

CONTROL RELIABILITY – Beyond the wire

Picture this - your company has mandated that safety is priority one and that all new machinery must include the latest in safety equipment. Suppose the next purchase is a two-hand operator station for an automated assembly machine that incorporates a pneumatic cylinder that extends for parts hold down and that this hold down could put the operator's hands at risk. The electrical output of the two-hand unit is wired to a single solenoid directional valve that causes the cylinder to extend and clamp when the solenoid is powered and causes the cylinder to retract upon removal of power. If the operator does not maintain contact with both of the palm buttons the cylinder will retract. Does your system require additional optimization?

For example, assume that the operator has depressed both electronic palm buttons to initiate the machine cycle and then notices that the part is not positioned correctly. Attempting to reposition the part, he lets go of the buttons which should retract the cylinder away from the hold position. However, the directional valve for some unknown reason does not return to the normally-closed position. Even though the operator has let go of the button, the cylinder will continue to extend creating the potential that the operator's hand may be injured.

When designing a circuit, the entire system, pneumatic as well as electronic, should be evaluated to minimize exposure to unnecessary risk. The control system as defined by a number of standards (including the ANSI Z244 and B11.19 lockout and machine guarding standards) includes not only the input, sensing, and interlock devices but also the output devices such as pneumatic and hydraulic valves. A properly specified safety system would include provisions for pneumatic valves, including:

- Must be redundant in function
- Must be self-monitoring and locking, without any dependency on external machine control or safety circuitry
- Must "fail" to a safe position
- Should have a dedicated, specific function reset input and prohibit reset by removal or re-application of pneumatic, hydraulic, or electrical power
- Must not be able to be automatically reset if the solenoids are energized.

These "critical application valves" have existed in the marketplace for years, but have remained relatively unheard of except in a few select industries where control reliability requirements were first initiated, such as stamping presses. The principle of these "double valves" is to provide dual internal functions (redundancy) so that an abnormal function of one side of the valve does not interfere with the overall normal intended function of the complete valve. At the same time, these double valves sense the abnormal operation in either side of the valve and then inhibit further operation until the problem is corrected and the valve has been deliberately reset. This sensing and inhibiting function is commonly referred to as monitoring. Is it appropriate that this critical function be performed using two standard air valves in parallel or in series? NO! By simply incorporating two standard air valves into the circuit, there is no provision to sense the abnormal operation of one side of the valve or, even more preferable, diminished performance, i.e. slowness/sticking. In addition, there is also no provision for inhibiting further operation of the circuit until repaired. Then, if one valve actuates abnormally, the second one continues to function and redundancy is lost. The circuit doesn't recognize that redundancy has been lost nor does it stop operation to put everyone on notice that redundancy has been compromised. Then, if the second valve also actuates abnormally, there is no "back up" and a hazardous condition may exist.

Applications for these critical application valves exist anytime reliability is an issue for either hydraulic or pneumatic equipment. Typical applications would include E-stop, two-hand-control, light curtains, safety gates, pneumatic locking devices for safety gates, hydraulic brakes, air brakes, amusement rides, hoists, elevators, pinch point applications, or any other application where control system integrity is dependent upon valve operation.

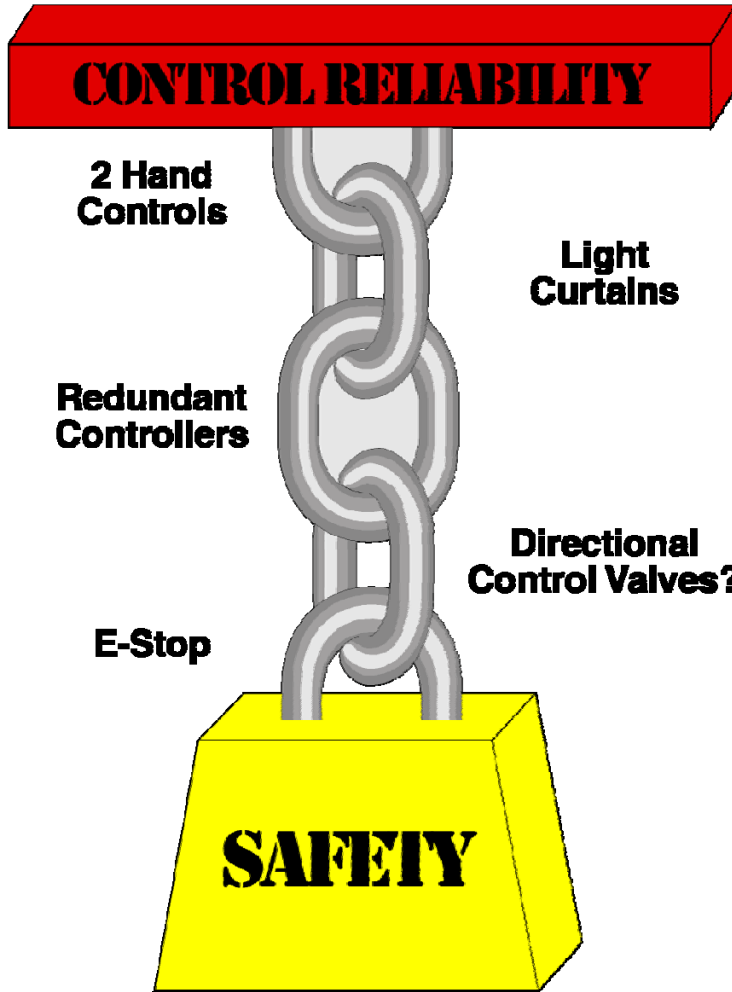
Another area where these critical application valves are used is in LOTO (Lock-Out/ Tag-Out). In many cases, a single point lockout (SPLO) device is used for complete energy isolation. The use of a SPLO device simplifies the lockout procedure. This is particularly true for applications where an employee may need to make numerous entries into an area requiring him to lock out three or four energy sources, e.g. pneumatic, hydraulic, and electrical sources. In some instances, the lockout procedure can take longer than the task that needs to be performed, a situation that discourages personnel from applying good LOTO practices. Incorporating a control reliable circuit with critical application devices into the main power disconnect will help to ensure that all of the potential hazardous energy (electrical, pneumatic, hydraulic, steam, and other forms of power) is isolated and only requires the employee to place one lock on the system when performing routine operations. Also, a control-reliable safety system is required when alternative methods are used during setup or other tasks requiring partial de-energization of a power source. *Please note that SPLO must only be used for tasks that are routine, repetitive, and integral to production, not for other maintenance procedures where a full lock-out of the system is required. Also, the decision to integrate a SPLO system must be based on a complete and thorough risk assessment of the entire system. Integrating a SPLO device should be considered as an addition to a Lock-Out/Tag-Out system, not as a replacement.*

In reviewing energy isolation in the past, most controls were designed to protect the operator. However, more than 50% of accidents happen during maintenance. Since the maintenance worker has less exposure time to the machine and a greater or equal accident percentage, this means that the potential for injury is actually higher for maintenance personnel than for operators. The National Institute for Occupational Safety and Health (NIOSH) states in its ALERT: ([NIOSH publication no. 99-110](#)), “Warning! Workers who install or service equipment and systems may be injured or killed by the uncontrolled release of hazardous energy.”

In order to design a control reliable circuit, the engineer must be able to break the reliability chain into links. Each link must represent a control device that meets control reliability, having the specifications listed above. If the device does not meet all of these criteria, it is not considered a control device but only a component for integration into a circuit, thus requiring re-design for control reliability.

Updating your system is not difficult if your electrical controls are already control reliable. Since some valves have all of the monitoring logic built right in, there is no need to modify the existing external control circuitry for valve monitoring. You simply replace your existing pneumatic or hydraulic valve with a critical application valve and wire it into your existing system accordingly. Also, be sure to incorporate a key operated reset switch.

So, the next time you design a circuit, remember that the ANSI, OSHA, CE, and consensus standards apply to the *entire* control circuit from beginning to end and you will not break the chain.



Consistent Control Reliability:

Are your pneumatic/hydraulic controls consistent with control reliability required by the circuit?

Let's look at an example of why two standard valves will not comply with the requirements for control reliability. In Figure A you see two valves connected in series. Either valve will exhaust the air from downstream. Both solenoids must be energized as seen in figure B for air to get to the outlet.

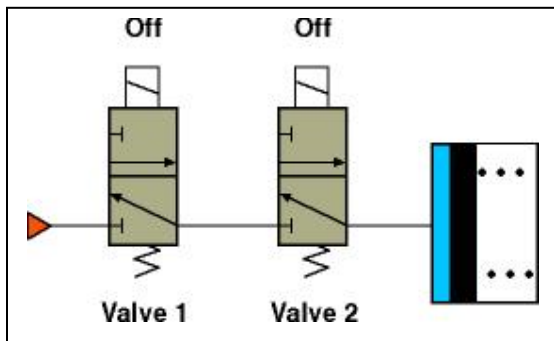


Figure A

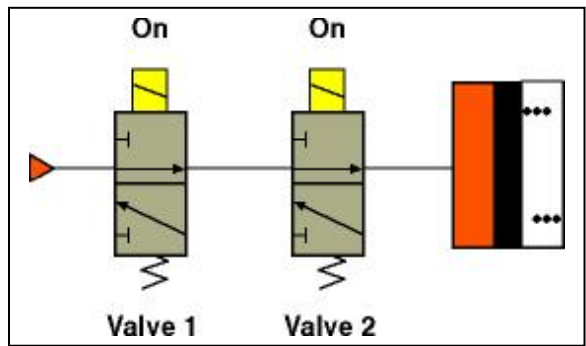
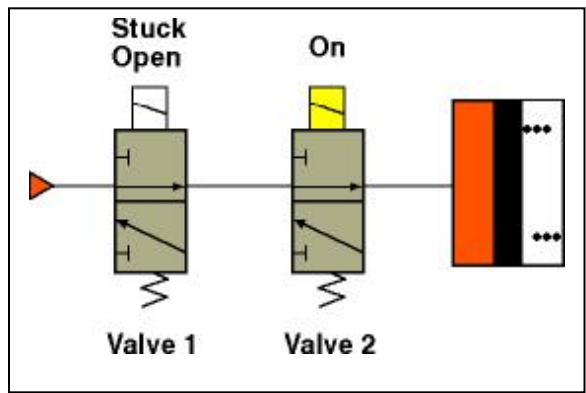
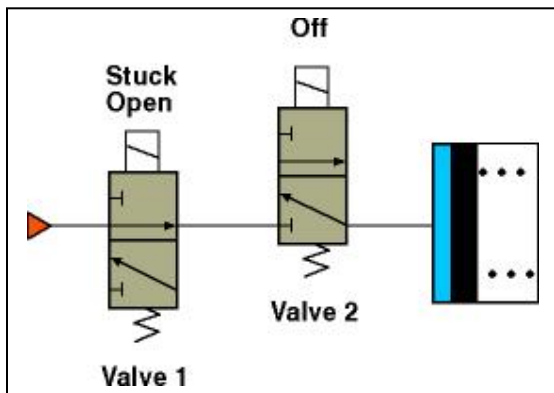


Figure B

But, let's take a look at what would happen if the first valve stuck in the "on" mode. You will see in Figures C and D that the second valve now has full control of the circuit and as long as it continues to operate, the system would appear to be functioning. The first valve has become nothing more than a piece of pipe and all system control is transferred to valve 2. But, the redundancy feature has been lost and if anything happens to valve 2, there is no other backup.



If a critical application valve were used instead of these two standard valves, the abnormal operation of the first valve section (valve 1) would be sensed and the valve would automatically lock itself out preventing further operation until repaired.

For more information, please contact one of the following Global Safety Team members:

Dan Henman- 249-764-1802
dan.henman@rosscontrols.com

Eric Cummings- 803-622-1161
eric.cummings@rosscontrols.com

Steve Boyette- 706-356-3730
steve.boyette@rosscontrols.com

Customer Service- 800-438-7677
 Technical Services- 888-835-7677