Technical Paper No.4

How to use EN 13849 Safety Related Control Systems

Strategic Safety Systems

Technical Paper

EN 13849 replaced EN 954-1, but many people find it hard to use as it tends to jump backwards and forwards. Some companies are still using EN 954-1, which is no longer applicable. When understood, EN 13849 derives some major benefits and identifies whether or not the control system is sufficient to control the risks, where any weak points are and where improvements can be made.

Benefits

This gives an outline of how to drive EN 13849. This enables system designers to:

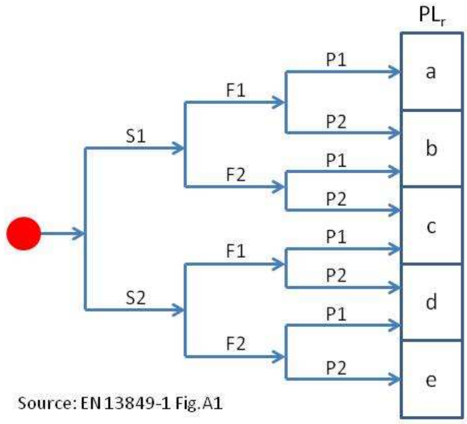
- Ensure that machinery has been assessed against EN 13849, which is a legal requirement of the Supply of Machinery (Safety) Regs.
- Be aware of whether or not the safety parts of the control system are suitable, where simplifications and therefore cost savings could be made, or where upgrades could be made

Step 1

Work out the required performance level PL_r using Fig. A1.

Choose appropriate values of S, F and P from the table below to determine was PL_r is required.

PL_r has values of a through to e (e = severe). You will have to do this for each risk point. However, if you have several similar risk points controlled by a common method, say interlocked guards, then you could start with the severest risk point. However, if you have different channels, even if they are controlled by a common method, then you would normally need to go through the following steps for each channel. For example, the damaging source of energy may be a hydraulic cylinder and an electric drive, all controlled by an interlocked guard; you would have to consider both channels.



Source: EN13849-1 Fig.A1

Severity of injury		Frequency of exposure to hazard		Possibility of avoiding harm	
S1	Slight (normally reversible)	F1	Seldom or exposure time is short	P1	Possible under specific conditions
S2	Serious (normally irreversible)	F2	Frequent or exposure time is long	P2	Scarcely possible

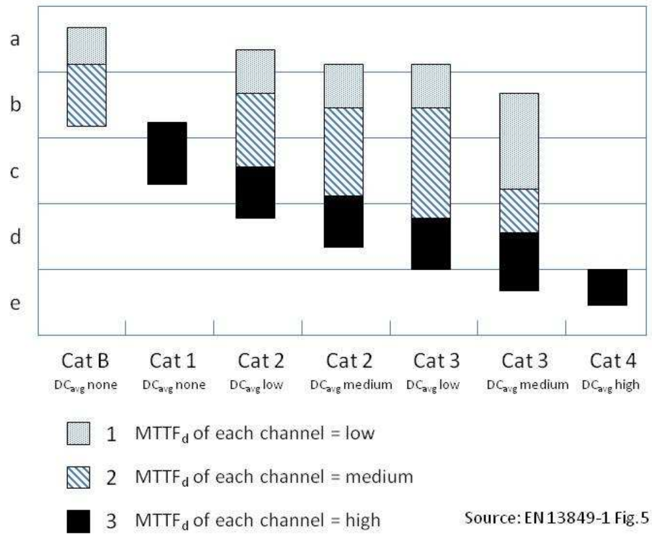
Step 2

Look at what categories of control system will deliver this PL_r using Fig. 5.

There are two terms that need to be defined:

- $MTTF_d$ = mean time to (dangerous) failure
- DC = diagnostic coverage

The options use a combination of $MTTF_d$ and DC_{avg}. Using a high MTTF control system enables you to achieve the same or higher levels of PL_r with lower requirements for DC. You can see examples of DC in table E.1 in Appendix E. I'd tend to go for the higher MTTF route rather than relying on DC; it is better to have something that is inherently reliable than to have a lower reliability device which you keep checking.



Source: EN13849-1 Fig.5

Technical Paper

Step 3

Draw a block diagram of the items in the control system, starting normally with the signalling level and working through to the device which is controlling the damaging energy.

For example, you may have an interlock switch, feeding a high-integrity relay, then a contactor and finally a hydraulic valve which controls the flow to a cylinder.

Using table C.1 in Annex C, determine the MTTF for each component. This will require an intermediate step if table C.1 specifies B_{10d} as this assumes that the MTTF depends on the number of annual operations.

Step 4

For each channel in the control system, calculate the overall MTTF. You do this by adding the reciprocals of the individual MTTFs, then taking the reciprocal of this total. This will give you a MTTF in years for each channel.

Determine what level of MTTF this is:

- MTTF between 3 and 10 years is a type 1 MTTF, ie low
- MTTF between 10 and 30 years is a type 2 MTTF, ie medium
- MTTF between 30 and 100 years is a type 3 MTTF, ie high

Step 5

If there are several channels, it is necessary to consider common cause failure. Use table F1 in Annex F which gives a scoring method to assess common cause failures. A score of at least 65% signifies that common cause failures are adequately controlled.

Step 6

If the MTTF is too low, consider what may be done to improve it or consider what methods of DC you would need to achieve the target PL_r. Conversely, if the MTTF is much higher than that needed, for example, it delivers PL_r=d where the target PL_r=b, consider if a simpler arrangement would still deliver the target PL_r.

Step 7

Ensure that the above steps are documented and are part of your technical file. Note that the CE assessment software used by SSS does the calculations in steps 4 and 5 and delivers a report for the technical file.

SSS provide CE support for machinery suppliers, agents etc. See http://www.strategicsafety.co.uk/CEMarking.html for information of what CE Marking is all about or contact SSS for more details on the support and services we provide.

Strategic Safety Systems Ltd., 8 The Highgrove, Bishops Cleeve, Cheltenham, GL52 8JA, UK
Phone: 01242 679713 Mobile 077680 11667
E-Mail: info@StrategicSafety.co.uk Web site: www.StrategicSafety.co.uk