Confusion over control safety: Regulations delayed

CONFUSION WILL REIGN THROUGHOUT 2005 FOR MACHINE BUILDERS, CAUSED BY A DELAY IN THE INTRODUCTION OF NEW SAFETY LEGISLATION WHICH WILL LEAVE DESIGNERS IN A QUANDARY AS TO WHICH CODE TO FOLLOW. BOB DOBSON REPORTS.

Machinery safety standards have been changing fairly constantly for as long as most practising engineers care to remember. There is a perception that it was not always like this; perhaps 15 or 20 years ago regulations were fixed entities and relatively easy to follow, but at some point faceless pen-pushers in Brussels got the upper hand and started writing and rewriting an endless stream of new regulations.

In fact these new regulations were a new way of thinking. Previously, standards and regulations had been prescriptive, saying precisely what needed to be done, and inspectors could check for compliance. The trouble was that the regulations were becoming inappropriate in an increasing number of situations.

So the idea was developed that the design engineers should themselves take responsibility for designing safe systems. The way safety was ensured would be immaterial, so long as their machines and systems were safe. Inspectors would no longer be needed, but if there was an accident the official enquiry would expect the design engineers to be able to prove that their machines were not at fault. Thus engineers became obliged to undertake thorough risk assessments and to keep comprehensive records.

This is a laudable principle that should have driven efficiency into machine design and construction, but numerous devils have been shown to lie in the detail.

For instance, many machines are extremely complex so could fail in a manner that is very difficult to foresee; machines are often adapted after they have been in use for a year or two, and this could compromise the original safety concepts (programmable machine control systems are particularly susceptible to in-field changes); and some working environments are highly unpredictable.

Another reason for the constantly changing standards is that revisions are necessary to keep pace with emerging and developing technologies. (Consider for instance an engineer of a previous generation envisioning concepts such as remote machine control via the Internet, fieldbus architecture, wireless control, or PC powered local intelligence.) And a final one that has emerged is that changes to one standard often lead to changes in another, and one to another, and another.

So the situation has now developed where machinery safety standards are understood to change constantly. Indeed, many people in the field will work to a rule of thumb that standards are valid for about five years before being significantly revised or superseded altogether.

Rise of the safety engineer

This has lead to the rise of the professional safety engineer, someone who keeps up with the changes and how they apply in one or more sectors of engineering. These specialists often also sit on the committees that revise and develop standards, and it is inevitable that as they delve deep into the details and consider all sorts of possible scenarios, sometimes they will overrun their planned schedule.

This has happened with ISO 13849-1 *(Safety of machinery, Safety related parts of control systems, General principles for design)*, which was originally expected to replace EN954-1: 1996 *(Safety of machinery, Safety related parts of control systems, General principles for design)* in 2003, but which is still unratified. Acceptance is now expected towards the end of 2005, although of course there is no guarantee.

Meanwhile, don't be confused if you see a reference to ISO 13849-1:1999, as this is simply the ISO equivalent to EN954-1:1996, not the heavily revised and controversial new standard that is still being put through the mill.

Both EN954-1 and the new ISO 13849-1 relate to the safety related parts of machine control systems, and as their titles are identical it can be surmised that a 'straight swap' was originally expected. EN954 has served industry well, although it had always attracted the criticism that its approach was too simple to effectively cover complex machinery and did not permit the use of programmable safety systems that are rapidly increasing in popularity today.

Picture courtesy Proctor Machinery Guarding

Safety regulations under revision: *ISO 13849-1 is setting out to reflect current safety practice*

One of the aims of the committee developing ISO 13849-1 was to bring it into line with IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems,* which has seven parts: General requirements; Requirements for electrical/ electronic/ programmable electronic safety-related systems; Software requirements; Definitions and abbreviations; Examples of methods for the determination of safety integrity levels; Guidelines on the

application of IEC 61508-2 and IEC 61508-3; Overview of techniques and measures.

It was never intended, however, that IEC 61508 would be used for machinery design, because a daughter standard (IEC 62061, *Safety of machinery, Functional safety of safety-related electrical, electronic and programmable electronic control systems)* was under development specifically for the machinery sector.

Nonetheless, due to the shortcomings of EN 954-1 for complex machinery and systems using programmable electrical/electronic/programmable electronic safety-related equipment, many machine builders sought to meet the requirements of IEC 61508. While IEC 61508 has been ratified for a couple of years now, IEC 62061 is about to be published – just as the finishing touches are being put to ISO 13849-1. And one of the problems is that there are likely to be some areas of conflict and confusion over which standard should be used.

The authors of ISO 13849-1 have set out to clarify the situation, address shortcomings of EN 954-1, embrace new technologies and reflect changes in safety practise.

Methods of calculating risk

For instance, quantitive methods for calculating risk have superseded the qualitive methods of the old standard, thereby bringing ISO 13849-1 more into line with IEC 61508 and IEC 62061. However, there is a suggestion that it seems to have been focused on the needs of large control systems, so is overly involved for simple situations. The worry is that designers of simple systems will ignore the new procedures and continue with the older, simpler ways – or, worse still, stop working to standards altogether.

It has been suggested that this problem has arisen because the committee developing ISO 13849-1 has not had any significant representation from small system builders. This situation is almost inevitable because builders of small systems will often be small companies who do not have sufficient manpower to be able to sit on committees, so committees naturally tend to be overly representative of large companies and their needs.

Throughout 2004 there was considerable public discussion of ISO 13849-1, both in committee meetings and in the media. The situation was such that by the end of the year the Health and Safety Executive (HSE) made its views publicly known.

One of the key points picked up on was the potential conflict between ISO 13849-1 and ISO 62061. It was felt that there was a real danger of the two standards being very different, yet apparently both applicable in at least some situations. The result of this could be designers trying to satisfy conflicting demands or choosing to use one standard and ignoring the other.

Identical guidance

However, the solution looks like being that both standards include identical guidance on which standard to use, based on a quantitive analysis of the proposed machine and its likely working environment.

Asked how engineers should proceed until the new standards are ratified, the HSE suggested using the existing standards for the time being. Further it suggested that EN 954-1 should be used for low complexity electrical/electronic systems and for machines using non-electrical technologies such as hydraulics and pneumatics, while IEC 62061 should be used for complex/programmable machines when it is published in the middle of 2005. Meanwhile, the umbrella standard IEC 61508 remains valid, of course.

In conclusion, the advice seems to be to carry on as you are, working to either EN 954-1 or IEC 61508 as appropriate.

When IEC 62061 is published, this could be a more straightforward option than IEC 61508 for those working with more complex machinery. If you believe that you can justifiably carry on working with EN 954-1 for now, then do so.

However, you will have no option but to switch to ISO 13849-1 when it is published – and that may mean you have to seek help from experts, unless you can get appropriate training and bring the required competencies in-house. Either way, you would be wise to build-in the budgetary requirements now. ■

Table 1. How the standards relate to each other

Standard	Title	Status	Comments
BS EN 954-1:1997	Safety of machinery. Safety related parts of control systems. General principles for design.	Current, but work in progress on its replacement.	BS equivalent to EN 954-1:1996. Soon to be replaced by new ISO 13849-1.
prEN 954-2	Safety of machinery. Safety related parts of control systems. Validation.	Draft; not being developed any further.	Originally intended to complement EN 954-1, but development of the draft ceased when it became apparent that EN 954-1 was to be replaced by the new ISO 13849-1.
PD CR 954-100:1999	Safety of machinery. Safety-related parts of control systems. Guide on the use and application of EN 954-1:1996.	Current (but only a Published Document, which does not have the same status as a standard).	Guide to use and application of EN 954-1:1996, but will become obsolete when EN 954-1 is replaced.
BS EN 61508 (in seven parts, all dated 2002)	Functional safety of electrical/electronic/programmable electronic safety-related systems.	Current.	BS equivalent to IEC 61508. Made up of seven parts. More applicable to complex machinery than EN 954-1.
IEC 62061	Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems.	First edition now being printed; expected to be available imminently.	A daughter standard to IEC 61508, specifically for the machinery sector. More applicable to complex machinery than EN 954-1.
ISO/DIS 13849-1	Safety of machinery, Safety related parts of control systems, General principles for design.	Latest draft has been voted on. Publication now anticipated in 2005.	Usually referred to simply as the new ISO 13849-1; the planned replacement for EN 954-1:1996 and ISO 13849:1999.
ISO 13849-1:1999	Safety of machinery, Safety related parts of control systems, General principles for design.	Under revision.	ISO equivalent of EN 954-1 1996; to be replaced by ISO/DIS 13849-1 when it is published.
BS EN ISO 13849-2:2003	Safety of machinery. Safety-related parts of control systems. Validation.	Current.	The BS equivalent of ISO 13849-2; the validation part of the new ISO 13849-1. Could conflict with new ISO 13849-1 when published.

Machine control combines speed and flexibility

The PacDrive machine control system from Elau has allowed German vertical form-fill-seal machinery manufacturer Hassia-Redatron to combine quick size and product change with high output on its latest range of baggers, capable of speeds in excess of 300 a minute from a twin tube arrangement.

"It is generally a contradiction in terms to equip machines so that they combine maximum output with maximum flexibility," says Andreas Hollmann, ffs machine sales manager at Hassia-Redatron.

He explains that the company needed improved controls and drive so that machines could be programmed by the user quickly and simply, in response to shortening product life cycles within the food industry in particular.

Specific objectives were to increase machine availability at the control engineering level by choosing standard modules for logic and motion control; to create a consistent control concept based on the existing HMI interface; and to use standardised programming languages.

Hassia-Redatron's new machines grew from the demands of a confectionery manufacturer that needed to increase capacity, but had no space for a second bagging line or a twin machine – two units in an extended frame. So the company developed the ContiBag 40/26 duplex, which is equipped with two filling tubes on a single unit.

Twin tube bagger: *ContiBag 40/26 duplex*

As standard, the ContiBag 40/26 runs at 150 packs a minute and, while the duplex is aimed at a speed of 300 a minute, it has already been run in trials at a speed of 2 x 190 a minute.

For flexibility, the ContiBag machines can be operated either intermittently or continuously at high speed. Servo motor control for all axes, including the sealing pressure, is said to provide consistently reliable sealing of all film materials under varying conditions.

Hassia-Redatron has also equipped its FlexiBag 40/26 intermittent machine with a control package from Elau, providing the flexibility for quick changeover for a range of films and pack sizes up to 260mm wide and 400mm long.

Elau points out that since a number of programming modules are already available for its PacDrive system, machinery manufacturers can produce their own programmes quickly.

"So many modules have already been programmed in advance that the machine manufacturer generally needs less than one month to create a standard programme of his own for his models. Start-up takes less than one week and new customer-specific requirements can often be met in less than one day," says the company.

Andreas Hollmann at Hassia-Redatron concurs. "The Elau ffs machine technology package solves the problems of axis synchronisation and sealing element pressure control. Our experience to date has shown that it is likely to be possible to shorten the time required for program start-up by 50 per cent."

T: 0049 9391 6060
E: info@elau.co.uk