a "fault exclusion" which justifies why such a single point of failure in the switch body is unlikely. There is guidance in EN ISO 13849-2 on fault exclusions which considers, amongst various factors, the environment (dirt & corrosion affecting the device during the lifetime), safe positioning and mounting (such as preference for actuation occurring on opening, and avoidance of using the device as a mechanical stop), and adequate dimensioning. Where a fault exclusion can not be justified and PLd is required, the solution is to use two independent switches; this is more likely and is already common practise on monitored guards, and at this point measures taken to reduce Common Cause Failures can be quantified.

The use of fault exclusions in PLd and PLe will become a moot point when ISO 14119, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*, is published, because in it reference is made to interlocking circuits providing PLd or PLe having to include at least two position switches, since fault exclusions of mechanical faults are not accepted in high-risk applications.

Conclusion

In summary, users of electromechanical safety components on guards are urged to carefully consider the onerous test requirements of Category 2 in EN ISO 13849-1 at the design stage, especially when seeking to achieve PLd. Incorporating Category 2 architectures into PLd systems without taking these test requirements into due consideration may introduce systematic failures and associated loss of production and expense. If after design, build, supply and commissioning the machine it's decided to convert from a Category 2 architecture to Category 3 or 4 it might be difficult or impossible in terms of fitting additional on-machine components, as well as in-panel devices required to step from single to dual channel architecture.

David Collier, BDM, Pilz