CONNECTING and INTERPRETING LIMIT SWITCHES

© Walter Driedger, P. Eng., 2000 May 20. walter(at)driedger(dot)ca
First published in *Intech,* January 1993 as "Limit Switches Key to Valve Reliability"
This Adobe® file is available for download at http://www.driedger.ca/.

INTRODUCTION. There is a great variety of possible combinations for installing and connecting limit switches on valves. The number of switches depends on the particular control objective and may be influenced by redundancy considerations. The way they are connected depends on the safety and reliability requirements.

In order to clarify this discussion, diagrams like Figure 1 will be used. All signals, switch positions, etc. are shown with the valve at the center of travel. No limit switches are actuated, all are shown in their shelf position as determined by their internal springs. Imagine the valve to be like a guillotine where the stem travels upward to open the valve and downwards to close it.

The limit switch that is actuated when the valve is fully open is labeled ZSO. The one at the extreme opposite end is labeled ZSC.

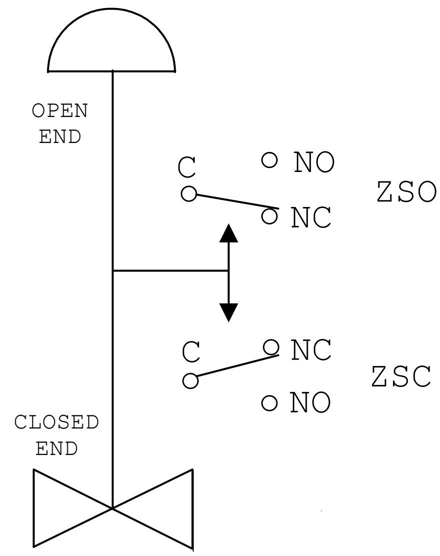

Figure 1 Limit Switch Symbols

The terminals on the electrical switches are labeled Common (C), Normally Open (NO), and Normally Closed (NC). This unfortunate choice of terminology has nothing to do with the state of the valve nor even the "normal" position of the switch. It refers to the state of the switch when nothing is pushing on it.

SINGLE SWITCH, DIRECT APPROACH. A single limit switch at the OPEN end of the valve (ZSO), as shown in Figure 2, will tell us when the valve is fully open. It cannot tell us if the valve is fully closed. The problem is that the term "open" is a bit ambiguous. Question: Is a half-open valve open, closed, neither open nor closed, or both open and closed? This discussion will use the following definitions:

OPEN	=	Partly or fully OPEN
CLOSED	=	Partly or fully CLOSED
Not OPEN	=	Fully CLOSED
Not CLOSED	=	Fully OPEN

According to these definitions the half-open valve is both open and closed. A single ZSO switch can only tell us if the valve is "fully open" and "not closed". It cannot tell us if the valve is partly open.

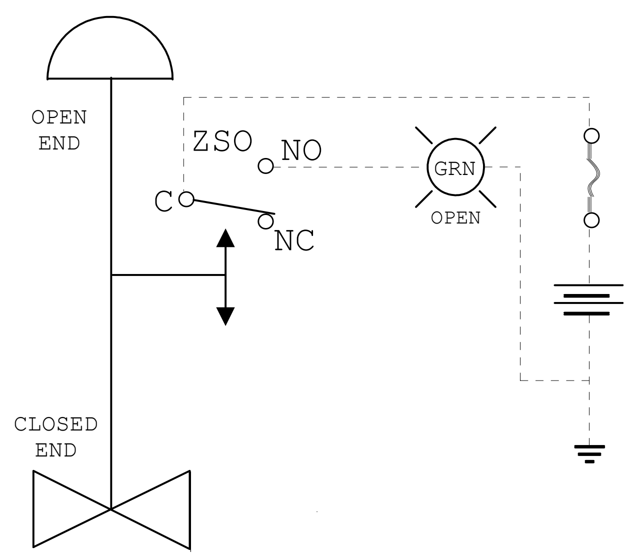

Figure 2 Single Switch, Direct Approach

Example 1: We need a limit switch and a status light to tell the operator that the fuel gas to a furnace is OPEN. If so, it is not safe to begin the light-off sequence. A ZSC switch at the closed end of travel is used so that we can be sure the valve is "fully closed" and "not open" even a little bit. The correct contact is NC. If the valve is even the slightest bit open, the OPEN light comes on.

Example 2: We need a limit switch and a status light to tell the operator that the fuel gas to a furnace is CLOSED. If so, it is safe to begin the light-off sequence. This is exactly the same limit switch as before: ZSC. We want to know if the valve is "fully closed". The only difference is that Example 1 uses the NC contact of the switch to turn off an OPEN light when the valve is fully closed while Example 2 uses the NO contact to turn on a CLOSED light when the valve is fully closed.

SINGLE SWITCH, FAILSAFE. "Failsafe" is a much abused word. It is very dramatic because it combines the apparently contradictory concepts of failure and safety in a single word. The reality is not so dramatic. It means that the failure of a component is unlikely to cause any harm. The formal definition I prefer is:

> **A FAILSAFE design is one in which**
> **the most probable failure mode results in**
> **the most probably safe condition.**

Note that there are several "probablies" in this definition. Failsafe design is a technique for stacking the deck in favor of safety. It does not guarantee safety but it makes it more probable. The Examples 1 and 2, above, accomplish exactly the same thing. The difference is in the behaviour of the two methods when failures occur. Table 1 shows all the possible modes of failure. All those failure modes marked "*" result in the bulb failing to light. The most probable failures are marked "+".

+	*	1.	Power fail or blown fuse
+	*	2.	Power wire open circuit
	*	3.	Power wire short circuit to ground or neutral
		4.	Limit switch fails to depress
		5.	Limit switch fails to return
+	*	6.	Limit switch fails as open circuit
		7.	Limit switch fails as short circuit
	*	8.	Limit switch short circuit to ground or neutral
+	*	9.	Signal wire open circuit
		10.	Signal wire shorts to power
	*	11.	Signal wire shorts to ground or neutral
+	*	12.	Bulb burnt out
+	*	13.	Bulb neutral open circuit
	*	14.	Bulb neutral short circuit to power

Table 1. Failure Modes of a Valve Status Light

For an arrangement like that of Example 1, there are eleven failures that would lead the operator to believe that the valve is not OPEN and to proceed to light the furnace. An explosion could result. Of these 11 possible failures, 6 have high probability. This would not be a failsafe arrangement!

If the circuit is arranged as in Example 2 and any of the above mentioned eleven failures occurred, the operator would conclude that the valve is not CLOSED and would attempt to close the valve. The CLOSED light would still not come on. He would then, we hope, call maintenance to find the cause of the problem. Of the two possible circuits, Example 2 is the one that is most probably safe.

In the case of Example 2, only failures 5, 7, and 10 could give the operator unsafe information. Note that these three are all low probability failures.

5. Limit switch fails to return
7. Limit switch fails as short circuit
10. Signal wire shorts to power

Thus we have eleven safe failures and three unsafe failures. All the most probable failures result in the same safe response: The operator does not attempt to light the furnace. Example 2 is a failsafe arrangement. The odds in favor of safety are greatly improved.

DOUBLE SWITCH, DIRECT APPROACH. Often it is necessary to be certain that a valve is either fully open or fully closed. The suction valve to a compressor must be fully open when the machine is being operated and it must be fully closed during an emergency. Two limit switches are required to provide this information. Figure 3 shows these arranged using direct wiring. The two limit switches have four combinations of states, as shown in Table 2 which also shows that there are 11 single failures that would lead an operator, or a logic system, to believe that the valve was stuck in transit. Only three of the fourteen possible failures are identified to the operator or logic system.

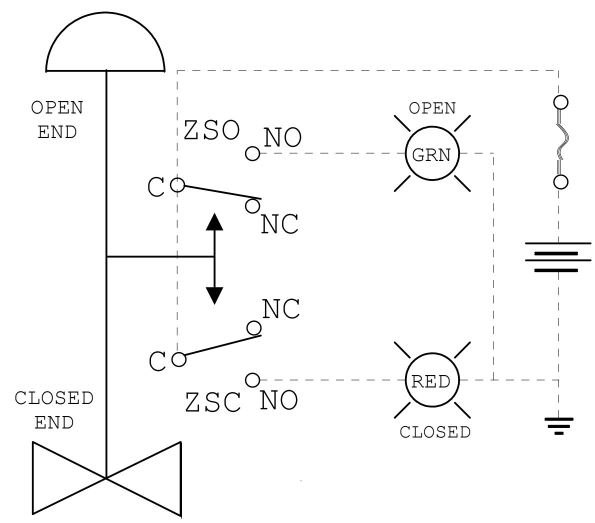

Figure 3 Two Switches, Direct Approach

OPEN light	CLOSED light	Interpretation of Lights	Causes of Error
on	off	The valve is fully open	none
off	on	The valve is fully closed	none
off	off	The valve is in transit	11 causes
on	on	There is a failure	3 causes

Table 2. Direct Approach Status Light Interpretation

DOUBLE SWITCH, FAILSAFE. Figure 4 shows the failsafe arrangement that provides the same information. Note that NC contacts are used instead of NO and that each light is connected to the opposite limit switch. The double negative makes a positive. Table 3 shows the interpretation of the lights. It shows that eleven of the fourteen failures could be identified by an operator or a logic system as signal failures. Three of the failures would give a misleading, and possibly unsafe, impression.

It is instructive to watch the status lights of a bank of valves undergoing test. The failsafe arrangement always has at least one light on for every valve. The lights begin all red. When the OPEN button is pushed and the valves begin to move, all the green lights come on as well. Then, as the valves complete their stroke, the red lights blink off one by one. At no time is the operator blind. The difference between a stuck valve and a signal failure is very evident.

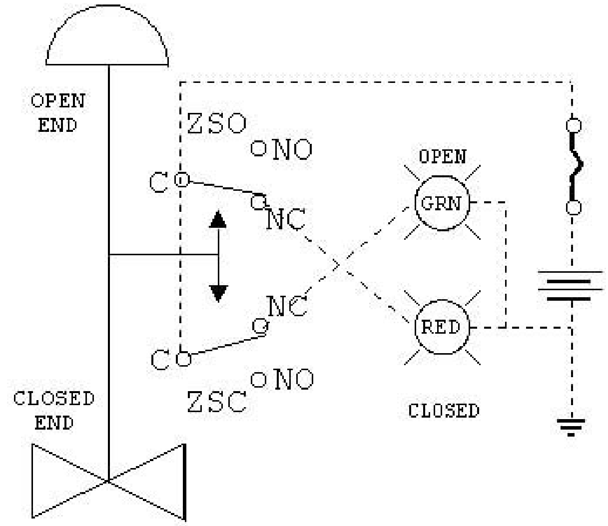

Figure 4 - Two limit Switches Failsafe

Figure 4 Two limit Switches Failsafe

OPEN light	CLOSED light	Interpretation of Lights	Causes of Error
on	off	The valve is fully open	none
off	on	The valve is fully closed	none
off	off	There is a failure	11 causes
on	on	The valve is in transit	3 causes

Table 3. Failsafe Status Light Interpretation

The same test carried out with direct wiring begins the same: All lights are red. Then the lights go out! Finally the greens come on one-by-one. There is an interval during which the operator is left entirely in the dark. A demonstration program, ZSC-101.exe, showing how the switches and lights work in practice is available for download at the end of this page.

TWIN, DOUBLE LIMIT SWITCHES. The failsafe approach to signal wiring has one serious drawback: Failures interfere with the normal operation of the plant. The fundamental attitude that is being embodied in the wiring is "If in doubt, shut down!" This is certainly the safest attitude but it is also the one that makes the plant least reliable from the operations point of view.

There are also circumstances when there is no obvious safe response. Consider a single engine aircraft in flight over the sea. There is an engine oil low pressure indication. There is also some doubt that the signal is correct. What is the safest response? Now consider the same situation with a twin engine plane.

Redundancy provides a way to resolve uncertainty. The off/off state of the double limit switch, failsafe arrangement clearly indicates that there is a signal failure. The use of twin limit switches at each end of the valve provides additional information so that the state of the valve can still be determined with some degree of certainty.

Four limit switches have sixteen possible combinations of states. Each has one of four possible interpretations. Table 4 lists all the states and the most appropriate interpretation of each one. Assume that the state has been stable for some time and that valve movement has ceased.

ZSO A B	ZSC A B	State Name	Failures
off off	on on	OPEN	none
on on	off off	CLOSED	none
on on	on on	TRANSIT	none
off off	off off	BAD SIGNAL	at least two unknown
off off	off on	OPEN	one, ZSC-A open circuit
off off	on off	OPEN	one, ZSC-B open circuit
off on	off off	CLOSED	one, ZSO-A open circuit
on off	off off	CLOSED	one, ZSO-B open circuit
off on	on on	TRANSIT	one, ZSO-A not switched
on off	on on	TRANSIT	one, ZSO-B not switched
on on	off on	TRANSIT	one, ZSC-A not switched
on on	on off	TRANSIT	one, ZSC-B not switched
off on	off on	BAD SIGNAL	two, one in each pair
off on	on off	BAD SIGNAL	two, one in each pair
on off	off on	BAD SIGNAL	two, one in each pair
on off	on off	BAD SIGNAL	two, one in each pair

Table 4 Twin / Double Interpretations

This arrangement is in essence a three-out-of-four voting scheme. It is totally immune to single failures and can still determine the correct state of the valve despite several forms of double failures. Let us examine several examples of possible states.

ZSO ZSC
A B A B

off off, on on.
OPEN

In this state both ZSO switches agree that the valve is fully open and both ZSC switches agree the valve is at least partly open. If the valve were actually CLOSED, four failures would be required to give this result. If the valve were still in TRANSIT, two failures would be required to give this signal.

off off, off on
OPEN, one error

In this state both ZSO switches agree that the valve is fully open but one of the ZSCs indicates that it is closed. There are three possibilities:

OPEN	with one open circuit
CLOSED	with two open circuits and one bad limit switch

TRANSIT	with three open circuits

Since two failures are improbable and three are extremely improbable, it can be reliably concluded that the valve is OPEN.

on off, on on
TRANSIT

This is a transitional state that occurs when one limit switch opens before the other. If the state persists it could mean the valve is:

TRANSIT	valve is stuck half-open with one open circuit
OPEN	with one bad limit switch
CLOSED	with one bad circuit and two bad limit switches.

A fully failsafe design would consider this state to be TRANSIT and respond accordingly after the allowable transit time had elapsed. If it is not essential to safety that the valve be fully open, the OPEN interpretation can be used.

off on, off on
BAD SIGNAL

This state cannot be resolved. Both ZSOs and both ZSCs flatly disagree with each other. It is probable that ZSO-A and ZSC-A, which should both be on the same fuse, have lost power and that the valve is actually in TRANSIT. If the valve persists in this state, that is one more failure. The proper failsafe response to this signal is to assume the valve is in the wrong state and take the appropriate action.

To make certain that a common mode failure does not cause the two errors that could cause a false reading, the circuits must be arranged so that an A switch circuit does not share a common component with its corresponding B switch. Note that it is acceptable for the two A switches to share components. For maximum reliability as well as failsafe response the following should occur in A/B pairs:

- Conduits to the limit switches
- Field junction boxes
- Home run cables
- DCS or PLC I/O modules

A single PLC or DCS processor will be needed to resolve the logic but this unit should have an on-line backup. Note that the use of redundant I/O modules in the PLC or DCS contributes very little safety. On the contrary, it detracts from the reliability by adding more components that can fail. We already have three out of four voting. To duplicate the input modules would result in eight input channels for a single piece of information. Questions: Which is safer, a four engine or an eight engine aircraft? Which is more reliable? This argument goes triple for triple modular redundant (TMR) systems.

Every state that is not one of the three "perfect" states is alarmed so that maintenance can be performed. As long as this is done before a second failure occurs, a nuisance shutdown of the system can never happen based on a single failure. Double failures are not only improbable but extremely improbable if maintenance responds promptly to the first trouble signals.

THE MOST IMPORTANT THING. This article describes a number of ways of arranging and connecting limit switches and the interpretation of their signals. But always remember **the most important thing** about limit switches before implementing any of these schemes. The most important thing is simply this: **Make certain that the limit switches are solidly, rigidly, immovably mounted.** More limit switch "failures" are due to sloppy mounting than to any other cause. Each one must be individually adjustable and must hold this setting firmly once it is set. If pulling on the conduit can move the switch, it is not firm enough. Better that the wire rip off than that the switch move! Make certain that movement of the valve stem cannot put force on the switch. If ice builds up on the face of a magnetic switch, the valve stem will move the switch. In such cases, enclose the entire assembly in a housing.

DOWNLOAD DEMONSTRATION PROGRAMS. The following files are available for download at http://www.driedger.ca/limitsw/LimitSw.html.

ZSC-101.exe the original DOS version of the valve limit switch demonstration program (45K)

ZSC-102.exe version 2.0, the Windows version of the demo program complete with tutorial and 'tests'. (71K)

ZSC.ico an appropriate icon for the shortcut

Msvbvm50.dll a Microsoft supplied DLL file that need only be downloaded if your computer sends an error message to the effect that the msvbvm50.dll file is missing. This file should be found in C:\Windows\System but has not been installed in all machines. It can also be found at the MS download website but I believer that is a slightly older version. (1316 K).

If you are accessing this web site via your office network, the firewall may block all executable programs. In that case you will have to download it at home and bring it in on a floppy.