

Pressure Switch Feedback in a Control Reliable System

By Eric Cummings & Steve Boyette
ROSS Controls® Troy, MI

The most typical application for the DM²® Series C and E valves is that of solenoid dump valve for air entry energy isolation. When a safety event occurs, such as the opening of a guard door or the operation of an E-stop device, these valves will exhaust the downstream pressure in the system removing the pneumatic energy.

There are two questions that frequently come up when it comes to the integration of this valve in a safety system.

1. Why doesn't the valve have two feedback switches for monitoring by the safety system?
2. How should I monitor the downstream pressure within my safety system?

To answer these two questions, some information about the valves' function is required. The DM²® Series valves are redundant, self-monitored devices in which both independent elements must function within a specific time frame of each other. This time frame is limited to less than 150 ms by ROSS design criteria at the rated pressures of the valve. This time will vary with valve size and supply pressure but must remain below 150 ms. If the valve were to operate abnormally due to an element not functioning synchronously with the other element within this time frame, the valve will default to its exhaust condition. It will remain in that position until the main solenoids are de-energized and the independent reset solenoid is given a pulse signal. The valve is third-party certified to ISO 13849-1 Category 4 PLe as a safety device by the German BG-Prüfzert.

These valves have a single pressure switch that functions as a status indicator. The status indicator informs the machine controls that the valve is in an "operational" state or a "non-operational" state. Operational meaning that the valve has pressure supplied to it and the valve does not currently need to be reset.

The status indicator is not related to the inherent safety function of the valve and is not required for the ISO 13849-1 Category 4 PLe certification. It is strictly a diagnostic device for use in an EDM (external device monitoring) system.

Because the valve has the redundancy, monitoring, and cross-checking internal to it and the status indicator pressure switch is not part of the safety function of the valve, there is clearly no need for two valve position sensing switches. The status indicator pressure switch simply provides a NO (normally open) and NC (normally closed) contact to indicate that the valve is ready to run. The switch will not change state each time the valve is energized or de-energized. So, there is no need to track the function of this switch versus the signals to the valve.

This brings up a secondary question of "What if the status indicator pressure switch fails to change state?" To answer this we must think through the foreseeable failure modes of the switch. There are two potential conditions.

The first scenario is that the valve is actually in the "ready-to-run" condition, but the switch says that the valve is in a faulted state. The EDM system should see the switch indicating that the valve is in the "not-ready-to-run" condition and extinguish any run signals to the valve such that the mistaken "fault" can be addressed. If the valve were already energized prior to the system checking the status indicator, a properly designed safety control system would signal to de-energize the valve and exhaust downstream pressure. If the valve were not already energized, disabling the run signals would only prevent energizing from occurring. Thus, the valve would be held in the exhaust mode.

The second case is that the valve is in a faulted state but the switch indicates that the valve is ready to run. In this case there would be no downstream pressure as the valve would be in its default exhaust condition and latched into that condition requiring a reset signal for further operation. The safety function of the pneumatics has not been compromised in this situation.

With that understanding of the function of the valve and status indicator switch we can better answer the second question regarding the monitoring of downstream pressure. In order to monitor the downstream pressure for a zero energy state, the downstream pressure condition should match the run signals applied to the valve. Also, the valve should always be sized to supply enough air for the machine processes downstream of the valve and, more importantly, to be able to exhaust downstream air in a rapid manner. The importance of sizing for exhaust is that the time it takes to exhaust a machine or zone is a function of downstream pressure, volume, and the flow rate of the valve. If the pneumatic circuit is unable to rapidly and safely exhaust downstream pressure, the circuit can remain temporarily 'energized' even after upstream pressure is blocked and the exhausting of downstream pressure begins.

The use of a control reliable type valve, such as the DM²® Series, maintains the safety integrity of the pneumatic circuit by helping to assure that both the upstream pressure is blocked and the downstream pressures are de-energized when the circuit is in a faulted or inoperable state. Inherent in the name, a 'control reliable valve' provides a level of reliability, or "assurance", that the valve will shut-off and exhaust downstream pressure when signaled to do so. In the event that the valve suffers an abnormal condition, control reliable valves default to the safest condition; namely, to exhaust downstream air pressure. When used in conjunction with sensing type devices such as light curtains, scanners, safety mats, E-stops, safety gate switches, etc., control reliable valves provide the highest level of reliability for shutting off the supply of air and exhausting the downstream pressure.

In a typical OSHA-compliant application incorporating electrical and mechanical interlocks and interrupts, a control reliable pneumatic valve is an integral part of the safeguards designed to stop the machine operation. Sensor type devices do not physically prevent access to the machinery, but may rather interrupt the electrical supply and can provide an alert if the containment area has been violated. Therefore, when concerned with ultimately ensuring stoppage of a hazardous air-powered device, the key question is the control reliability of the final control element, that being the valve. When there are no other contingencies for stopping motion there is no point in monitoring downstream pressure. The operator has already entered the sensing area and the control logic and exhaust valve would have already operated regardless of any extra monitoring of pressure.

Monitoring downstream air pressure is only truly useful for safety when utilizing barrier guards with solenoid locks. If using light curtains or safety mats, there is no recourse if the downstream pressure signal does not match the run signals on the valve because there is no physical barrier to prevent access to the hazard area. Also, the speed of exhausting may be critical when performing stop distance calculations.

If the system utilizes barrier guards with solenoid locks you must monitor the downstream pressure in order to determine whether to allow the solenoid locks to release the barrier guard. Having a control-reliable valve within this system ensures the pressure in the system is being released, whereas, a downstream switch verifies that the volume of air was released. This is especially important if there is a significant volume of air which may take time to be released. In this case a malfunctioning switch could lead to confusion in the safety system that could allow access prior to a safe state being reached. In this scenario, controls engineers should use redundancy in monitoring that pressure. This is the only redundant way to ensure that energy is released prior to the door unlocking.

Additional resources

For extended information related to products in this article, please download Digest Catalog 105, Safety Bulletin 510 or contact your local ROSS distributor.

Also, please visit the safety page at www.rosscontrols.com.

