

Machinery safety control systems and fluid power



This article is the third of a six-part series providing an overview of requirements, principles, applications and technology for pneumatic and hydraulic safety systems of machinery. On 29 June 2006 the revision of Australia's AS4024.1 Safeguarding of Machinery 1996 was released with new guidelines for fluid power designers that include those for fault consideration and exclusion.

The standard was prepared by the Standards Australia Committee SF-041 and is now known as AS4024.1 2006 Safety of Machinery Series. The new edition has adopted European (EN) and internationally-based (ISO) safety and design standards with some modifications to meet Australia's tough safety practices and regulations.

The edition has been published as a series of 26 parts rather than the single standard previously published. In doing this the committee has cleared the way for simple revisions in the future. When a new edition of a relevant standard becomes available at the international level, it can be adopted and published within the framework of AS4024 with minimum delay.

Part 1502: Design of safety related parts of control systems — Validation has the purpose of confirming the specification and the conformity of the design of safety-related parts of the control system. This includes mechanical, pneumatic, hydraulic and electrical parts, as well as the specified category of control according to the revised AS4024.1 Part 1501. (For more on category of control see part 1 of this series in the April/May 2006 issue).

Validation consists of applying analysis and, if necessary, executing tests, with the results recorded. By undertaking analysis at the design stage, problems can be corrected while they are still relatively easy to correct.

As it is important to check for errors, and particularly for omissions in design, a set of appendices is provided as a guideline. These provide basic safety principles for each of the mechanical, pneumatic, hydraulic and electrical disciplines, well-tried safety principles where

available, well-tried components, fault lists and fault exclusions.

The fault lists are quite comprehensive. For both pneumatics and hydraulics they include directional control valves (DCVs), stop, non-return, quick-action venting, shuttle, flow and pressure valves. Other areas covered include, but are not limited to, pipework, hose assemblies, connectors, sensors, filters and energy storage.

To provide an example, faults listed for consideration for DCVs in the generic tables of part 1502 include change of

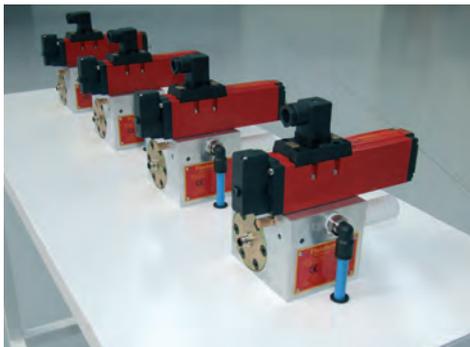
switching times, valve sticking, spontaneous change, leakage and bursting.

If applying to a typical solenoid operated DCV, you would find that no fault exclusion is provided for the first fault consideration, being change of switching times. Therefore, possible causes for change of switching time such as contamination, silting, wear, etc should be considered as well as the effect on the safety function.

A delay in switching time could lead to an extended stopping time of the machine. This has effect on the safe distance between the dangerous part of the machinery and accessible guarding. Especially where light curtains are applied. Depending on several parameters outlined in AS4024, a vertical finger-protection light curtain can be mounted no closer than 200 mm to the dangerous parts if the machine has an overall stop time of 100 ms. However, if the stop time increased to just 300 ms, the safe distance requirement increases to approximately 500 mm, now requiring a second horizontal light curtain to prevent non-detection of an operator between the vertical curtain and hazard.

What does all this safe distance jargon have to do with fluid power safety? A lot! It is a good demonstration of how change in a valve switching time can mean an operator could potentially breach a light guard and have their hand or limb exposed to a hazard before the safe state has been achieved. It is also a good example of where fluid power and electrical safety control systems need to work together and how the validation of the design can identify aspects that have been omitted.

When considering change of switching



time, a designer should consider what the valve stop time needs to be in a fault condition and can it be monitored. Interfacing electrically monitored dual safety valves can provide the best level of safety integrity where solenoid valve switch times need to be monitored for consistency and need to be minimal. They empower the electrical engineer to configure the safety monitoring system to detect if either one of the safety valves takes longer than the predetermined safe time to close on every cycle and prevent further valve operation until the fault is rectified. Correctly integrated, this type of solution can comply with the performance requirements of up to and including category 4 control systems. Of course a quality fluid supply with appropriate filtering and a regular maintenance program are also essential for general fluid power control reliability.

As per Part 1502, to demonstrate use of well tried safety principles required for categories 1 to 4 control systems, an electrical monitoring function requires positive mechanically linked contacts with positive mode operation and no undefined states. The functionality and potential failure mode orientation of a standard inductive sensor is

not recognised as a well-tryed safety principle and therefore should not be used for monitoring of a safety-related valve.

According to the standard, validation should be carried out by persons who are independent of the design of the safety-related parts, but does not necessarily mean that a third-party test is required. Competent personnel should be used in each part of the validation for mechanical, pneumatic, hydraulic and electrical systems.

Because design guidelines can sometimes be shortcut at installation, validation of safety control system designs does not remove the need for thorough final testing. Functional testing of a safety control system should always be carried out, inclusive of ensuring its ability to detect faults as required.

It is also commonsense not to exclude a fault if it is reasonably foreseeable that it could occur within the specific design or environment it is being applied to, regardless of whether there is a related fault exclusion listed within the generic tables of Part 1502.

To obtain a copy of AS4024.1 2006 Safety of Machinery Series, contact Standards Australia on 1300 65 46 46.

Written By David Shead, operations manager and Murray Hodges, director of Fluidsentry Pty Ltd. Murray is a member of the SF-041 Technical Committee for AS4024.1 Safeguarding of Machinery and is the fluid power design representative for the Safety & Environmental Risk Consultants of Australia.

*Fluidsentry Pty Ltd
www.fluidsentry.com*

