XVII International Scientific Conference on Industrial Systems (IS'17)
Novi Sad, Serbia, October 4. – 6. 2017.
University of Novi Sad, Faculty of Technical Sciences,
Department for Industrial Engineering and Management
Available online at http://www.iim.ftn.uns.ac.rs/is17

Failsafe behaviour of basic pneumatic systems

Vule Reljić
(Teac. Ass., Faculty of Technical Sciences, Trg D. Obradovića 6, Novi Sad, Serbia, vuketa90@uns.ac.rs)
Ivana Milenković
(Ass. Prof., Faculty of Technical Sciences, Trg D. Obradovića 6, Novi Sad, Serbia, ivanai@uns.ac.rs)
Dragan Šešlija
(Full Prof., Faculty of Technical Sciences, Trg D. Obradovića 6, Novi Sad, Serbia, seslija@uns.ac.rs)
Slobodan Dudić
(Ass. Prof., Faculty of Technical Sciences, Trg D. Obradovića 6, Novi Sad, Serbia, dudic@uns.ac.rs)

Abstract

Failsafe in engineering encompasses predetermined actions that ensure unsafe consequences of system failure. In the case of compressed air systems, when failure happens system responds in a way that will cause no or minimal harm to other equipment, the environment or to people. The causes of failure could be (a) a loss of air, (b) a loss of signal (either pneumatic or electric) and (c) a loss of solenoid power supply. This paper describes experimental setup of six simple pneumatic circuits and their behaviour in the case of the air and the electricity breakdown. Half of the experiments are realised with the single acting cylinders, and the other half with the double acting cylinders. In addition, all the experiments are repeated, with the integrated compressed air reservoir in the circuits.

Key words: *failsafe, failure, pneumatic systems*

1. INTRODUCTION

Analysis of failed problem-solving efforts enables people to guide subsequent problem solving to avoid similar failures [1]. A system's being "fail-safe" means not that failure is impossible or improbable, but rather that the system's design prevents or mitigates unsafe consequences of the system's failure.

The failsafe algorithm determines the type of faults and enables appropriate failsafe actions depending on the type of faults. Also, failure mode and effects analysis can be used to examine failure situations and recommend safety design of different devices [2].

Some systems can never be made fail safe, as continuous availability is needed. Redundancy, fault tolerance, or recovery procedures are used for these situations (e.g. multiple independent controlled and fuel fed engines). This also makes the system less sensitive for the reliability prediction errors or quality induced uncertainty for the separate items. On the other hand, failure detection and correction and avoidance of common cause failures becomes here increasingly important to ensure system level reliability [3].

2. PNEUMATIC CIRCUIT - EXPERIMENT

Pneumatic actuators need solenoid valves to control the supply of compressed air. This they do by diverting or stopping the supply of compressed air to one side of the piston or vane while allowing for compressed air to be exhausted from the other.

In this paper are described six simple pneumatic circuits. Three of them have single acting cylinder as working element, and the other three have double acting cylinders (Figure 1). Single acting cylinder has diameter 20 mm, and stroke 50 mm. Double acting cylinder also has 20 mm diameter, but 100 mm stroke length.

All cylinders are operated with electro pneumatic (solenoid) valves, either monostable or bistable.

One of the benefits of pneumatic actuators is springs can be used to return a valve to its pre-determined “failsafe” position in the event of failure of:
a) air,
b) signal or
c) solenoid power supply [4].

However it is important to note that the failsafe position might be the last set position.

The magnetic plunger acts directly on the valve seal to open or close the valve orifice depending upon whether the solenoid is energised or de-energised. The pressure and flow capability of this type of solenoid valve depend directly on the orifice size and the coil power. Direct acting solenoid valves are rarely used on their own to control pneumatic actuators as although they can usually handle the pressure, the orifice size restricts the flow rate to the actuator and limits its speed of operation [5].

The failsafe scenarios were examined on all given pneumatic circuits, in two different situations. The first case encompassed examination on the circuits that are directly connected to air supply. In the second set of examinations the compressed air reservoir was added right after air supply, as can be seen in Figure 1. The failsafe scenarios were examined for two different types of failure:

a) loss of electricity,
b) loss of compressed air supply.

3. RESULTS

As can be seen from Figure 1, Circuit I and Circuit II are quite similar. The only difference is in directional control valve. In the first case, directional valve is electrically actuated monostable valve. The main characteristics of this type of valve is that it will go to the initial position in the case of electricity breakdown and cylinder will retract. Should the air fail and the solenoid remain energised then, providing the air from the actuator piston chamber can exhaust back via the supply line, the valve will again move to the pre-determined failsafe position. Should the air pressure decay but not fail completely, a point may be reached where the spring force behind the actuator pistons overcomes the air pressure and the actuator will gradually move. To overcome partial or slow movement a dump valve can be fitted that will exhaust the supply line if the pressure drops below a certain level; the actuator will then move to the pre-determined failsafe position.

On the contrary, cylinder in the Circuit II is actuated by bistable valve. In the case of electricity breakdown, this valve will stay in the position. Therefore, the cylinder will stay in the position.

The actuator will behave in the same way as system 1 when the air fails.

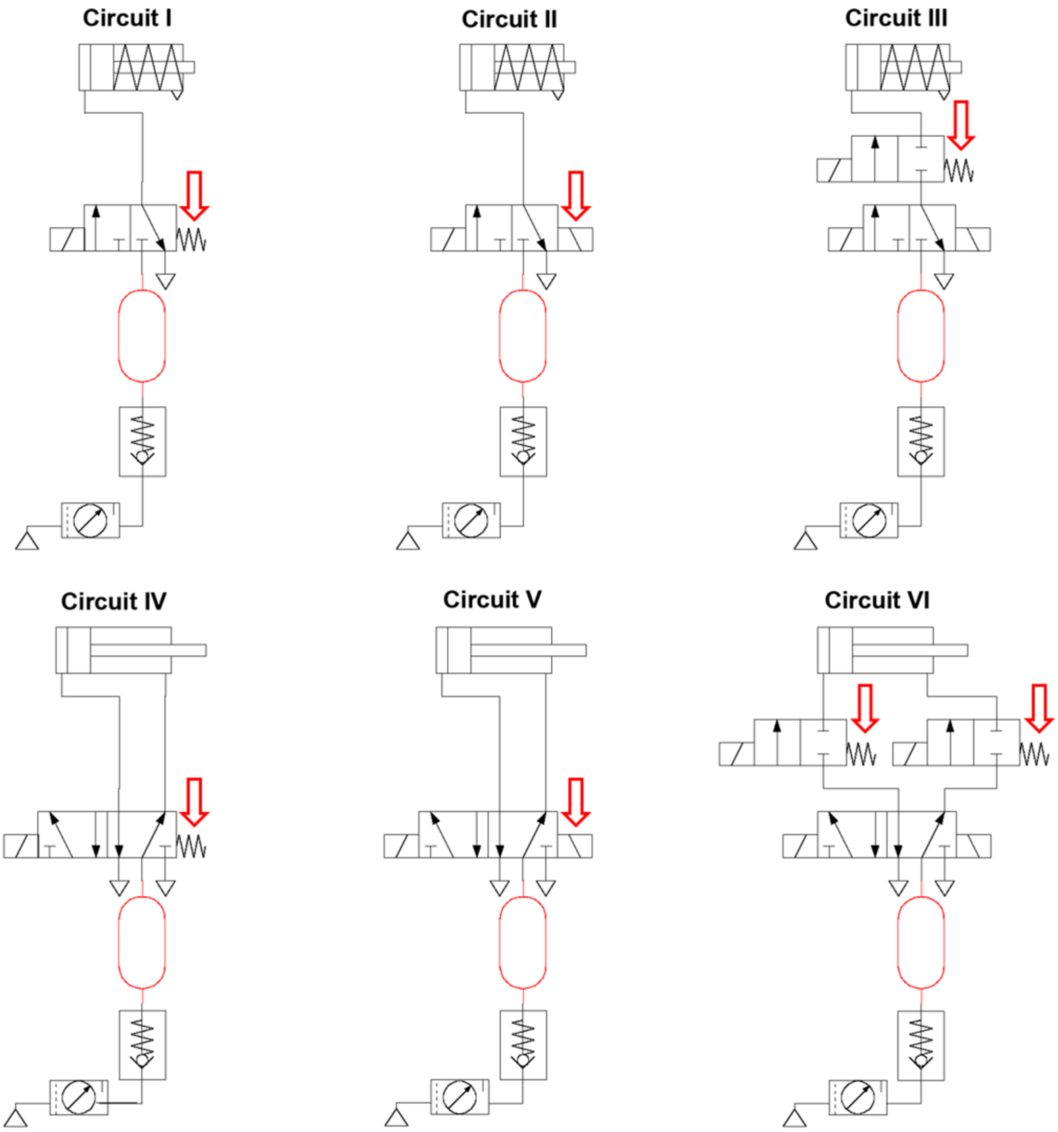

Figure 1. Electro pneumatic circuits for failsafe examination

In the Circuit III additional 2/2 valve was added between cylinder and directional valve. If the air fails the air in the pilot chamber will not be allowed back up the supply line until the additional 2/2 valve is operated.

Both solenoids have to be energised to fill the actuator but nothing will happen when it is de-energised because the additional valve has to be energised before the air will vent from the actuator. The actuator will therefore stay in the position on electrical failure.

The additional valve provides a lock condition trapping air in the actuator if the supply pressure falls below a specified limit. This will cause the actuator to also stay in the position on pneumatic failure. This is the same as “double acting stay in the position” (like Circuit VI) but using a single acting cylinder

Circuit IV shows the most common way of controlling a double acting cylinder. Monostable 5/2 electrically actuated valve was used. When it is energised air fills the piston chamber of the actuator and air from the piston rod chamber is allowed to vent (cylinder extends). When the solenoid is de-energised the process is reversed and the actuator moves in the other direction (cylinder retracts).

If the air is available and the power to the solenoid fails the actuator will either stays in the position, or retracts.

However, if the air fails and there are no significant out of balance forces originating from the valve then the cylinder should stay in the last signalled position.

However, it is important to realise that when a single solenoid control system, such as this, is used, a double acting cylinder will not necessarily stay where it is on electrical failure. This can either be a useful feature or something to be avoided depending on the nature of the application.

Circuit V is widely known double acting stay-in-the position solution. Two solenoids are used. One is energised and the other de-energised to enable cylinder to extracts and the process is reversed to move it in the other direction.

If air is available and the power to both solenoids fails the cylinder will stay in the last signalled position assuming there are no forces acting on the valve to drive the actuator from its rest position.

If the air fails and there are no significant out of balance forces originating from the valve then the actuator should stay in the last signalled position.

Circuit VI is functionally very similar to Circuit 5.

Between cylinder and directional valve were added two monostable, electrically actuated 2/2 valves. Operating together with directional valve, they can execute all the positions like 5/3 valve with blocked central position.

Two solenoids are used. One is energised and the other de-energised to enable cylinder to extracts and the process is reversed to move it in the other direction. Additional valves ensure the third “centre lock” position when both solenoids are de-energised or the power fails. In this third position air is locked in the chambers of the cylinder.

If the supply air fails the actuator will stay in the last signalled position even if there are out of balance forces originating from the valve.

All experiments are repeated with added pneumatic reservoir after the source of compressed air. It is observed that systems behave the same in the case of electrical breakdown, like systems without reservoir.

But, in the case of compressed air breakdown systems continue to work certain number of cycles, depending on cylinder size and the number of other equipment integrated in circuits.

The behaviour of cylinders of each examined pneumatic circuit in the case of breakdown of electricity or compressed air supply is given in Table 1.

Table 1. Cylinders’ responses to various breakdowns

		Electricity breakdown	Compressed air breakdown
Circuit I	without reservoir	retracts	retracts
	with reservoir	retracts	55 cycles without load
Circuit II	without reservoir	stays in the position	stays in the position
	with reservoir	stays in the position	48 cycles without load
Circuit III	without reservoir	stays in the position	stays in the position
	with reservoir	stays in the position	40 cycles without load
Circuit IV	without reservoir	stays in the position or retracts	stays in the position
	with reservoir	stays in the position or retracts	20 cycles without load
Circuit V	without reservoir	stays in the position	stays in the position
	with reservoir	stays in the position	16 cycles without load
Circuit VI	without reservoir	stays in the position	stays in the position
	with reservoir	stays in the position	14 cycles without load

4. CONCLUSION

From previous chapters, it is quite clear that failsafe behaviour of a system is dependent on various factors:

a) the most important part is the nature of a system and the task for which is designed for,
b) the type of components and the type of energy that is needed for their functioning,
c) the way of their installation and integration in the system,
d) nature of possible failures and their interaction.

In order to ensure no or minimal harm to other equipment, the environment or to people, it is possible to apply different strategies:

a) redundancy,
b) fault tolerance,
c) recovery procedures are used for these situations.

However, the most important part is fully understanding of system functioning.

5. REFERENCES

[1] Jang, I., Kim, H., Lee, H. and Han, S. (2007), "*Height control and failsafe algorithm for closed loop air suspension control system*", International conference on control, automation and systems 2007. ICCAS '07 in Seoul, Korea.
[2] Rutherford, B. (1992), "*What Do You Mean - It's Fail-safe?, Part 3*"
[3] Bornschlegl., S. (2012), "*Ready for SIL 4: Modular computers for safety-critical mobile applications*". Mikro Elektronik,
[4] Oexler, G. (2009), "*Pneumatic drives*", Festo Didactic, Germany.
[5] K Controls. (2010), "*Solenoid control of pneumatic actuators*", United Kingdom.