FLOW CONTROL ELECTRO-HYDRAULIC SERVO VALVE ASSEMBLY WITH IN-BUILT AUTOMATIC FAILURE DETECTION AND COMPENSATION

José Javier Álvarez García
Industria de Turbopropulsores, S.A.

Abstract

The main contribution to the overall critical failure rate of an engine control system based on a dual lane digital electronic controller may be attributed to the actuation system. It is usual practice to design the control system such that reversionary or alternative control actions may be introduced in the event of actuator failure. These actions protect the engine from major damage but usually impose a severe restriction in engine modulation and may also involve a quite complex logic and therefore be inherently untrustworthy.

An accepted approach to mitigate these limitations consists in providing redundancy of the weakest point in the actuation system (normally the electro-hydraulic servo valve driving the actuation piston) such that control may be transferred from the failed to the operative component and a similar engine response may be attained by the alternative control.

This paper describes an actuation system, following this approach, which does not require failure detection by the digital electronic controller and minimises undesirable transients by reducing failure detection and reaction times as well as preventing excessively large actuator excursions during the transfer process.

1 Introduction

The use of Digital Electronic Controllers (DEC) as the core of the control system design of jet engines has progressively been increased over the last twenty years. The DECs are usually provided with redundancy concepts, e.g. DECs consist of two channels, with only one of the lanes usually controlling at a time, each having its own set of input data from duplex sensors and controlling the engine actuators by means of dual lane Electro-Hydraulic Servo Valves (EHSV), solenoids, Direct Drive Valves (DDV), etc., which have enabled a significant improvement to be obtained in overall engine reliability. The DEC also incorporates extensive Built-In Test (BIT) features to check the status of its inputs and outputs to and from the actuation system.

The engine control system overall reliability may then be considered to be basically determined by the actuation system, the typical critical failure rate of which is in the range from 1 to 10 failures per million hour of operation. As it is obviously not possible to design a single actuation system which is never going to fail hard-over to the fully open or fully closed position, it is usual practice to design the DECs with reversionary or alternative control means in the event that the actuator control is lost. The introduction of these alternative control ways should not only be based on electrical drive checks so actuator model checks are usually provided to check the complete electrical system related to the electro-hydro-mechanical elements. These types of reversionary control actions can be quite complex and, although they protect the engine from severe damage, there is usually a severe restriction in engine modulation and operation, which makes the typical failure rates mentioned above may be easily considered acceptable for twin engined aircraft operation, but it is questionable whether they would for single engined aircraft where a typical target breakdown for engine control failure contribution requires a figure better than 1 failure per million hour of operation.

This leads to the need of introducing some form of duplication of components for the actuation system to be provided with redundant means of performing its function (back-up control). The most straightforward approach would be duplicating the whole system, but the obvious negative impact on mass, envelope, power needs and complexity (leading to a poorer overall engine reliability at the cost of increasing operational availability), makes the right approach be focusing on the points in the system with the highest weakness to system impact ratio. A typical point of this kind in most of the actuation systems is the EHSV driving the actuation piston.

2 Back-up control qualitative requirements

Besides the reliability quantitative requirements outlined above, which referred to critical failure rate figures that the actuation system should typically meet, some qualitative requirements should also be pursued. Typical widely accepted requirements are the following:

- Transfer from primary system to back-up system and back to primary system should be possible at any power setting without engine instability or change in control system input. Reversibility should be allowed for to preclude loss of redundancy on false invokes of the back-up system due to spurious signals in the feedback position control loop.
- Demand input signals should be identical to those of the primary control system. This should allow shorter processes of validation and verification of the control laws and software implemented as well as the use of common pieces of hardware within the actuation system.
- The back-up system should prevent the engine from exceeding any specified limits, which may be more easily accomplished provided transient departures from demanded control positions are maintained at a minimum, i.e. achieving fast detection, isolation and compensation of failures in the main system.
- The compensation for failures is better dealt with by complete isolation of the failed system, precluding undesirable and unpredictable interactions between both systems.
- The back-up system should be designed to provide a similar engine response to the primary system. Simple back-up systems may make the aircraft impossible to fly safely and merely decrease system reliability. Manual back-up systems on the other hand are often used, mainly in single engine applications, which provide a complete override to the normal engine control system. These systems however increase pilot workload, which may be specially dangerous during an aircraft flight critical phase. The development of ever increasing reliability integral DECs makes this type of systems become of more than questionable use today.
- The change-over process from the main to the back-up system should be predictable at any engine operating condition. This is more easily achieved if the reaction of both systems and the change-over process itself under a failure situation is kept independent on the engine condition as far as practical. This also reduces the amount of verification and validation tests necessary on the system.
- Single point failures should be reduced to an absolute minimum.

3 Failure detection, isolation and compensation

Most of the actuation systems provided with a back-up control operate on the primary control with the back-up control isolated. The actuation system relies completely on the DEC to detect primary control malfunctions via BIT and actuator model checks. It is usually relatively easy to detect out of range defects but becomes quite more difficult to ascertain whether those out of range signals really represent an actual hydro-mechanical failure. Offset type defects and spurious electrical signals render a need for further control logic checks, which are time consuming, in order to confirm the failure. With the ever increasing requirements on engine control and response, more reliance on complex engine controls and accurate positioning of the actuators has been placed. This trend has driven the requirements for fast detection, isolation and compensation of the failures to increase as well. In next section it is presented a system design method in which the first faults in the actuator drives are self-compensated and isolated thereby ensuring the fastest possible reaction time.

4 EHSV assembly with automatic detection

The design method described herein (see functional diagram in Figure 3) is provided with hydraulic means of detecting abnormal operation of the main control EHSV servo flow input to the actuator. Failure detection hydraulic logic is in-built into the system and does not hence require any further input from the DEC. As detection is based upon hydraulic parameters, reaction will follow immediately.

This system consists of three EHSVs of identical design, operating under regulated pressure conditions, Regulated Pressure (RP) minus Return Pressure (RP) kept constant, each EHSV receiving an electrical current input from separate dedicated feedback position control loops in the DEC at a time. The three control loops are functionally identical and simultaneously receive, under normal control of the EHSVs, the same actuator position demand reference signal and are fed with the same actual actuator position signal from a Linear Variable Differential Transformer (LVDT), mechanically attached to the actuator piston. In these conditions, the three control loops deliver the same electrical current signal to the three EHSVs, which will react in the same way as they are functionally alike.

Two of the EHSVs, called Main Control Servo Valves (MCSV), are hydraulically interconnected to each other providing a single flow output to move an actuator piston. The remaining servo valve, called Emergency Control Servo Valve (ECSV), operates isolated from the other two and is ready to provide an alternative flow output to move the actuator piston when required. The interconnection of the former two MCSV forms the core of the isolation and compensation logic and functions in the following manner (if two four-way valves, each with two control lines, are used):

- Opposite control lines, from the operational point of view, of each MCSV are interconnected to form a pressure reference line. The other two remaining control lines, one from each servo valve, are used to drive the actuator piston.

- If both MCSV operate free of failures, the two control lines driving the actuator act as if one single servo-valve was used, controlling actuator piston flow and hence displacement velocity. The reference pressure of the line formed by the other two control lines joined together will nominally have a constant level typical of a single control servo valve (usually half way of supply and return pressures).

- The reference line is connected to one end of a slide valve, spring loaded on both sides, called Pressure Control Valve (PCV), which has its other end connected to a fixed potentiometer reproducing the nominal servo valve control pressure. If the two interconnected MCSV operate correctly, the slide valve should stay half way of its physical end stops.

- The ECSV remains isolated from the primary control (MCSV and actuator piston). This is achieved by another two-position slide valve, called Servo Valve Select Valve (SVSV), which would switch actuator piston servo control from the MCSV to the ECSV, piloted by the PCV. The ECSV may have its two control lines open circuited in stand-by, as described and shown in Figure 3, or it may alternatively have them connected to a separate back-up actuator piston, which should then remain isolated from the main control, in stand-by operation, but continuously shadowing the main actuator piston.

- If any of the two MCSV failed to react as it should, congruent with actuator piston actual and demanded positions (the failure may be due to the servo valve, its feedback position control loop or the electrical connections between both), the other interconnected servo-valve would not be, in principle, affected by the failure (the probability of a failure in both MCSV is remote). This means that both MCSV would react differently, one departing from and the other following the demand. This would create an actuator piston servo flow shift which would bring the actuator piston off the demanded position in a direction corresponding to the demand of the failed MCSV. The shift in actuator position would be fed as an error into the feedback position control loops of both MCSV, but while the failed MCSV cannot react according to the error, the operative MCSV would, opposing the failed MCSV. This deviation in the way both servo valves perform would cause:

a) a departure of the MCSV reference pressure value off its nominal which in turn off-centres the PCV (the direction it moves to would depend on the type of failure but it is irrelevant for failure determination). This movement of the PCV to either side would, after an adequate dead band had been travelled to cater for component deviations off nominal, set a high pressure connection in the line which pilots the SVSV. The SVSV would then move to its fully compressed spring end stop, which would disconnect the MCSV control lines from the actuator piston and would connect the ECSV control lines instead.

b) a progressive reduction in actuator piston servo flow shift due to the opposing reaction of the operative MCSV. The servo flow shift would eventually become null as soon as the operative MCSV had moved sufficiently to fully counteract the failed MCSV. This situation may always be nominally achieved as both MCSV are alike. This reduction in servo flow shift implies a progressive reduction in actuator piston velocity off the demanded position until it becomes null and a determined position offset is attained. This is quite an important feature of the system since a single MCSV failure does not imply a continuous actuator piston travel off the demanded position (until it would eventually hit either stop) but simply an actuator position offset, proportional to the effective MCSV failure current (the proportional constant being the feedback position control loop electrical current to piston position gain). Furthermore, in the case that the effective failure current was lower than the MCSV saturation current, and the feedback position control loop was provided with integral compensation, the actuator position offset would not be permanent. This behaviour of the system may then reduce the criticality of any failure to a great extent.

- The system, as configured, is reversible. If the failure disappears, the MCSV recovers control as soon as the PCV goes back to its centred position and the SVSV recovers its equilibrium position.

5 EHSV assembly without automatic detection

The feature of the system, described in section 5, of being capable of preventing large excursions of the actuator piston in a failure situation allows that DEC detection of control malfunctions via BIT and actuator model checks may be reconsidered provided the DEC model checks are sufficiently accurate to ascertain whether those position offsets caused by a failure correspond to an actual hydro-mechanical failure. This is so because failure detection times become much less critical with this approach, assuming the effect of the position offset is far from being really dangerous to the engine.

If the conditions mentioned before are met, the detection logic could be transferred from the hydro-mechanical side into the DEC, and a hardware simplification could be obtained by removal of the PCV. Nevertheless, in this case an additional servovalve, called Change-Over Servo Valve (COSV), would be needed to interface between the DEC and the system, and send the change-over signal directly to the SVSV (see functional diagram in Figure 4).

6 Simulation results

Computer simulations have been run for the EHSV assembly with automatic detection, incorporating failure injection capability to one of the MCSV. Figures are included showing the evolution of various system parameters when a worst case hard-over failure (EHSV saturation electrical current) is injected in both directions to one of the MCSV at 0.2 s simulation time. Steps up and down to the piston position demand are introduced at 0.5 and 1.5 s respectively. Piston position offsets and position recovery once the change-over process is accomplished may be observed.

Figures 1A, 1B, 1C and 1D show piston actual position and position demand, MCSV and ECSV electrical input currents, PCV and SVSV positions, and PCV pressure recovery on both sides ((P-LP)/(RP-LP)), respectively in the case a failure to increase piston position is introduced.

Figures 2A, 2B, 2C and 2D show piston actual position and position demand, MCSV and ECSV electrical input currents, PCV and SVSV positions, and PCV pressure recovery on both sides ((P-LP)/(RP-LP)), respectively in the case a failure to decrease piston position is introduced.

7 Conclusions

The system as described complies with the qualitative requirements laid down for back-up controls in section 2. It provides a fast, consistent yet relatively simple method to compensate for any type of electro-hydro-mechanical failure. This concept has been devised for its use on single engine aircraft application actuation systems although its potential benefits may be traced to other applications as well .

Figure 1A. Piston actual position and position demand. Upward failure.

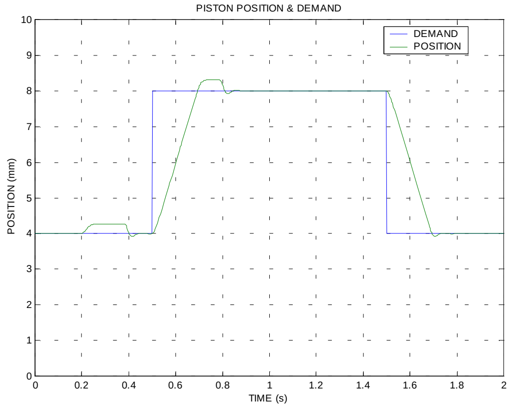


Figure 1B. MCSV & ECSV electrical input currents. Upward failure.

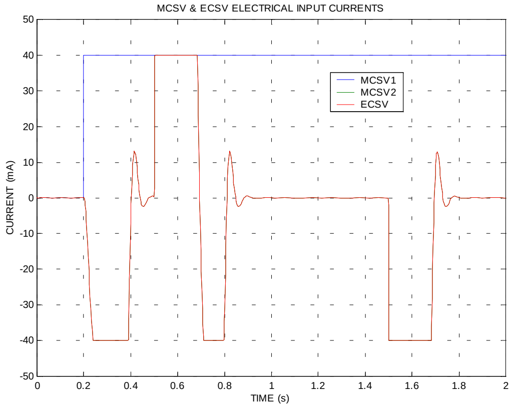


Figure 1C. PCV & SVSV positions. Upward failure.

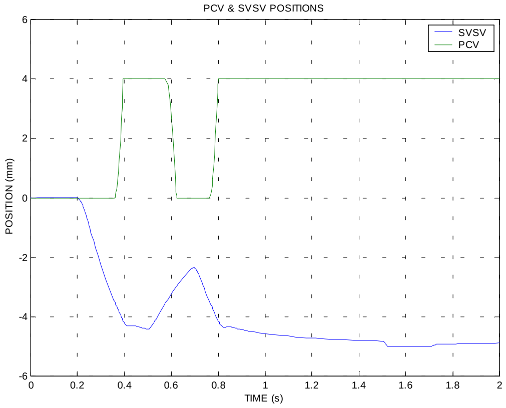


Figure 1D. MCSV control servo pressure. Upward failure.

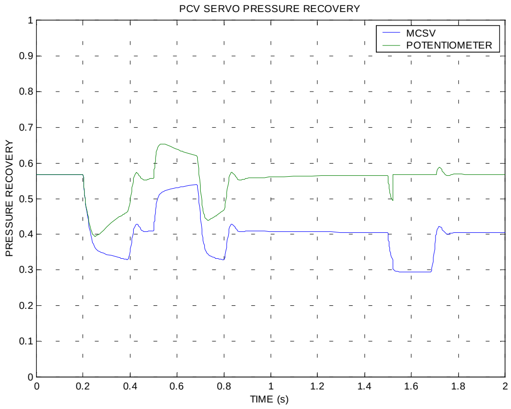


Figure 2A. Piston actual position and position demand. Downward failure.

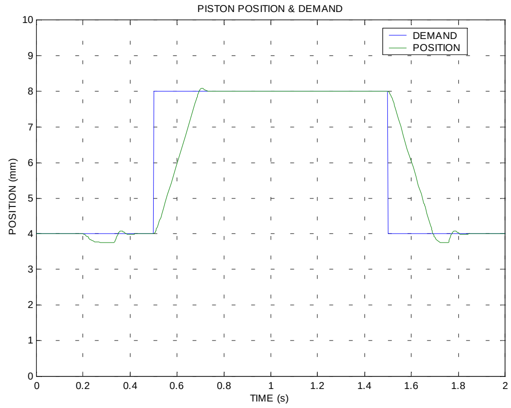


Figure 2B. MCSV & ECSV electrical input currents. Downward failure.

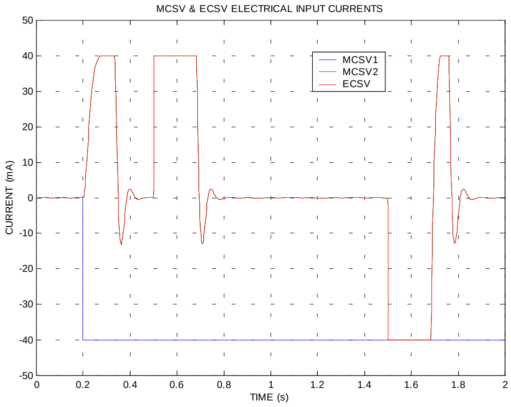


Figure 2C. PCV & SVSV positions. Downward failure.

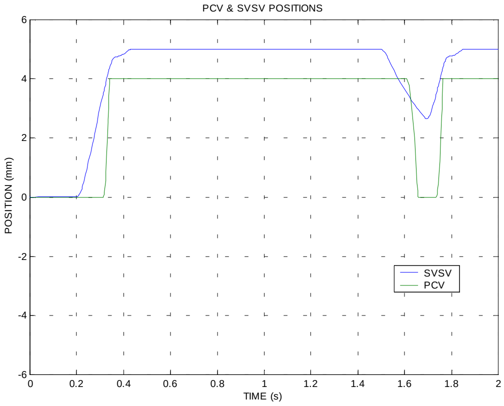


Figure 2D. MCSV control servo pressure. Downward failure.

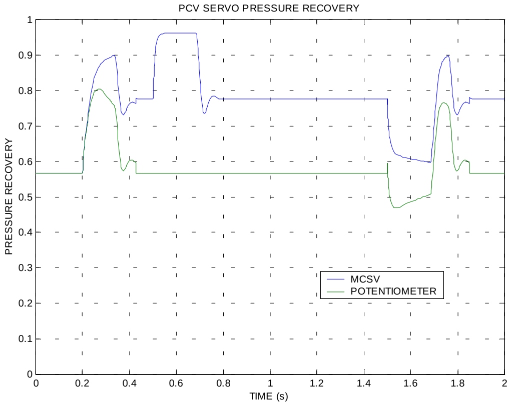


Figure 3. Functional diagram EHSV assembly with automatic detection

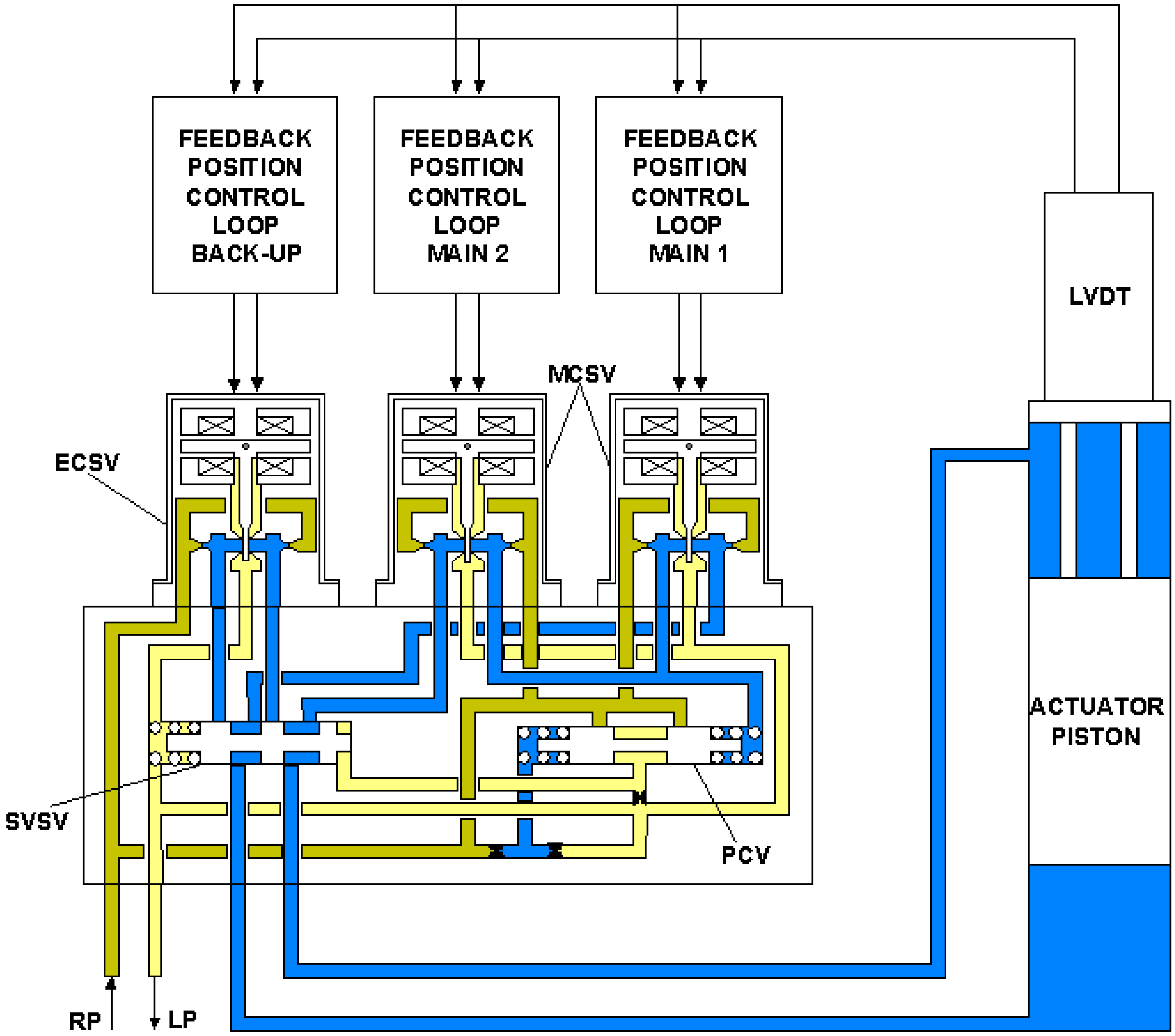
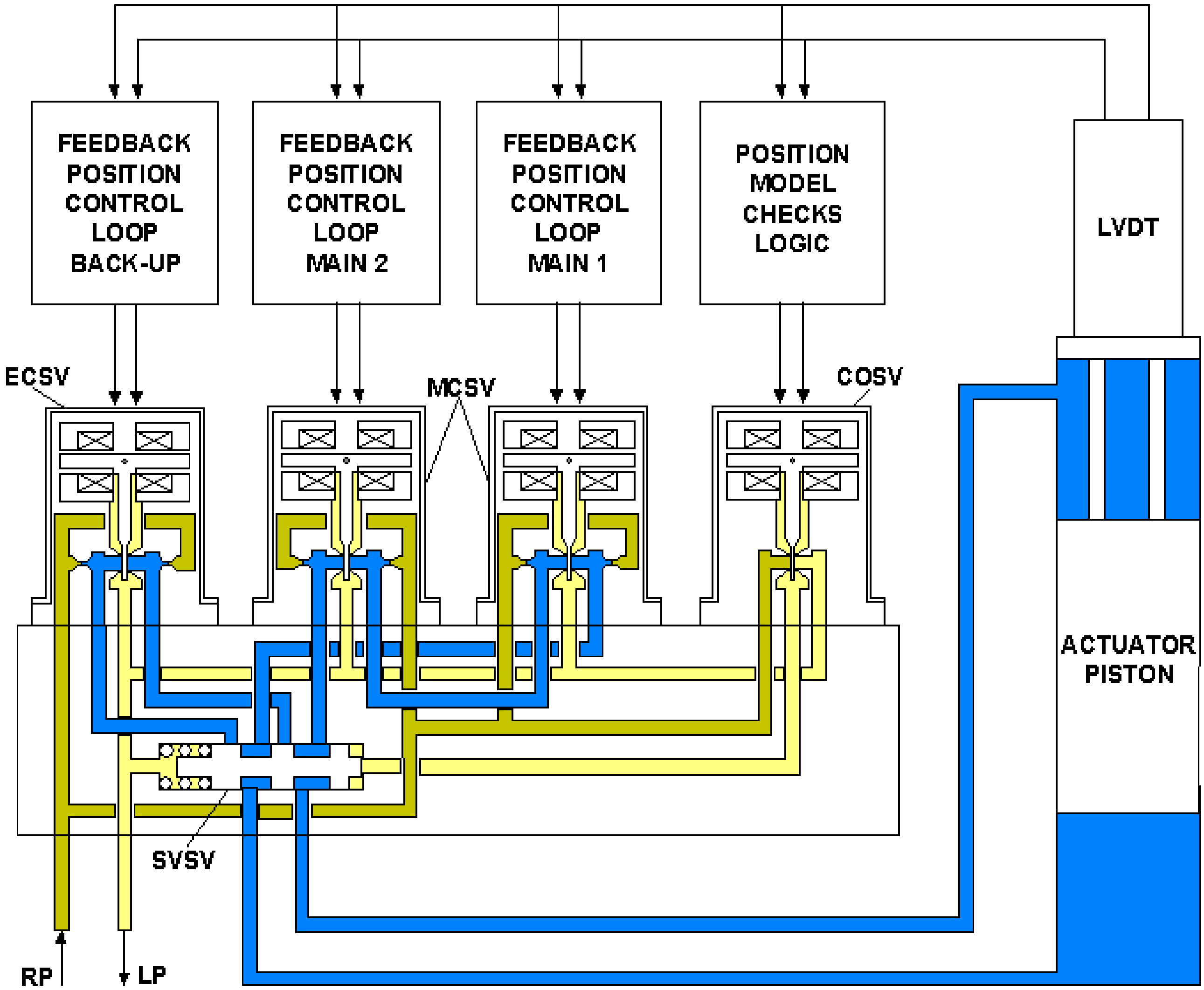

FEEDBACK POSITION CONTROL LOOP BACK-UP
FEEDBACK POSITION CONTROL LOOP MAIN 2
FEEDBACK POSITION CONTROL LOOP MAIN 1
LVDT
MCSV
ECSV
SVSV
PCV
ACTUATOR PISTON
RP
LP

Figure 4. Functional diagram EHSV assembly with automatic detection


FEEDBACK POSITION CONTROL LOOP BACK-UP
FEEDBACK POSITION CONTROL LOOP MAIN 2
FEEDBACK POSITION CONTROL LOOP MAIN 1
POSITION MODEL CHECKS LOGIC
LVDT
ECSV
MCSV
COSV
ACTUATOR PISTON
SVSV
RP
LP