Technical Paper

White Paper No.41

Safety and Reliability

By Phil Chambers BSc, CMIOSH

Safety and reliability are often thought of as being synonymous. They are related, but they are not the same.

- Safety is the prevention of hazardous situations occurring.
- Reliability is the confidence that those measures put in place for safety reasons continue to do their job.

Example: When I first started driving, cars had single channel brakes. The brake pedal activated a master cylinder which was connected by a pipe to the brake cylinder on each wheel. Reliability factors [2] and [3] (see below) were missing. When working properly, it was safe. However, leakage of hydraulic oil would cause the entire system to fail, and you would not know about this until you felt no resistance on the brake pedal. Then it was obviously unsafe.
Nowadays cars have dual channel systems and loss of hydraulic oil in one channel does not cause a loss in braking ability (Reliability factor [2]). In addition, there is cross-checking between the channels and a light on the dashboard tells you that you have a braking system fault (Reliability factor [3]). This is obviously more reliable than the single channel system.

Reliability in safety devices comprises any combination of the following:

1. Prevention of failure
2. Coping with failure
3. Knowing that something has failed

Reliability can be measured as either the probability of failure or, more commonly, the mean time to failure (MTTF).

EN 13849 Safety Related Control Systems is a standard which tells you what type of system and what MTTF is needed for different combinations of severity of the outcome, frequency of exposure and ability to avoid. As it is not very readable, SSS White Paper 4 How to Use EN 13849 Safety Related Control Systems steers you through this.

What is not often realised is that all of the MTTFs in the chain combine; having a high reliability switch feeding a low reliability device means that the overall MTTF is low. Therefore, emergency stops normally feed a high reliability safety relay (eg Pilz) to achieve a high MTTF.

It may seem safe that a device such as a light beam stops the machine via the PLC, but you cannot rely on this. The practice of including a standard PLC in the safety channel is not acceptable for safety related channels as the MTTF of the software is typically quite low. To those people who claim that software is reliable, ask yourself how many times you've had to reboot a computer because it hangs up?

Therefore, the safety related parts of the system must act downstream of the PLC. There are PLCs which are designed for safety related control systems but these are not normally the ones incorporated into machines.

Where specific channels need to be inhibited for safety reasons with power being maintained, then it is often acceptable to interrupt the individual channel. For example, where an axis driven by a servo motor need to be inhibited, where there is a servo enable input on the motor controller, then it is normally acceptable to interrupt this signal rather than switching the motor power lines with a relay which has its own MTTF.

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

Technical Paper