SAE Aerospace
An SAE International Group

AEROSPACE INFORMATION REPORT

AIR5273

Issued 2001-12
Reaffirmed 2007-01

Actuation System Failure Detection Methods

RATIONALE

This document has been reaffirmed to comply with the SAE 5-year Review policy.

FOREWORD

This AIR is a sister document to AIR4094 and AIR4253. It provides only the failure detection method detail to accompany the more complete architecture and hardware descriptions contained in the referenced AIRs.

TABLE OF CONTENTS

TO PLACE A DOCUMENT ORDER: **Tel:** **877-606-7323 (inside USA and Canada)**
Tel: **724-776-4970 (outside USA)**
Fax: **724-776-0790**
Email: **CustomerService@sae.org**
SAE WEB ADDRESS: **http://www.sae.org**

TABLE OF CONTENTS (Continued)

1. SCOPE:

This AIR provides descriptions of aircraft actuation system failure-detection methods. The methods are those used for ground and in-flight detection of failures in electrohydraulic actuation systems for primary flight control. The AIR concentrates on full Fly-By-Wire (FBW) flight control actuation though it includes one augmented-control system. The background to the subject is discussed in terms of the impact that factors such as the system architecture have on the detection methods chosen for the flight control system. The types of failure covered by each monitoring technique are listed and discussed in general. The way in which these techniques have evolved is illustrated with an historical review of the methods adopted for a series of aircraft, arranged approximately in design chronological order.

1.1 Purpose:

The purpose of this document is to aid the designers of the systems of the future by showing what succeeded in the past.

2. REFERENCES:

2.1 Applicable Documents:

The latest issue of the documents shall be used except in those cases where an invitation for bid or procurement contract specifically identifies the issues in effect on a particular date. In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence.

2.1.1 SAE Publications: Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001. Web site: www.sae.org. Telephone: (724)-776-4970

SAE AIR4094, Aircraft Flight Control Systems Descriptions.

SAE AIR4253, FBW Actuation System Descriptions.

SAE Paper 831484, Development of Redundant Flight Control Actuation Systems for the F/A-18 Strike Fighter, H.E. Harschburger.

SAE Publication, Aircraft Flight Control System Design, E.T. Raymond and C.C. Chenoweth.

2.1.2 U.S. Government Publications: Available from DODSSP, Subscription Services Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094. Web site: http://assist.daps.mil or http://stinet.dtic.mil/

MIL-F-9490, Flight Control Systems – Design, Installation and Test of, Piloted Aircraft, General Specifications for.

MIL-STD-882, System Safety Program Requirements.

2.1.3 FAA Publications: Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591

AC 25.1309–1A FAA Advisory Circular, System Design Analysis, (1988, June).

NPA 25C-199 JAA Notice of Proposed Rule Making, Interaction of Systems and Structure, (1996, April).

2.1.4 RTCA Publications: Available from RTCA Inc., 1140 Connecticut Avenue, NW, Suite 1020, Washington, DC 20036.

RTCA DO-178 Software Considerations in Airborne Systems and Equipment Certification

2.2 Related Publications:

The following publications are provided for information purposes only and are not a required part of this SAE Aerospace Technical Report.

2.2.1 SAE Publications: Available from SAE, 400 Commonwealth Drive, Warrendale, PA 15096-0001

SAE Publication, Fly-By-Wire A Historical and Design Perspective, V.R. Schmitt, J.W. Morris and G. Jenney (1998)

2.3 Definitions:

2.3.1 Acronyms and Abbreviations:

BIT	Built-In-Test
CBIT	Continuous Built-In-Test
CCDL	Cross Channel Data Link
CCM	Cross-Channel Monitoring
CMM	Common Mode Monitor
CRM	Command Response Monitor
CSAS	Command and Stability Augmentation System
DDV	Direct Drive Valve
DFCC	Digital Flight Control Computer
ECU	Electronic Control Unit

2.3.1 (Continued):

EHV	Electrohydraulic Servovalve
EICAS	Engine Indicating and Crew Alerting System
FAA	Federal Aviation Administration
FBW	Fly-By-Wire
FCC	Flight Control Computer
FHA	Functional Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FO / FS	Fail-Operate / Fail-Safe
FO^2 / FS	Double-Fail-Operate / Fail-Safe
FS	Fail-Safe
IBIT	Initiated Built-In-Test
IFCM	Integrated Flight Control Module
ILM	In-Line monitoring
JAA	Joint Aviation Authorities
LCA	Light Combat Aircraft
LES	Leading Edge Slat
LRU	Line Replaceable Unit
LVDT	Linear Variable Differential Transformer
MBIT	Maintenance Built In Test
MCV	Main Control Valve
MMC	Mechanical Mode Coupler
MTBF	Mean Time Between Failures

2.3.1 (Continued):

NPRM	New Proposed Rule Making
NVM	Non-Volatile Memory
PBIT	Preflight Built-In-Test
PLOC	Probability of Loss of Control
RLS	Reservoir-Level-Switching
RVDT	Rotary Variable Differential Transformer
RVT	(Sometimes used) RVDT With Only Four Wires
SVM	Servovalve Monitor
WRA	Weapon Removable Assembly

3. BACKGROUND:

This section discusses some of the aspects of the design of flight control actuation systems. It attempts to discuss their impact on failure detection design only and to avoid a more general discussion of control system design.

3.1 Evolution:

Primary flight control actuation systems have evolved through three generations since the general adoption of full-time powered actuation. Analog FBW replaced the electronic augmentation of mechanical commands and has in its turn been replaced by digital FBW. Meanwhile, the servoactuators have also changed significantly. Hydromechanical complication and relatively simple electrical interfaces marked the earlier FBW actuation concepts found in the Space Shuttle and the F-16. The current generation, typified by the Airbus “family”, the Boeing 777 and the V-22, employ significantly simpler hydromechanical logic and depend much more upon electronic failure detection and the associated electronic equipment.

The reasons for this are:

- Increased confidence in integrated electronics and digital processing, because of the increased competence and reliability of the hardware, allows advantage to be taken of the weight and initial cost savings made possible by the use of electrical logic instead of hydromechanical logic.
- Decentralization of the associated electronics makes the cable weight penalty for a more complex electrical interface less severe, a factor of increasing importance, as actuation systems become less centralized.

3.2 Avoiding the "Nuisance-Disconnect":

The flight control and actuation systems used in FBW aircraft employ redundancy for safety and incorporate many elements, as shown Figure 1, that interact in a closed loop manner.

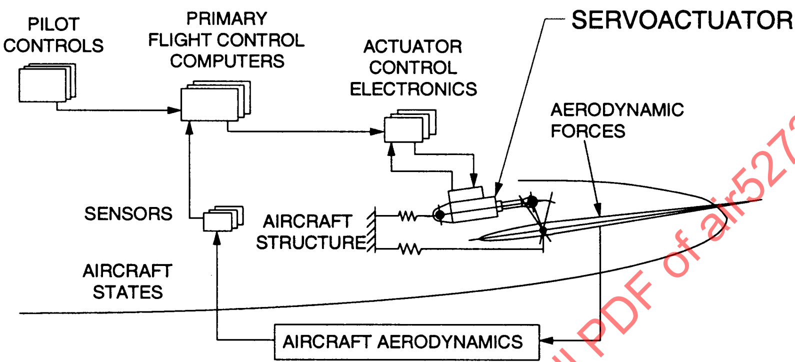

FIGURE 1 - The FBW Servoactuator and Its Interactions

Because of the interactions and because the precise states of many of the elements cannot be known, it is often difficult to diagnose servoactuator failures as quickly as the aircraft requires. To one degree or another, all of the satisfactory methods developed to date filter out transient events and require persistence of indication before a failure will be declared. The design of a diagnostic method always requires a balance to be drawn between satisfactory performance and an acceptable risk of the "nuisance-disconnect". This is defined as the declaration of a failure when none exists and the consequent mistaken attempt to provide protection by disconnecting correctly operating system components.

3.3 Architecture and Application:

The primary flight control servoactuators flying today use many different diagnostic techniques. These differences are a function of the year in which they were designed, the differing performance they must provide and the various system architectures in which they are employed. There is no universally applicable, "best" architectural approach. The architecture chosen for each new aircraft will be determined by its mission and by the component and subsystem technology available to the design team. This available technology will change for each new generation of aircraft and this will force a re-evaluation for each new aircraft.

3.3.1 Cross-Channel Versus In-Line Monitoring: The architectures proposed for the first generation of FBW aircraft were frequently differentiated by their approach to monitoring. Four-channel architectures featuring cross-channel comparison for failure detection competed with triplex architectures employing "in-line" monitoring.

Cross-channel comparisons between four channels typically allows the detection and isolation of the first and second failures but not the third since a one-on-one comparison provides no basis for distinguishing the bad channel from the good. With this type of architecture care must be taken to avoid the potential for single failures that will result in an even number of channels being compared since there is no way to distinguish the bad from the good. Two dual transducers, for example, provide no protection against disconnection of a single load path to the two probes of one paired transducer.

In-line monitoring provides "self-monitoring" of each channel and therefore can be designed to provide sustained operation with only one remaining channel. A triplex in-line monitored approach therefore provides the same degree of fault protection as a quadruplex cross-compared architecture, though each channel of the triplex architecture contains appreciably more hardware than each channel of the quadruplex architecture. In-line monitoring allows a greater degree of system separation, a desirable feature for flight critical applications and of great assistance to the certification of commercial aircraft. Present-day FBW architectures almost invariably use combinations of in-line and cross-channel monitoring, protected for system safety, as described in the system separation discussion of 3.5.

3.4 Designing "By the Numbers":

3.4.1 Probability of Failure: Actuation systems were once designed to operate following a selected combination of failures such as "any hydromechanical failure plus loss of any two electrical systems". It is now customary to design an actuation system and each Line-Replaceable-Unit (LRU) to achieve allocated probabilities of loss of function and loss of control. Loss of function means that the system can no longer perform its intended function. In general it will have reverted to a Fail-Safe (FS) mode of operation that allows continued safe flight and landing. This loss of function may or may not allow completion of a mission and mission reliability is one way in which military actuation systems are specified. Loss of control, by contrast, means loss of control of the aircraft.

Some military actuation systems have an FS mode that does not allow safe landing. Such a mode may allow continued flight for a time sufficient only to allow engine restart or safe ejection.

In the military aircraft field the terms Probability of Loss of Function (PLOF) and Probability of Loss of Control (PLOC) are customarily used. During the preliminary phase of a military air vehicle design, the prime contractor and the procuring agency must agree on the vehicle mission reliability, its PLOC and the associated safety hazard categories, see 3.4.3 and 3.4.4.

3.4.1 (Continued):

Each possible failure must be considered for its probability and for its consequences using Failure Modes and Effects Analysis (FMEA) or Failure Modes and Effects Criticality Analysis (FMECA), Fault Tree Analysis and Functional Hazard Analysis techniques, see 3.4.3. The design of the failure-detection methods and the "coverage" they achieve is a vital part of this process.

Accessing historical data covering the failure rates and failure modes of actuation system components is also of prime importance. SAE publication "Aircraft Flight Control System Design", section 12.1.9, lists potential sources.

3.4.2 Fault Coverage: Fault coverage is the number of failures that will be detected expressed as a percentage of all failures that could occur. It is a direct result of a system's overall architectural design together with the detailed design of its hardware and software. Fault coverage is a vital system aspect, because it is often true that certain undetected failures can result in loss of control. In this case the product of the probability of these failures and their "lack of coverage" will increase the PLOC for the system.

A FMEA is conducted early in a system design to allow the failures to be separated into safety-critical, mission-critical and non-critical categories and hence to determine which faults contribute to the PLOC and which to the PLOF. This categorization is mission dependent. For example, trailing edge flap failures might be neither safety nor mission critical for a land-based aircraft but safety critical for a carrier-based aircraft. The failure categorization allows a more realistic assessment to be made of the fault coverage required since failures that are not critical can be monitored with a relatively low coverage without impact on PLOF or PLOC. The results of the FMEA are used to develop algorithms to detect critical failures or to iterate the design to remove failure modes.

In a voting triplex or quadruplex redundant FBW actuation system the issue of fault coverage is not so critical for first failures upstream of the last voting plane. This plane could be a digital voter or an averaging mechanism such as a magnetic flux summing point within a servovalve or a mechanical force sum point within or downstream of an actuator. The ability of such a voting plane to absorb the effects of an undetected failure allows the coverage of the upstream failures to be relatively low. This is because their contributions to the PLOF and PLOC are measured by combined probabilities and the calculation of series additive events suppresses the impact of the undetected failures on the overall failure rate.

For example, for a triplex system the calculation might be as follows. The PLOC for upstream failures would be the product of the probability of the first failure, its lack of coverage and the probability of the second failure. It should be noted that the precise form of these calculations is dependent on the type of monitoring used.

3.4.2 (Continued):

Failures within a specific channel or lane upstream of a voter can be grouped by their effects and isolated as a group. All of these failures must be addressed correctly to allow the PLOC allocations to be met. The PLOC is likely to be driven, however, by failures downstream of the voter. These must be sufficiently remote and monitored with sufficient coverage to yield an acceptable PLOC. Overall fault coverage during real time computations is typically 90 to 95%. Achieving a higher percentage of coverage typically causes penalties in the Mean Time Between Failures (MTBF), cost, weight, and volume because of the additional circuitry and software required.

3.4.3 Commercial Aircraft Failure Criticality and Probability: The safety analysis of an aircraft flight control system starts with a Functional Hazard Analysis (FHA). The FHA identifies the hazards associated with the failure modes of the system for that aircraft. These hazards are categorized with respect to their effect on the aircraft, the ability of the crew to deal with the failure condition and the safety of the occupants.

Commercial aircraft airworthiness requirements define the various effect categories in terms that vary from “Minor” to “Catastrophic”. They define the criticality of the loss or degradation of function caused by the failure in terms that range from “Non-Essential” to “Critical”. They define the allowable probability of occurrence of each category in quantitative terms ranging from “Probable” to “Extremely Improbable”. Finally, they dictate the quantitative range of the allowable probability of occurrence for each in failures per flight-hour terms. Table 1 illustrates these relationships with information extracted from the FAA Advisory Circular AC 25.1309-1A. It also shows the differences in definition between the Federal Aviation Administration (FAA) of the United States and the Joint Aviation Authorities (JAA), the equivalent certification authority for Europe. The table shows that the certification authorities allow differing software levels to be associated with the differing effect categories. This allows design approaches that segregate the detection of non-safety-critical failures to a separate lane of processing and a lower level of software. Similarly, different design criteria for the robustness of the detection with respect to component tolerancing could be adopted.

These requirements must be satisfied by the architecture chosen for the aircraft. The design of the failure detection plays an important part in the choice of architecture and design of the elements of the architecture. Correct detection and reconfiguration minimizes the hazard that results from a failure; failure to correctly detect a failure can create an immediate hazard or set the system for a later catastrophic effect from a second failure as discussed in 4.2.3.

Analysis of the effects of each failure mode for a servoactuator allows differing approaches to be adopted for the differing failure modes. More hazardous effects demand full-time, continuous monitoring. Less serious effects can be addressed by background monitoring. See 3.8 for discussion of the different categories of testing. In the commercial aircraft field, failures with less serious effects and with low probabilities are tested for during scheduled testing every few hundred flight hours.

TABLE 1 - FAA and JAA Failure Criticality and Probability Definitions

Effects on aircraft and occupants of the identified failure condition.	FAR – AC 25.1309-1A definitions.	No significant degradat - ion of aircraft capability. Crew actions well within their capabilities.	Reduction of the aircraft capability or of the crew ability to cope with adverse operating conditions.		Prevention of continued safe flight and landing of the airplane.
	AMJ of JAR 25.1309 definitions.	Slight reduction of safety margins, slight increase in work-load, (e.g. routine changes in flight plan), or physical effects but no injury to occupants.	Significant reduction in safety margins, reduction in the ability of the flight crew to cope with adverse operating conditions impairing their efficiency, or injury to occupants.	Large reduction in safety margins, physical distress or workload such that the flight crew can-not be relied upon to perform their tasks accurately or completely, or serious injury to or death of a relatively small portion of the occupants.	Loss of the airplane and/or fatalities.
FAR effect category AC 25.1309-1 A.		Minor	Major		Catastrophic
Effect category AMJ of JAR 25.1309 and Eurocae ED-12A.		Minor	Major	Hazardous	Catastrophic
Criticality category RTCA DO-178A for system functions.		Non-essential	Essential		Critical
DO-178A Software Levels.		Level 3	Level 2		Level 1
DO-178B Software Levels (Level E - No Effect).		Level D	Level C	Level B	Level A
FAR quantitative probability terms.		Probable	Improbable		Extremely Improbable
JAR quantitative probability terms.		Frequent Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
FAR and JAR quantitative probability ranges.		10^{-3} 10^{-5}	10^{-7}	10^{-9}	

Probability of Failure Condition (for one flight hour or flight if less than one hour).

3.4.3 (Continued):

The effect category also determines the subsequent action taken by the system. Failures that impact safety must lead to immediate and automatic reconfiguration. Failures that reduce the robustness of the system to subsequent failures may be annunciated to the pilot and used to prevent subsequent flight dispatches until corrected. More benign failures and degradations may be collected by a maintenance system for correction at a scheduled time and location. An assessment of the effects and probabilities of all of the possible latent failures must be performed to justify the scheduled maintenance time intervals.

3.4.4 Military Aircraft Failure Criticality and Probability: Almost all of the content of the previous subsection applies equally to actuation systems designed for military aircraft. Similar hazard definitions are established for military aircraft, though there is less consistency to the categories and to their allowed probability of occurrence. The hazard categories are adjusted and their accompanying quantitative requirements assigned on a program-by-program basis using MIL-F-9490 as a guide. A single-engine fighter requires different treatment from a multi-engine transport.

Tables 2 and 3 contain information extracted from MIL-STD-882 providing guiding definitions for hazard safety categories and an example of a qualitative hazard probability ranking, respectively.

TABLE 2 - Military Usage Hazard Severity Category Guide

Description	Category	Definition
CATASTROPHIC	I	Death, system loss or severe environmental damage.
CRITICAL	II	Severe injury, severe occupational illness, major system or environmental damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system or environmental damage.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

TABLE 3 - Example of Military Usage Hazard Probability Ranking

Description	Level	Specific Individual Item	Fleet or Inventory
FREQUENT	A	Likely to occur frequently	Continuously experienced
PROBABLE	B	Will occur several times in the life of an item.	Will occur frequently
OCCASIONAL	C	Likely to occur some time in the life of an item	Will occur several times
REMOTE	D	Unlikely but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur
IMPROBABLE	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

3.5 System Separation:

Some applications demand a “brick wall” between the redundant electrical control channels. This design approach forbids the use of electrical cross-channel interaction to avoid the corruption of one channel by a neighbor. The issue of hydraulic and electrical system separation is similar. Hydraulic system switching is sometimes seen in military aircraft, usually protected to prevent loss of multiple systems through a single leakpath, but very rarely used in commercial aircraft. Electrical bus switching is used in both military and commercial aircraft, accompanied by dedicated un-interruptible back-up power for flight critical systems.

For commercial aircraft, brick wall separation greatly assists the certification process because of the elimination of some common-mode failures that could disable more than one electrical channel. A brick wall compels the use of “in-line” monitoring, that is, monitoring contained within the channel being monitored. The Space Shuttle monitoring description in 5.3 provides one example of this approach.

High-performance military aircraft typically operate at flight conditions that demand such close control of failure transients that the differences between channels must be minimal and divergence from the ideal state must be detected immediately. This situation has been addressed with the use of cross-channel equalization or voting and cross-channel comparison for failure detection

Brick-wall requirements have become less absolute. Design techniques and technology have been developed to provide safe means of cross channel information handling through “buffering”, the use of data buses and optical coupling. Data buses now carry multiple commands generated by parallel channels. DC buses that power each channel are themselves derived from redundant DC power supplies. Logic states of an actuation system can be signaled from one channel to another as a hydraulic pressure. This pressure is often provided with a “fuse” to protect against loss of two systems from a single-point-failure.

There is program cost associated with many of these means of protection, for example the additional verification and validation required for Cross-Channel-Data-Link (CCDL) hardware. Despite their use, any data transfer between channels carries risk and in some situations remains prohibited. Where it is adopted care must be taken to limit cross-channel corruption by the use of, for example, authority limiting and particular care used to prevent a failed channel from turning off a healthy channel.

3.6 Fighting Between Redundant Commands to a Surface:

When multiple command channels are summed to position a common surface in a majority-vote or "active-active" manner, the commands will tend to fight one another. The summation may be within the position control loop or velocity control loop of a single servoactuator, or within the structure of a single surface driven by multiple servoactuators. It may take the form of a fight between electrically induced magnetic fluxes, a fight between summed flows, a force fight at the level of the forces required to drive a control valve or a force fight at the level of the full output force capability of the servoactuator. The fighting is caused by small differences between the loops closed around the servoactuator. These differences are dominated by the tolerances of the elements of the loops, exaggerated by their high gain.

This fighting can degrade the performance of the servoactuator and, in the worst case, could damage the structure of the aircraft. In addition, successful failure detection within a system architecture that did not address force fight would be jeopardized because of the resultant effects on the measured indicators typically used in failure detection. Servovalve output pressure, for example, could be strongly biased or even hardover due to force fight, even though no failure had occurred.

The Space Shuttle servoactuators, see 5.3, employ an architecture that diminishes the effect of the fighting, places the fighting in a location where it cannot harm the life or performance of the actuator and provides good failure detection despite a complete brick-wall. The actuation hardware is very complex hydromechanically, however. Simpler actuation schemes with better positioning accuracy are practicable if electronic rigging is adopted.

3.7 Electronic Rigging:

3.7.1 Electronic Rigging Purpose: In some digital fly-by-wire flight control systems electronic rigging functions have been developed to reduce maintenance costs by eliminating the manual adjustments of actuator length normally required to accommodate manufacturing tolerance in the air vehicle structure. These functions have a secondary benefit in that they can compensate for the effects that cause the force fighting between redundant channels described in 3.6.

The critical end result of a rigging process is the correct alignment of the trim positions for the surfaces, since this affects the aircraft range performance, and this part of the rigging process always requires some manual input. The accuracy over stroke, by contrast, the part of rigging which can be automated, may be very important for the flight control system but is much less important for the aircraft, This is because, in FBW aircraft, the pilot commands aircraft rates and accelerations and the control laws automatically adjust the control surface positions to meet the commands. The actuators are normally provided with sufficient stroke to allow the rate and acceleration requirements to be met with worst case tolerances and structural deflection.

3.7.2 Rigging Definitions: The following related terms are sometimes used to define differing parts of the overall process:

- Rig – An on-ground manual process to adjust each of the actuators to their required trim position and to ensure that they are capable of achieving their required surface deflections. Typically an external human interface is required to provide feedback that the correct surface position has been achieved.

- Autorig – An automated process by which limited authority offsets are inserted in the servoloop electronics of the redundant actuation system. Autorig typically requires less human intervention as feedback of surface position is handled within the redundant electronic control.

3.7.3 Rigging and Failure Detection: All forms of electronic rigging require the storage of command offsets for the parallel channels in Non-Volatile Memory (NVM). These offsets are added to the commands to compensate for the fight-producing differences. The procedure sometimes compensates for gain differences as well as null offsets, thereby reducing the differences between the fault monitoring signals in the redundant channels. This can allow the failure-detection thresholds to be reduced in size to permit faster detection and diminished transients. Since the rigging must be a ground procedure, however, it cannot correct for in-flight effects, such as temperature variations from system to system, and the thresholds must allow for these. Because the LVDTs, which many systems use to sense actuator position, are sensitive to temperature the maintenance procedures must define the hydraulic fluid temperature range acceptable for accurate rigging. Electronic rigging is easiest to perform when cross-channel transmission of information is allowed. If applied to a brick-walled architecture, each channel must at least know when a neighboring channel is performing certain operations.

The issue of where to store command-offset information creates concerns for the on-time departure of commercial aircraft and for the sortie rate of military aircraft. Any failure that cannot easily be isolated to the failed LRU is likely to lead to the replacement of different LRUs in the attempt to find the failure. If the LRU containing the stored rigging information is replaced, the actuation system design must ensure that the system must be rerigged before flight. While autorig can be short in duration the manual rig process is not.

3.8 Real-Time Monitoring, Continuous Built-In-Test and Initiated Built-In-Test:

The monitoring techniques described in this document are used for continuous monitoring and for periodic initiated testing. The terminology used to define Built-In-Test (BIT) in its various forms is not consistent across the industry but the following usage is typical:

- Real-Time Monitors – These provide failure detection of all safety critical functions so that the Redundancy Management System / Actuator Signal Management can isolate the failures.

- Continuous Built-In-Test (CBIT) – CBIT normally employs background processing. It is used to perform failure detection on non-flight critical functions and report the status of all of the ‘real time monitors’. CBIT also performs some analysis of status from real time monitors to further identify failed components and collects information to provide the aircrew with system status and data for subsequent maintenance actions. Sometimes the term CBIT is used to describe all of the in-flight monitoring of actuation system functions.

- Initiated Built-In-Test (IBIT) – IBIT includes all of the pilot and maintenance crew initiated test sequences performed on the ground, pre-flight, post-flight and during scheduled maintenance. IBIT has the ability to check the entire system including actuator slew rate, shutdown and reset of the actuators, tests of failure detection hardware and checks for passive or latent failures.

The IBIT sequences will detect the same genuine failures that the real-time monitors will find and will test the operational functions and the failure detection hardware to limits more stringent than the real time monitor thresholds. Checking the failure detection hardware is sometimes more difficult than testing the operational functions. For example, the hydromechanical servovalve failure detection method described in 5.6 for the LAVI detects servovalve failures but not electrical failures. During pre-flight testing, to demonstrate that the comparator spool is not silted up and will move if a failure occurs, a servovalve failure must be electrically simulated which requires additional connections in the command paths to the actuator.

In addition, the IBIT sequences are able to perform tests that would not be safe in the air. They can turn hydraulic systems on and off, perform rate checks, examine thresholds and look more closely at the performance of the operating components. All of this takes time. Choices must be made as to what must be performed at every pre-flight check and what may be delayed for one, several or many flights.

Within the Airline industry, IBIT that can be performed post-flight or at scheduled intervals is much preferred over pre-flight IBIT. Post flight IBIT may reveal faults that can be fixed by maintenance action between flights. Pre-flight IBIT can reveal the need for maintenance just as a loaded aircraft is leaving the gate, a situation that one airline refers to as “maintenance by surprise”. Consequently, preflight IBIT will be very limited, post flight will perhaps contain more tests and maintenance IBIT will contain different sequences for different ‘check’ intervals, determined by the criticality of the failure, the likelihood of its occurrence and the terms of the Airworthiness Certificate.

3.8 (Continued):

For military aircraft there will be two IBIT modes, preflight/post-flight IBIT and maintenance IBIT. Preflight IBIT running time is normally limited to 1-2 minutes. Typically it will move several actuators simultaneously at high rates and will not include any of the manual intervention tests needed to check some of the flight control crew station switches and functions. Maintenance IBIT assumes the aircraft is operating on external hydraulic carts and includes the manual intervention tests necessary for a complete system test.

4. MONITORING TECHNIQUES:

4.1 Failure Locations:

Figure 2 illustrates the essential elements of a typical FBW actuator.

All of these elements have failure modes that must be addressed.

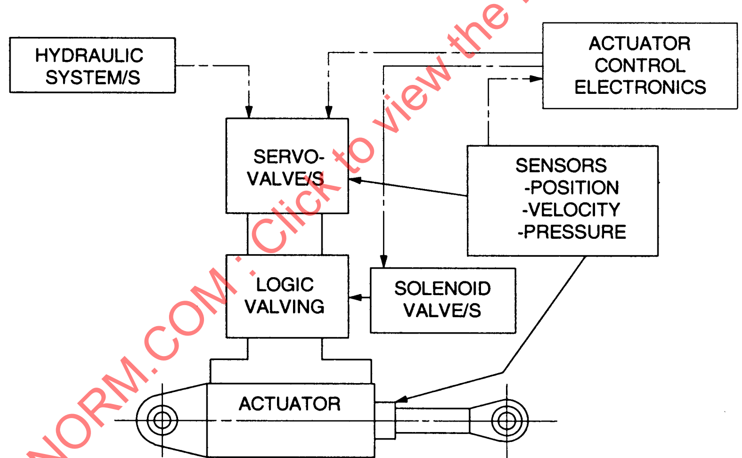

FIGURE 2 - The FBW Primary Flight Control Actuator

4.2 Failure Types:

4.2.1 Passive Failures: A “passive” failure of an element of a servoactuator makes that element unable to respond to commands. For example, a solenoid valve may fail open and cause the servoactuator to fail passively to a damped bypass mode. Alternatively, a non-redundant servovalve may jam at a position away from null and cause an active hardover of the servoactuator. Finally, an open solenoid failure could cause a servovalve to be bypassed while other redundant servovalves allow satisfactory servoactuator operation to continue.

4.2.2 Active Failures: An "active" failure of an element of a servoactuator causes an uncommanded output of the element that is likely to cause an uncommanded motion of the servoactuator. The particular arrangement of the redundancies within the servoactuator and its closed loops may allow the effects of the failure to be suppressed or rejected while the failure is being detected and the servoactuator reconfigured. For example, whereas a hardover of a non-redundant servovalve will cause immediate uncommanded motion of the servoactuator, a hardover of a voted position command will be rejected without significant output motion.

4.2.3 Latent Failures: A "latent" or "dormant" failure of an element of a servoactuator is a failure that has occurred, has not been detected and isolated, and has not yet prevented the servoactuator from responding to commands. The danger lies in subsequent failures of other elements. For example, a jam of a bypass valve in the operative position would have no immediate effect on the servoactuator but could prevent isolation of a subsequent hardover failure of a servovalve.

4.2.4 Oscillatory Failures: Oscillatory failures are of particular concern because they can be damaging at levels that are hard to detect. The concern has three different aspects. There may be oscillatory loading of the aircraft structure in a "Global" sense, there may be damaging dynamic loading of the structure "Local" to the actuator or a cockpit vibration may create an intolerably fatiguing environment for the flight crew.

- The JAA and FAA established "Global Structure" design load criteria. The JAA criteria may be found in NPA 25C-199. These criteria limit the time for which two differing levels of oscillation, specified against frequency, are allowed to exist. Oscillations below Level 1 are allowed to continue for the rest of the flight. Oscillations above Level 2 shall be disabled within one cycle if occurring at a frequency of less than 5 Hz. If they occur at a frequency higher than 5 Hz they must be disabled within 0.2 seconds. Oscillations between Levels 1 and 2 must be detected and disabled within 5 cycles or 3 seconds per failure occurrence, whichever is less. The airframe designer is responsible for determining the structural loading and hence the control surface amplitudes that correspond to Levels 1 and 2 for the aircraft in design.

  Since modern flight control systems are extremely complex it may be argued that it is impossible to visualize all of the mechanisms that could lead to oscillatory failure. Instead, failures that exceed the requirement are postulated. They are assumed to be rare but must be detected and shutoff since they are safety items. The allowable surface deflections and frequencies set the thresholds and persistence for the monitors.

- "Local Structure" oscillatory effects may be of concern if multiple actuators are used to drive a single surface in an active-active manner. Oscillatory force fights between the actuators may consume the fatigue life of the structure or even cause the disconnection of an actuator. This type of failure therefore often has a safety implication and always creates an economic concern. The failure criteria for these failures are expressed in terms of actuator differential pressure and frequency. The oscillatory pressures must conform to the limits or must be detected and shutoff within a specified time. The monitor threshold and persistence may be arranged to limit the fatigue damage to a small percentage of the structural life.

4.2.4 (Continued):

- Crew station environmental failure criteria are expressed in terms of vibration amplitude at the pilot and copilot's seats. A low level of vibration is defined as tolerable for the time required to divert the flight to an alternate airport, closer than the scheduled destination. A higher level requires detection and shutoff within a certain time.

4.3 Failure Detection Approach:

The failure-detection design always attempts to detect as many failure modes as practicable with real-time monitors and CBIT. Some modes have to be detected by periodic inspection and others must be made extremely remote by design and tested by IBIT.

The types of servoactuator failure that are usually covered by CBIT or IBIT are listed in Table 4 and those that are detected by inspection or protected against by design are contained in Table 5.

The element that has historically received the most attention is the servovalve, which takes one of two forms:

- The Electrohydraulic Servovalve (EHV), or
- The Direct Drive Valve (DDV)

Most EHVs are two-stage devices though some are single stage and most DDVs are single stage though some have two stages.

TABLE 4 - Servoactuator Failures Covered by Real-Time Monitoring or BIT

COMPONENT	FAILURE MODE
EHV	Open or shorted coil
	First stage zero output
	Broken feedback wire
	First stage hardover
	Second stage jam
DDV	Open or shorted coil
	Valve jam
LVDT	Open or short primary or secondary
	Probe disconnect
Logic spool valve	Jam
	Restrictor clog
Solenoid valve	Open or shorted coil

TABLE 5 - Servoactuator Failures Typically Covered by Inspection or Prevented by Design

COMPONENT	FAILURE	PROTECTION
Solenoid Valve	Jam or leak	Three-way, poppet-type
Actuator LVDT	Probe disconnect	Dual retention of threaded adjustment
Actuator	Rod seal leakage	Inspection
	Mechanical failure of rod, rod end, attachment	Conservative design, dual load path

4.4 EHV Failure Detection:

EHVs incorporate electrical torque motors that consume small amounts of electrical power, typically tens of milliwatts, to produce a fraction of one inch.lb of torque. This torque offsets a friction-free first stage that produces a flow output of less than one cubic inch per second. This flow and the differential pressure that the first stage can also generate, is used to drive a spool-and-sleeve-type second stage capable of providing many horsepower to the actuator. Normally a loop is closed around the spool position with a mechanical spring that feeds a torque back to the torque motor so that, in the equilibrium condition, the second stage position and output flow are proportional to the current supplied to the valve. These elements are shown in Figure 3.

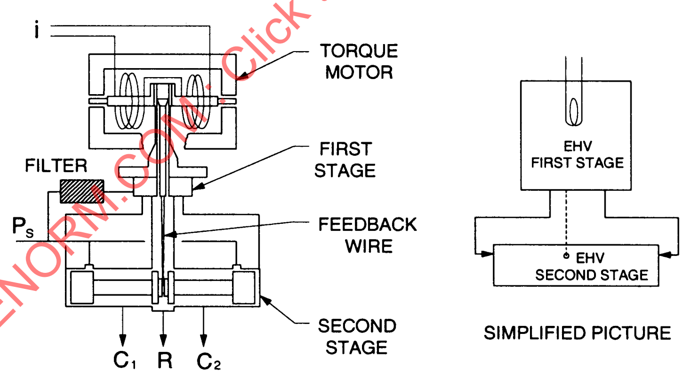

FIGURE 3 - The EHV

4.4 (Continued):

The EHV has “passive” failure modes, in which the second stage refuses to change its flow output, despite changes to the current command, and “active” failure modes in which the second stage output makes uncommanded changes. Note that a passive failure of the EHV can result in an active failure of the actuator that may be driven towards its hardover position at a high but fixed rate. Passive EHV failure modes include an open torque motor coil and a jammed spool. Active modes result from unbalanced orifice-plug modes of the first stage, mechanical failures of the first stage and failure of the feedback wire spring from the second stage. A third category of failure mode includes changes of gain caused by partial coil shorts or by magnetic gain changes from electromagnetic or temperature mishaps, erratic operation caused by severe contamination of the second stage and oscillatory failure modes (see 4.2.4). The probability of an oscillatory failure is “extremely remote” ($<10^{-7}$/flight hour) for a conventional EHV with mechanical feedback providing the loop closure around the second stage. For a valve with electrical loop closure it is “remote” ($<10^{-5}$/flight hour) because of the higher probability of an electronic open failure and the consequent loop instability.

4.4.1 Passive Failures and the use of Bias: A passive failure of a servovalve, or loss of the current to it, will induce a hardover failure of the actuator, but normally at a lower rate than an active failure will. This should give a smaller failure transient but may not since passive failures can be hard to detect. Because of this, passive failures are sometimes converted into active failures by biasing the first stage of the servovalve so that, in normal operation, zero current does not correspond with zero flow. Biasing is also often used to obtain a preferred polarity of failure. A biased first stage will ensure a preferred hardover direction in the event of the loss of the electrical command. With a conventional EHV zero current will correspond to zero flow but with a biased valve a current must be applied to achieve zero flow and this performance is illustrated by Figure 4.

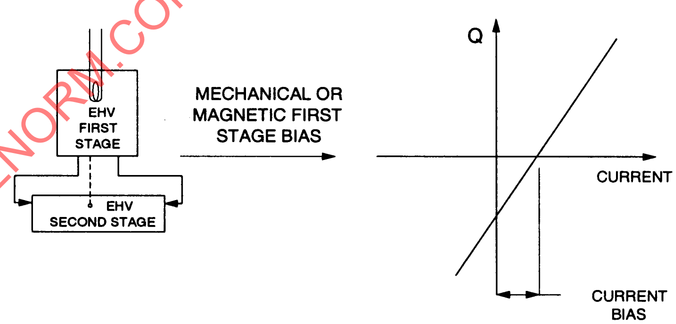

FIGURE 4 - Biased Servovalve Operation

It is now conventional for FBW spoiler actuators to achieve fail-to-retract in this manner. Similarly, a spring bias of the second stage will give a preferred hardover direction if the first stage loses its ability to provide a force to control the second stage. It is sometimes used for other reasons such as to ensure that the second stage is open at start up or following loss of supply pressure. In normal operation this type of bias will be suppressed by the first stage pressure gain and will not provide a hardover second stage as a result of, for example, an open coil.

4.4.2 Where to Detect Failure: The sooner an active failure is detected and dealt with, the smaller will be the failure transient. Ideally then, active failures of the first stage of an EHV should be detected at the first stage. Detection at the second stage is second best and detection at the servoactuator output is likely to give the worst transient. In practice, detecting failures at the first stage must be approached with care because of the non-linearities of the device and because this method will usually not detect a jam of the second stage. Reliable detection at the output of a surface actuator is difficult to do because a good actuator will exhibit a wide range of performance due to the wide range of applied loads, as discussed in 4.9. Most often then, EHV failures are detected at the second stage, helped by the linearity of the torque motor and of the feedback wire spring which together make the relationship between the current and the EHV spool position very linear and therefore predictable.

4.5 Direct Drive Valve Failure Detection:

DDVs use an electrically powered force motor to position the high-power valve spool directly. They usually employ multiple-coil redundancy wherein three or four electrical channels each drive a separate coil within a common magnetic structure to control the output of the DDV through the summation of magnetic flux. A typical single-stage DDV is shown in Figure 5. A linear force motor design is shown. Rotary force motors are also frequently used.

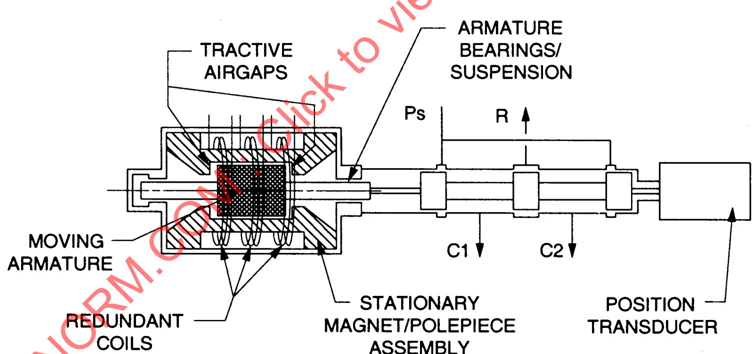

FIGURE 5 - Typical DDV

Those DDVs that use tractive air gaps employ centering springs to cancel the negative magnetic spring rate and to help the force motor to generate a chip-shearing force to return the spool to the zero flow position. In order to provide the resolution required for primary flight control an electrical loop is invariably closed around spool position. However, the presence of the centering spring means that a few watts of electrical power must be applied to hold the valve wide open.

Providing for the detection of the active failure modes of an EHV causes much of the typical hydromechanical complication shown in the examples of 5.1, 5.2 and 5.3. DDVs may suffer from passive failures caused by coil opens and spool jams but they do not have the potential for active pilot stage failures. The application of DDVs to flight control has therefore allowed the introduction of actuators that are much simpler hydromechanically.

4.5 (Continued):

Coil opens and shorts may be detected with “high-end” cross-channel voltage level comparisons or in-line modeling of the loaded servoamplifier. The short failure is a special case because the currents in the non-failed coils that result from the mutual inductance cause poorer dynamic performance than in the open failure case. Because of the large inductance portion of the impedance of the typical DDV coil, this effect is much more marked with a DDV than with an EHV. The algorithm required for the diagnosis of a short failure is more complicated than that for an open failure but has been shown to be practicable.

Flight control DDVs typically have a chip-shearing capability in excess of 100 lb and are provided with perhaps 10 to 50 watts of electrical power to achieve it. Even though this force level is high compared with the force normally required to operate the spool valve, it is much lower than the force levels designed into previous generations of hydromechanical flight control servoactuator and carried over into EHV FBW servoactuators. Consequently, the provision of reliable detection of a jam and the ability to reconfigure the servoactuator following the jam is always considered to be mandatory. Reconfiguration is achieved, as it would be with an EHV servoactuator, with a solenoid-driven bypass valve operated by the failure logic. The jam-failure detection logic could be performed hydromechanically but the electronic approach is lighter, cheaper and more reliable.

Figure 6 illustrates the typical logic tests for a jam:

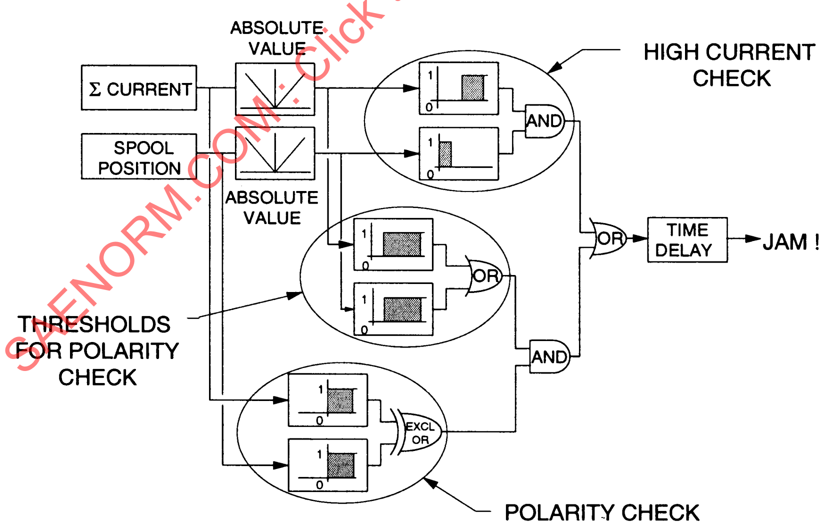

FIGURE 6 - DDV Jam Detection Logic

4.5 (Continued):

They are listed as follows:

- A sustained high current with the spool close to null.
- A sustained polarity error between current and displacement, outside a threshold for current.
- A sustained polarity error between current and displacement, outside a threshold for displacement.

It should be noted that the absence of a pilot stage often causes the DDV to require a high electronic gain, at least for higher-performance applications. This high gain, in combination with minor null biases between channels, would drive adjacent channels into opposite-sense saturation, causing problems with performance, power consumption and failure-detection, if cross-channel current equalization or voting were not used.

4.6 Linear and Rotary Variable Transformer Failure Detection:

Linear and Rotary Variable Differential Transformers (LVDTs and RVDTs) are invariably in-line tested and sometimes cross-channel compared. The in-line testing requires a center-tapped secondary winding. The center tap allows the individual output voltages to be measured with respect to ground and then summed for failure detection. By contrast, the difference, which could be measured without a center tap, is the proportional output normally used for control. For failure detection, the sum of the voltages is compared with a minimum expected value to provide confirmation that the excitation voltage is reaching the LVDT, that the LVDT has retained its continuity and that all three secondary leads are correctly connected to the electronic set, as illustrated by Figure 7. This failure detection method detects all opens, shorts across the primary and shorts to ground of either output but not an isolated "high-to-low" short of the output. Detection of this last type of fault requires a "six-wire" LVDT allowing the output voltages of the two halves of the secondary to be measured separately in an isolated manner.

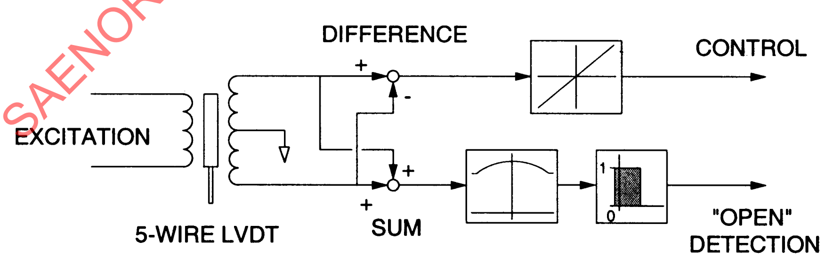

FIGURE 7 - LVDT Failure-Detection

Rotary variable differential transformers supplied with only four wires, for situations where in-line testing is not required, are sometimes called "RVTs".

4.6 (Continued):

It may be noted that “ratiometric” LVDTs are wound to provide an output voltage sum that is constant over stroke. The demodulation of this type of LVDT is arranged to provide a normalized output, of difference divided by sum, which is independent of supply voltage and much less variable with temperature.

4.7 Logic Valve Failure Detection:

Logic spool and sleeve valves are usually spring-loaded, sometimes pressure-loaded, to the “safe” position required to deal with a failure. By definition they are not proportional and usually see a sudden reversal of polarity of a generous applied force at the time they are required to move. Consequently, they are normally very reliable devices despite the potential for silting of the lap-fits. Nonetheless, the consequences of say, a bypass valve jammed in the normal position when it is needed to shutoff a hardover valve, could be disastrous. Consequently, such valves are customarily periodically ground-tested. Sometimes the correct switching operation can be confirmed by two comparative performance tests. Sometimes it is inferred from the operation of another device. For example, the bypass for an EHV can be arranged to turn the hydraulic pressure to the EHV on and off, as illustrated by Figure 8.

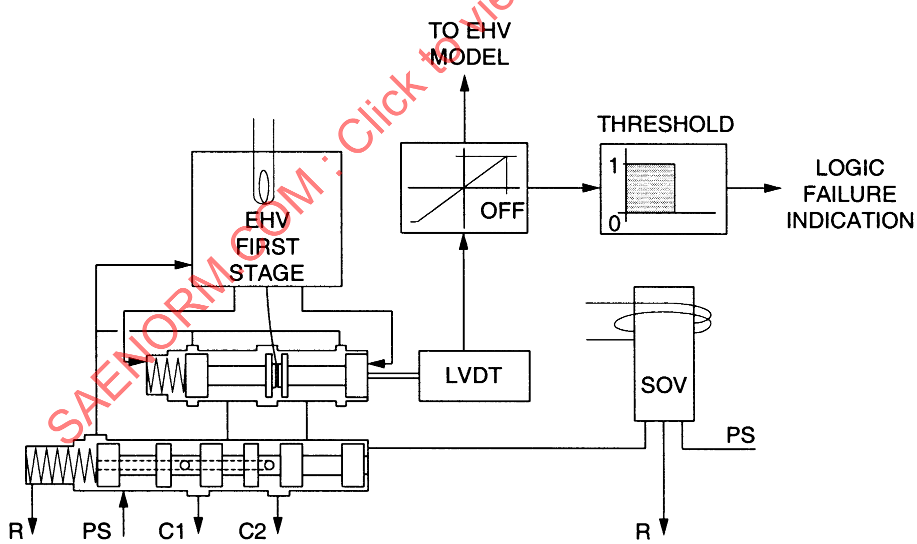

FIGURE 8 - Logic Valve Failure Detection

Then, if the EHV second stage is spring-loaded hardover at loss of pressure, the ability of the bypass spool to move as the solenoid valve is energized and deenergized is confirmed by the output of the second stage LVDT. This approach is used in the V-22 servoactuators

4.8 Solenoid Valve Failure Detection:

The scheme described above and shown in Figure 8 also allows the solenoid pilot valve function to be completely checked. More often the diagnostic method is less complete. Voltage and current monitoring can detect coil opens and shorts, respectively. Mechanical jams are avoided by the use of poppet-type valves and protection against leakage of the poppets is provided with three-way valves so that any seepage from pressure or to return is made insignificant by the vent to return or the opening to pressure.

4.9 Outer Loop Modeling:

The F-111 Series Damper servoactuator made successful use of outer loop monitoring. However, that actuator was a secondary actuator so that it was only exposed to linkage friction and inertial loading.

By contrast, the modeling of the output position of a surface actuator is difficult because of the wide variation in servovalve output that results from the power drawn from the actuator. Although information about the varying hinge moment demanded from the actuator is often available from differential pressure transducers provided for other reasons, such as load damping, the varying hydraulic pressure supplied to the actuator is rarely known. In consequence, outer loop modeling, illustrated in Figure 9, needs generous fail-detect thresholds and is normally included only for final failure detection.

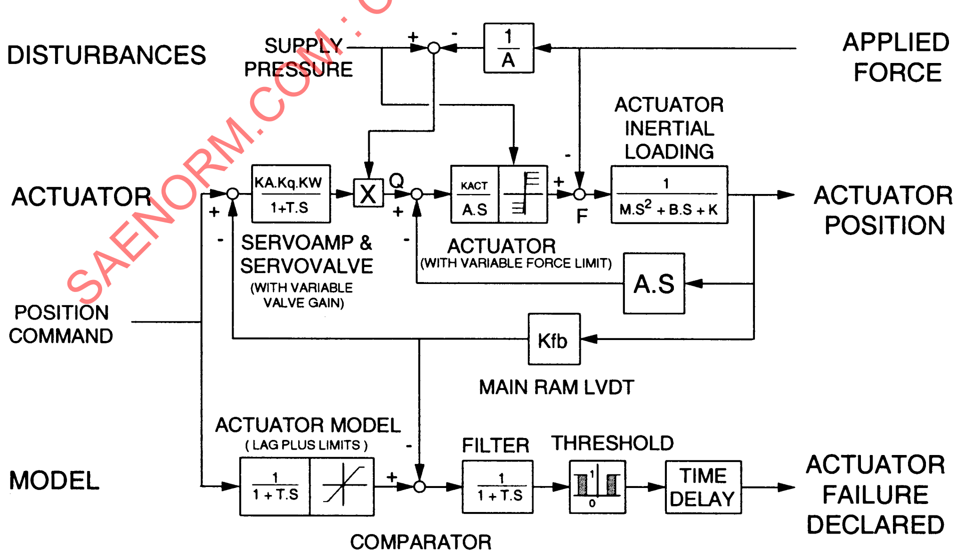

FIGURE 9 - Outer Loop Modeling

5. SERVOACTUATOR FAILURE DETECTION DESCRIPTIONS:

5.1 F-111:

The F-111 is a fighter/bomber aircraft. Its flight control system is mechanically commanded with electronic augmentation in each axis provided by the redundant series servoactuator, the failure detection for which is described in this section.

5.1.1 Series Augmentation Servoactuator Configuration: The actuator is a small, equal-area, dual-tandem design, controlled by two two-stage EHVs, force-summed at the actuator. This design can be said to be the forerunner of today's FBW servoactuator. In fact, these servoactuators were used in the YF-16 to provide FBW pilot commands to the hydromechanical surface servoactuators. More information about the flight control actuation system may be found in AIR4094 and "Aircraft Flight Control System Design".

5.1.2 Actuation Architecture: The design featured a very simple electrical interface. The outer loop closure is mechanical so that the current commands to the EHVs are proportional to the required output position and the actuator is turned on and off with latching solenoid valves. The servoactuator is complex hydromechanically. It uses two hydraulic systems and three electrical commands each driving a two-stage EHV. Two EHVs operating on different hydraulic systems power the tandem actuator while the third EHV drives a small actuator that models the servoactuator position output. Figure 10 shows the F-111 actuator in much simplified form

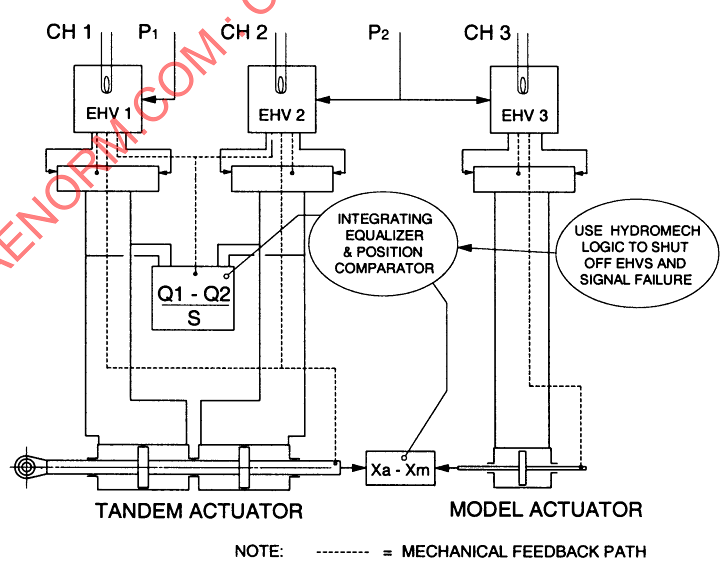

FIGURE 10 - F-111 EHV Failure Detection

5.1.3 Failure Detection: The two functional valves are hydromechanically equalized for good performance through mechanical feedback from the integrating equalizer. The equalizer compares the differential output pressures of the two operational EHVs and provides equal and opposite feedback to each valve. If the equalizer approaches its limited authority to equalize, a failure is indicated and the third channel determines which of the two functional channels can be allowed to continue to control the output. This decision is made through a polarity check conducted by a device comparing the positions of the actuator and the model actuator.

If the remaining functional EHV or the model EHV were to fail, the model position discrepancy would cause the actuator to shut down if one functional valve had already been lost or the model to shut down if both functional EHVs were still operative.

It is noteworthy that the failure-detection comparisons are at the level of the integrated second stage output and that the loop closures around this output are made with linear mechanical springs. These springs suppress the non-linearities within the EHVs, except those of the torque motors, which are very linear devices, provided saturation effects are avoided.

5.2 Tornado:

The Tornado is a multiple-role combat aircraft. Its flight control system is full FBW with backup, mechanical command reversion. This section describes the failure detection for the Taileron servoactuator that provides control of the differential horizontal tail surfaces.

5.2.1 Taileron Servoactuator Configuration: The Tornado Taileron servoactuator is a partially balanced dual tandem design. The principal mode of control is full FBW. The actuator has a full mechanical reversion feature that enables a smooth and immediate transfer of control from electrical to mechanical signaling, either automatically or upon the pilot's command. More information about the flight control servoactuators may be found in AIR4253.

5.2.2 Actuation Architecture: Figure 11 shows a schematic of the overall FBW control system. Pilot's demand (stick position) and flight data are processed by a triplex Command and Stability Augmentation System (CSAS). The last voter/monitor stage of the CSAS converts the three input lanes to four output lanes for feeding the Taileron actuator, which is quadruplex to match the dual hydraulic supply. This actuator incorporates a complex sub-assembly called the quadruplex actuator, which performs two important functions. It converts the CSAS electrical output signals into a mechanical input signal to the actuator main control valves that control the ram position, and it also allows for variations between the four CSAS electrical lanes. Should there be a substantial variation in one lane, then the quadruplex actuator automatically isolates that CSAS lane from the common mechanical input to the main valves.

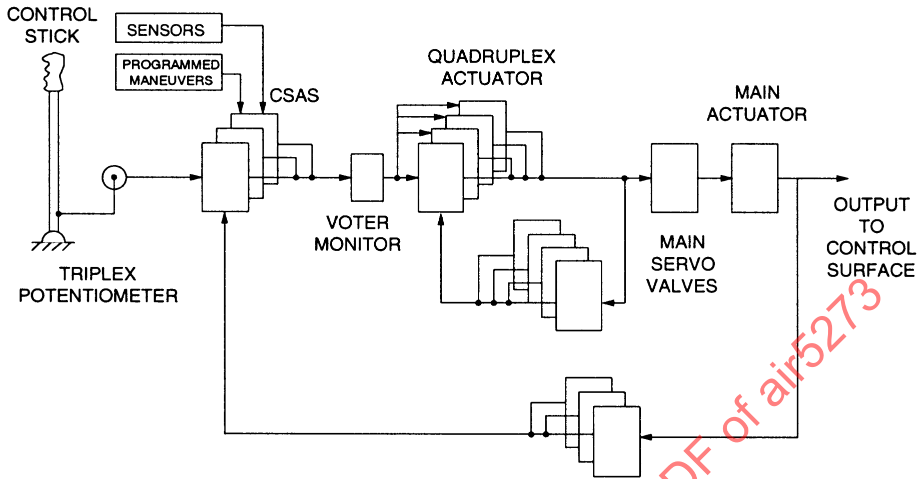

FIGURE 11 - Tornado Taileron Actuator FBW Control Architecture

5.2.3 Failure Detection: Each of the quadruplex actuator input lanes commands a separate electrohydraulic servo valve that governs the position of a small hydraulic actuator with feedback from a D.C. potentiometer. Thus, the four electrical inputs are converted to four independent mechanical movements. The four actuators drive ‘connecting rod’ links, each of which rotates a clutch plate that is hydromechanically loaded onto a driven plate secured to the output shaft. The variable degree of coupling between the clutch plates and the output shaft enables the quadruplex actuator to:

- Operate with four lanes functioning, despite minor disagreements.
- Disconnect any lane whose degree of disagreement exceeds a critical value.
- Disconnect all operating lanes in the event of multiple faults.

The disconnect coupling comprises three conical pegs projecting axially from the face of each driven plate and normally mating with detent sockets in the corresponding face of each clutch plate. With hydraulic power on and all lanes operating, the four actuators drive four clutch plates arranged in two pairs, each pair gripping a driven plate between them. The whole assembly moves together and establishes a consolidation of the output displacements of all four control lanes in the inner loop. In the event of the output of one lane seriously differing from the other three, the output consolidation favors the three concurrent lanes. Minor deviations are accommodated by the detent sockets of the clutch plates, riding away from the conical pegs on the driven plates against the clamping force of hydraulic clutching pistons inside the hollow output shaft. This allows each clutch plate to move through an angle of about 4° relative to its mating driven plate, which represents twenty per cent of the total lane displacement in that direction.

5.2.3 (Continued):

Once the disagreement in any lane causes the relevant clutch plate to move through a relative angular distance greater than approximately 5° the axial travel of that clutch plate along the output shaft becomes sufficient to cause effective disengagement. A spring-loaded latch plate drops between the clutch plate and driven plate preventing the faulty lane from being re-engaged (until the latch plate is deliberately manually raised). The axial travel of the clutchplate closes a switch signaling a failure of that lane. Further rotation of that clutch plate, such as would occur with a faulty hard-over signal, carries the detent sockets out of engagement with the conical pegs of the driven plate, so that the torque it can transmit is effectively zero. The output drive thus continues to be maintained by the three surviving channels.

Two of the quadruplex channels are supplied from one hydraulic system, while the remaining two channels are supplied by the other hydraulic system. The clutch plate loading pistons are energized in pairs from the two hydraulic systems and clamp the quadruplex top shaft assembly axially overcoming the separating force from concentric pairs of coil springs. In the event of failure of either hydraulic system, these springs push apart the two affected clutch plates until they are no longer in engagement with their driven plate. This is again signaled as a fail-operate condition (if no other failure has previously taken place).

The system continues to function on at least one hydraulic system and at least two correctly operating electrical channels. Any further fault, however, will cause an immediate reversion to mechanical signaling.

5.3 Space Shuttle Orbiter:

The Space Shuttle Orbiter is the reusable “Spaceplane” currently employed for delivery of payloads such as satellites to low earth orbit. This section describes the failure detection employed by all of the full FBW flight control and thrust vectoring servoactuators.

5.3.1 Actuator Configuration: The Space Shuttle Elevon flight control and the Thrust Vector Control servoactuators are all equal-area, single-chamber designs. They are controlled by four two-stage EHVs and supplied with two or three hydraulic systems, selected for use by integral switching valves. More information about the flight control servoactuators may be found in AIR4253.

5.3.2 Actuation Architecture: The actuators employ a quad-channel, brick-walled arrangement. The four channels of control are brick-walled down to a mechanical summing point at the Main Control Valve (MCV). Each of the four electronic channels drives a separate EHV and the pressure outputs of the four EHVs are force-summed, in a majority-vote manner, at four pistons rigidly coupled to the MCV. To aid this force summing the two-stage EHVs use internal pressure feedback for reduced pressure gain.

5.3.3 Failure Detection: The four EHV pressures are in-line equalized, to maintain the brick-wall. That is, the output pressure of each EHV is measured with a pressure transducer and an attempt is made to hold this pressure down to a third of supply pressure with an integrating, equalizing circuit of limited authority. If this equalization runs out of authority and the pressure climbs above the fail-detect threshold a failure of the control channel is declared.

The fail-detection portion of the flight control actuators is illustrated in Figure 12.

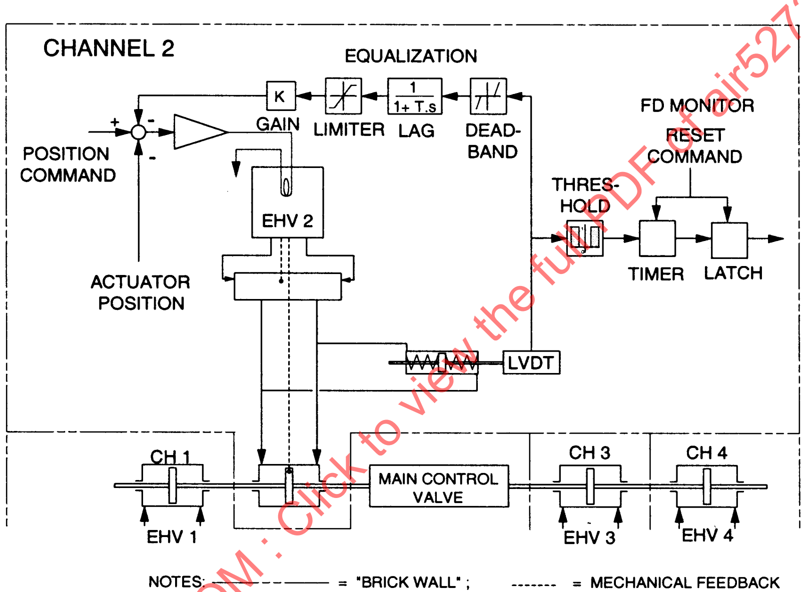

FIGURE 12 - Space Shuttle EHV Failure Detection

This failure detection method is a brick-walled, electronic equivalent of one of the hydromechanical methods used in the F-111 servoactuator. The corrective action is to depressurize and bypass the failed EHV with a solenoid valve. Note that this in-line equalization works because the EHV output summation is at a secondary level, that is, the EHVs are not providing the actuator output force directly.

5.4 F-16:

The F-16 is a single-engine fighter aircraft. This section describes the failure detection used for all of the full FBW primary flight control servoactuators.

5.4.1 Actuator Configuration: The F-16 flight control servoactuators used to control the stabilator, rudder and aileron primary flight control surfaces of the F-16 show a close family relationship to the F-111 series servoactuator approach. The control is integrated with the power actuator, the electrical interface remains simple and the hydraulic schematic remains complex compared with some of the later examples provided in subsequent sections. More information about the flight control actuation system may be found in AIR4094, AIR4253 and "Aircraft Flight Control System Design".

5.4.2 Actuation Architecture: Like the F-111, the F-16 servoactuators are dual hydraulically and triplex electrically with each electrical channel commanding a separate two-stage EHV. Two of the EHVs are flow-summed to drive a modulating piston that drives the tandem MCV. This provides the velocity command to the power actuator. The third EHV is arranged to drive a second MCV modulating piston half the size of the first, in an active-standby manner.

5.4.3 Failure Detection: Figure 13 shows only the EHV diagnostic elements.

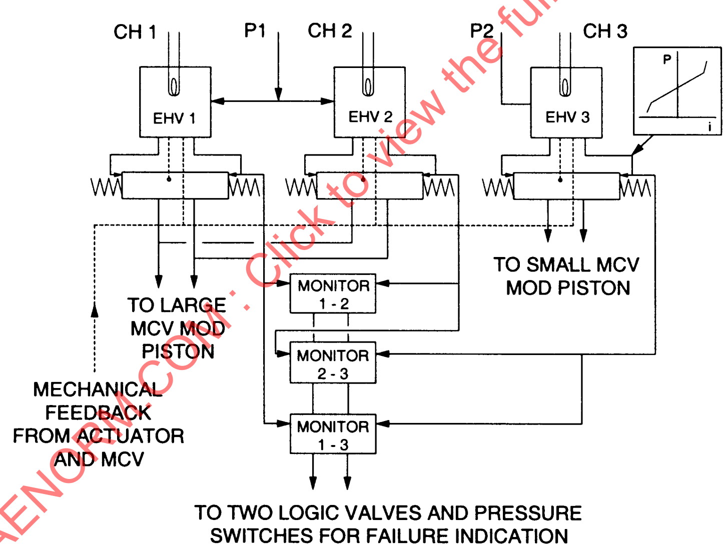

FIGURE 13 - F-16 EHV Failure Detection

The three servovalves are compared in pairs for failure detection. The comparison uses the first stage pressures from the EHVs but is not corrupted by the first-stage non-linearities because of an interesting feature of the EHV design. The first stages are designed to have a high-pressure gain and the loop is closed around the second stage with a conventional feedback wire. However, the second stage also has a centering spring so that a proportional first-stage differential pressure accompanies an achieved second stage position. The elegance of this feature is degraded to a degree by the single-ended pressure comparisons but single-ended comparators are simpler than differential comparators since they need only two driving areas instead of four.

5.5 F/A -18 C/D:

The F/A-18 C/D aircraft is a Naval dual-role fighter/attack aircraft with two engines. The flight control systems are full FBW with a mechanical command reversion capability at the Stabilator Servoactuator only. This section covers failure detection for all of the primary and high lift actuation.

5.5.1 Actuator Configuration: The Aileron and Rudder servoactuators are single-chamber, single-hydraulic-system designs controlled by a single two-stage EHV. The Stabilator and Trailing Edge flap Servoactuators are dual hydraulic-system designs controlled by two pairs of single-stage EHVs. The mechanical actuation system for the Leading-Edge Flap for each wing is separately powered by a single hydraulic motor and controlled by a servocontrol containing a single EHV. The Aileron, Rudder, Leading Edge flaps and Stabilator actuation are all provided with a backup hydraulic supply through upstream switching valves. More information about the flight control actuation system may be found in AIR4094, SAE Paper 831484 and "Aircraft Flight Control System Design".

5.5.2 Actuation Architecture: The flight control system is centralized with a quad-channel digital Flight Control Computer (FCC) divided into two, separated, dual channel Weapons Removable Assemblies (WRAs). Its normal mode of operation is full FBW but the Stabilator servoactuators provide mechanical pitch and roll command reversion capability. Each of the two engines powers a separate hydraulic pump pressurizing two, separate, Reservoir-Level-Switching (RLS) "branches". The electrical commands are "flux-summed" at the actuators though the use of multiple-coil EHVs. The Aileron, Rudder and Leading Edge flap actuation are all provided with dual-coil EHVs and dual electrical commands for Fail-Operate / Fail-Safe (FO / FS) electrical command redundancy. The Stabilator and Trailing Edge servoactuators employ quad coils in each EHV in each pair, receiving four electrical commands for Double-Fail-Operate / Fail-Safe (FO^2 / FS) electrical redundancy.

5.5.3 Failure Detection:

AILERON AND RUDDER ACTUATION: Failure monitoring of each actuator within each command channel of the FCC is as follows:

Servovalve: The EHV is a conventional two-stage design with mechanical feedback of the second stage position. This position is also monitored with a dual LVDT for failure detection. Each of the two driving FCC channels compares its dedicated EHV LVDT output with the output of a servovalve model. This model employs a first order lag to represent the EHV dynamics and is driven by the sum of the command currents from the two channels driving the EHV. Loss of the pressure supply to the servoactuator is detected with an integrated, dual pressure switch. The switch discretes are used to prevent the EHV failure detection from latching during the transition time for the upstream switching valve and, in the event of an extended loss of pressure, to declare failure regardless of the EHV monitor status.

5.5.3 (Continued):

Servoamplifier: All of the electronic forward and feedback path elements are modeled in each FCC channel. The model accepts the position command signal and the undemodulated actuator LVDT position feedback signal and generates a model EHV command current. This model current is compared with the actual current supplied by the same channel.

Command Signal: The actuator command signal is compared to the signal wrapped around through the model path. A failure is declared if the error exceeds a specified value.

Main Ram LVDT: The LVDT is center-tapped and the sum of the output voltages is monitored to allow the detection of open failures and most short failures.

LEADING EDGE FLAP ACTUATION: The monitoring of this actuation system is essentially the same as that for the Aileron and Rudder servoactuators, though the EHVs employ electrical rather than mechanical feedback of second stage position. The system employs two additional monitors:

Broken Shaft Monitor: A command versus position monitor examines the inboard shaft position. This monitor detects internal hydraulic motor failures.

Asymmetry Monitor: The inboard and outboard flap positions are compared to detect, for example, a broken torque shaft. This monitor also controls the engagement of the asymmetry brakes to prevent any additional asymmetry.

STABILATOR AND TRAILING EDGE FLAP ACTUATION: The failure monitoring for these components is as follows:

Servovalve: As shown in Figure 14, there are four EHVs in each actuator, used in a dual-pair arrangement, each pair pressurized by a separate hydraulic system. The EHVs are single-stage, four-way, quad-coil valves and are commanded by all four FCC channels. Each pair is provided with a differential pressure sensor for detection of EHV hydromechanical failures.

Each four-way EHV provides only one active output pressure for control so that a pair of EHVs drives two areas on the MCV. The two inactive ports are coupled together to produce a reference pressure that is compared with the average of the two control pressures by a differential pressure sensor. A hydromechanical failure of either EHV, such as a plugged orifice, will unbalance this pressure relationship. If the imbalance exceeds a spring detent threshold, the sensor piston will move and drive its quad LVDT to provide a failure indication to each FCC channel. The result is depressurization of the pair of EHVs through a quad-coil solenoid valve and the servoactuator continues to operate on the remaining pair of EHVs. These servoactuators are therefore FO/FS for hydromechanical EHV failures.

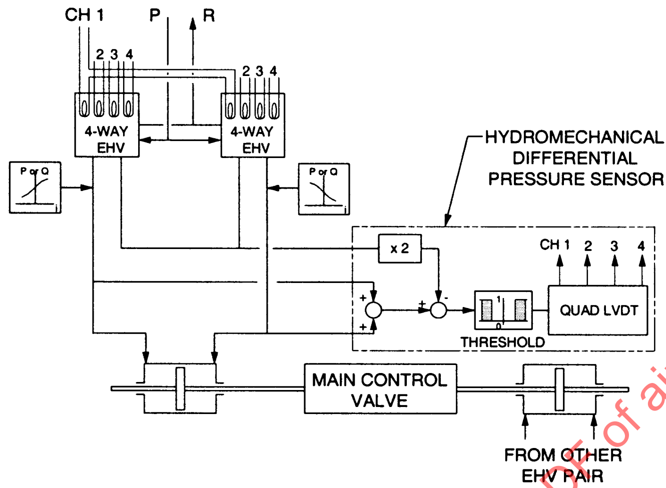

FIGURE 14 - F/A-18 C/D Servovalve Failure Detection

5.5.3 (Continued):

Servoamplifier: The servoamplifier is modeled within each FCC channel and the model output current is compared with the actual current for failure detection. The model inputs are the inner loop position command voltage and the inner loop position feedback signal so the model also includes the inner loop-summing junction.

Commands, Feedback LVDTs and Inner Loop: The inner loop or MCV position servo, referred to as the “servo ram”, is provided with a monitor capable of detecting many types of failures. This monitor models the servo ram with a rate-limited first-order lag, receives the inner loop command voltage as an input and generates a model servo ram position for comparison with the actual position. This position is the result of all four commands. Since the commands are averaged in the forward path by flux summing and since the inner loop is closed electrically the position achieved is negligibly affected by the failure of any one channel. As a consequence of this, without resorting to cross-channel comparisons, this in-line monitor can detect failures of the servo ram, the inner loop LVDT, the main ram LVDT and the command signal.

TEF Asymmetry: The left and right TEF positions are compared to detect asymmetries. A failure of this type will cause both actuators to drive to 0°. This failure detection is disabled while in autoflap up mode.

5.6 LAVI:

The LAVI is a single engine fighter aircraft with a full FBW flight control system. This section covers failure detection for the servoactuators for the elevon, rudder and canard primary flight control surfaces.

5.6.1 Actuator Configuration: The actuators are equal-area, dual-tandem, full FBW designs and use conventional EHVs. More information about the flight control servoactuators may be found in AIR4253.

5.6.2 Actuation Architecture: The flight control system is centralized and the Digital Flight Control Computer (DFCC) has four cross-compared channels. The actuator EHVs are single-stage valves, force-summed on separate drive areas on the dual-tandem, spool-type MCV which controls the flow from the two hydraulic systems to power the actuator. The actuators achieve FO^2/FS performance, with respect to electrical failures and this electrical redundancy is independent of the dual-system hydraulic redundancy, because of the use of multiple-coil EHVs. The actuator commands generated by all four channels of the DFCC are provided to all of the servovalves in series so that, following loss of one hydraulic system, the valves pressurized by the remaining good system continue to be commanded by all four channels.

5.6.3 Failure Detection: As shown in Figure 15, there are four EHVs per actuator in a dual-pair arrangement, one pair pressurized by each of the two hydraulic systems. Each pair of valves generates two control pressures, like a single four-way servovalve, which are used to drive a pair of areas on the MCV. The pressures are also summed and compared with the differential supply pressure to the servovalve pair, for EHV failure detection. This summation and comparison is performed hydromechanically with a centerline that opens four switches to signal all four computer channels when the difference exceeds a threshold set to the equivalent of more than 10% of torque motor authority. This failure detection can only detect EHV failures and cannot detect command failures since each of the two summed pressures is controlled by all four command signals from the DFCC. DFCC failures then are detected upstream by a combination of self-monitoring and cross-comparison.

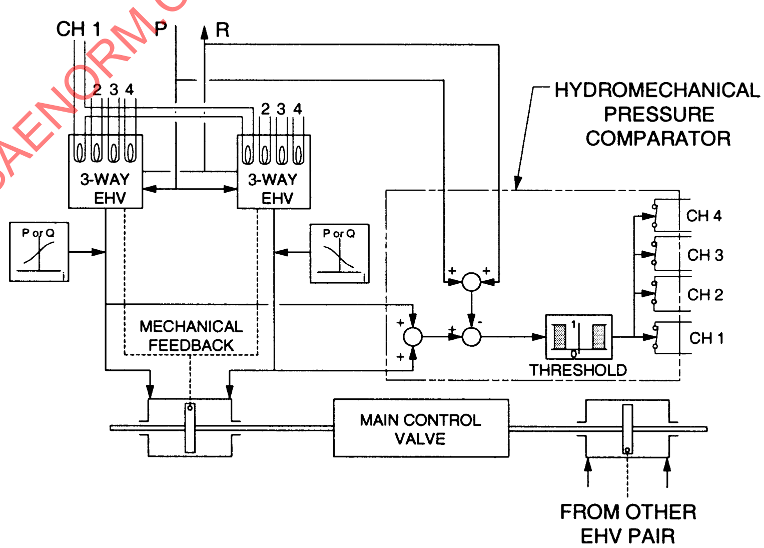

FIGURE 15 - LAVI Servovalve Failure Detection

5.6.3 (Continued):

IBIT checks the status of the fail-detect centerline by introducing an electrical imbalance between the two EHVs it monitors, using an intermediate tap in the series electrical connection mentioned in 5.6.2.

5.7 X-29A:

The X-29A is an experimental Forward-Swept-Wing aircraft. The aircraft employs a full-FBW flight control system with F-16 servoactuators used for all but one of the surfaces. The exception was the Aft Body Strake surface that was powered by a servoactuator designed specifically for the X-29A.

5.7.1 Actuator Configuration: The X-29A has two strake surfaces, each positioned by a dual tandem actuator. A pair of EHVs described below controls each half of the actuator. Each actuator is powered by dual 3000 psi hydraulic systems. More information about the flight control actuation system may be found in AIR4094 and “Aircraft Flight Control System Design”.

5.7.2 Actuation Architecture: The X-29A employs triplex digital flight control computers in a brick wall arrangement with an analog reversion mode.

The Strake actuator operates in an active/standby fashion with a fail-safe mode if all electronic channels fail. The fail-safe mode fully extends the actuator at a restricted rate with a force limitation controlled by built-in pressure regulators. Each half of the dual actuator contains separate mode control valving and a pair of two-stage EHVs. The EHVs coils are triplex.

5.7.3 Failure Detection: Actuator failures are detected by the ram LVDTs and at the EHVs. In the case of the ram LVDTs, in-line failure detection is accomplished by monitoring the transducers’ output summed voltage. If the summed voltage of one of the triplex LVDTs strays outside of a defined tolerance and persistence a failure for the offending channel is declared.

Figure 16 shows a mechanism within each EHV assembly pair that senses a discrepancy between the two EHV spool positions. For differences larger than 25% of stroke a triplex microswitch set is actuated which alerts the flight control computer of an EHV failure, at which point the corresponding half of the tandem strake actuator is commanded to bypass.

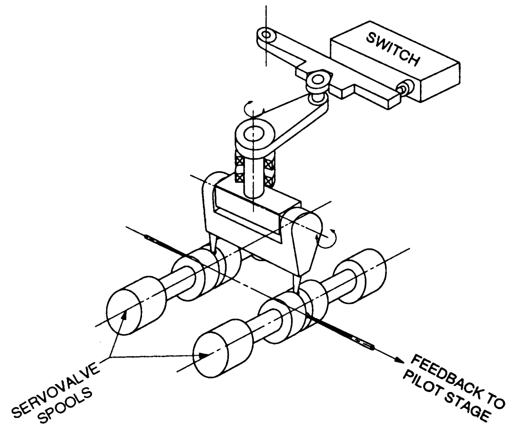

FIGURE 16 - X-29 EHV Failure Detection Mechanism

5.7.3 (Continued):

Each EHV pair is a unique arrangement with the valves plumbed in series such that the output of the first EHV serves as the supply (both pressure and return) to the second EHV's second stage. Furthermore, the first EHV has a 50% underlap to supply pressure while the second valve is axis cut. Since all EHVs on an actuator receive the same current commands the second servovalve is the controlling valve while the first (underlapped) servovalve "goes along for the ride" as long as both servovalves are functioning properly. If one of the two EHVs malfunctions and does not respond to commands the actuator position loop commands the valves toward the opposite quadrant from the actual position of the failed valve. Thus the "good" valve spool is opposite in polarity from the failed valve which cuts off the flow to the actuator immediately, thereby stopping its motion, since the two EHVs of a pair are plumbed in series.

5.8 V-22:

The V-22 is a military tilt-rotor transport aircraft with a full FBW flight control system. This section describes the failure detection used by the servoactuators for the swashplate and the flaperon and elevator primary flight control surfaces.

5.8.1 Actuator Configuration: The Swashplate Servoactuator is a tandem design while the Flaperon and Elevator Servoactuators are single chamber designs. They are powered by 5000 psi hydraulic systems and controlled by two-stage EHVs. More information about the flight control servoactuators may be found in AIR4253.

5.8.2 Actuation Architecture: The V-22 employs a triplex, in-line-monitored, brick wall arrangement. The swashplate actuators are flight-critical and therefore are triplex for double-fail-operate performance while the Flaperon and Elevator Servoactuators are only simplex since they are used in multiples at each surface. The system is not completely brick-walled; some interchannel communication is allowed for sensor failure detection and for synchronization and equalization. The flight control dc supplies are appropriately redundant while leak-protected hydraulic system switching valves are used to increase the safety of the flight-critical swashplate servoactuators

5.8.3 Failure Detection: EHV failure detection is achieved by comparison of the second stage position, measured with an LVDT, with that of an electrical model, as shown by Figure 17.

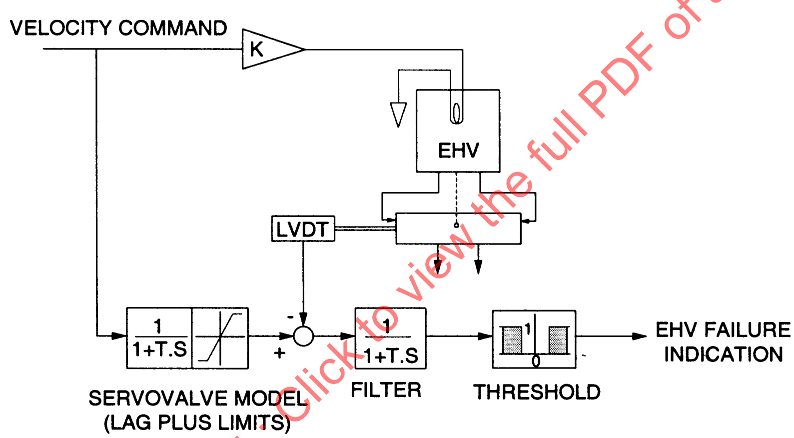

FIGURE 17 - V-22 EHV Failure Detection by Modeling Second Stage Position

This electrical failure detection required the addition of only five wires to the interface rather than the fifteen that would have been required for a triple-coil EHV. The method has the appeal that, ignoring dynamics, spool position will normally be related to the current supplied by the linearity of the torque motor and feedback wire since the non-linearities of the first stage are suppressed by the high internal loop gain of the EHV.

5.9 A319/A320/A321 - A330/A340:

These are medium and large commercial transport aircraft. The general architectures of the actuation systems of the Airbus Standard Body and Long Range families are very similar in principle, the differences being limited to the number of aileron and spoiler surfaces. The servocontrols and the associated failure detection techniques described in this section are also similar in principle though they are sized differently for the two applications.

5.9.1 Actuator Configuration: The Aileron Servocontrol is a balanced-area electrohydraulic actuator incorporating a two-stage electrohydraulic servovalve, a piston-position LVDT, a mode selector valve controlled by a solenoid valve and fitted with an LVDT, inlet/outlet blocking valves, anti-cavitation valves, a compensator and, on A330/A340, a differential pressure transducer incorporating an LVDT.

The Elevator Servocontrol is a balanced-area electrohydraulic actuator incorporating a two-stage electrohydraulic servovalve fitted with a spool-position LVDT, a piston position RVDT, a mode selector valve controlled by solenoid valves and fitted with an LVDT, a feedback mechanism, inlet/outlet blocking valves, anti-cavitation valves, a compensator and, on A330/A340, a differential pressure transducer incorporating an LVDT.

The Rudder Servocontrol is a balanced-area, mechanically signaled, hydromechanical actuator incorporating a control valve, pressure relief valves, anti-cavitation valves and, on A330/A340, a valve-jamming detection switch.

The Spoiler Servocontrol is an unbalanced-area electrohydraulic actuator incorporating a two-stage electrohydraulic servovalve, a piston-position LVDT and anti-extension and maintenance-mode valves.

More information about the flight control actuation system may be found in “Aircraft Flight Control System Design”.

5.9.2 Actuation Architecture: The ailerons and elevators are fitted with two servocontrols in an active / stand-by arrangement. The elevator surfaces drive position transducers independent of the servocontrols. The rudder is powered by three servocontrols active in parallel, the electrical commands to the rudder system being transmitted to the servocontrol input linkage through two electrohydraulic yaw damper servoactuators in an active / stand-by configuration. Each spoiler surface is powered by one servocontrol. The actuators are supplied from three independent hydraulic systems.

Aileron, Elevator, Rudder and Spoiler Servocontrols achieve different operating modes, as follows:

- Aileron Servocontrol: One servocontrol in active mode positions the surface, the adjacent stand-by unit being in damping mode. Change over takes place in the event of loss of control of the active unit. In the event of loss of control of both units they both adopt the damping mode to provide flutter protection.

- Elevator Servocontrol: One servocontrol in active mode positions the surface, the adjacent stand-by unit being in damping mode. Change over takes place in the event of loss of control of the active unit. In the event of loss of control of both units they both adopt a centering mode to hold the surface at neutral. In the event of loss of the hydraulic supply to both units they both adopt the damping mode to provide flutter protection.

- Rudder Servocontrol: The three simultaneously active units drive the surface in parallel.

5.9.2 (Continued):

- Spoiler Servocontrol: In normal operation the unit positions the surface. In the event of loss of control the unit automatically retracts the surface. In the event of loss of hydraulic supply the unit prevents the surface from rising and enables it to retract under the air loads. A maintenance mode enables the surface to be manually moved when depressurized.

5.9.3 Failure Detection: Basic failure detection of servocontrol and other servoloop components is achieved through the monitoring of the following parameters, generally continuously performed by the monitor units of the flight control computers, according to the following general principles:

- Servovalve current: comparison of the commanded and measured currents detects computer / wiring / servovalve failures.

- Servovalve spool position: comparison of the commanded and measured spool positions detects servovalve failures.

- Piston position: comparison of the commanded and measured piston positions detects servovalve / position transducer mechanical failures.

- Mode selector valve spool position: comparison of the commanded and measured spool positions detects computer / wiring / solenoid valve / mode selector valve failures.

- LVDT / RVDT output voltages: out-of-range parameters detect computer / wiring / transducer failures.

- Rudder servocontrol valve jamming signal: detects servocontrol / input linkage failures.

The continuous operation of the above monitoring algorithms may be complemented by periodic ground checks:

- Functional checks of the stand-by servoloops.

- Measurement of the damping coefficient of the damping mode: The maximum rate of an A320 active unit driving the stand-by unit, or the differential pressure information of a stand-by A330/ A340 unit driven by the active unit detect servocontrol failures.

- Functional check of the blocking valves and compensator.

- Functional check of the Rudder servocontrol valve jamming detection system: detects servocontrol / wiring / computer failures.

Implementation of these monitoring techniques, tuning of the associated thresholds and confirmation times, application and periodicity of the ground checks, depend on the criticality of the associated failure modes and the actual purpose of the failure detection function which could be either to cover safety or maintenance requirements. They are not necessarily applicable to all control surfaces.

5.10 C-17:

The C-17 is a military transport aircraft intended for heavy airlift into undeveloped forward areas. This section describes the failure detection employed for all of the full FBW servoactuators for the primary flight control surfaces.

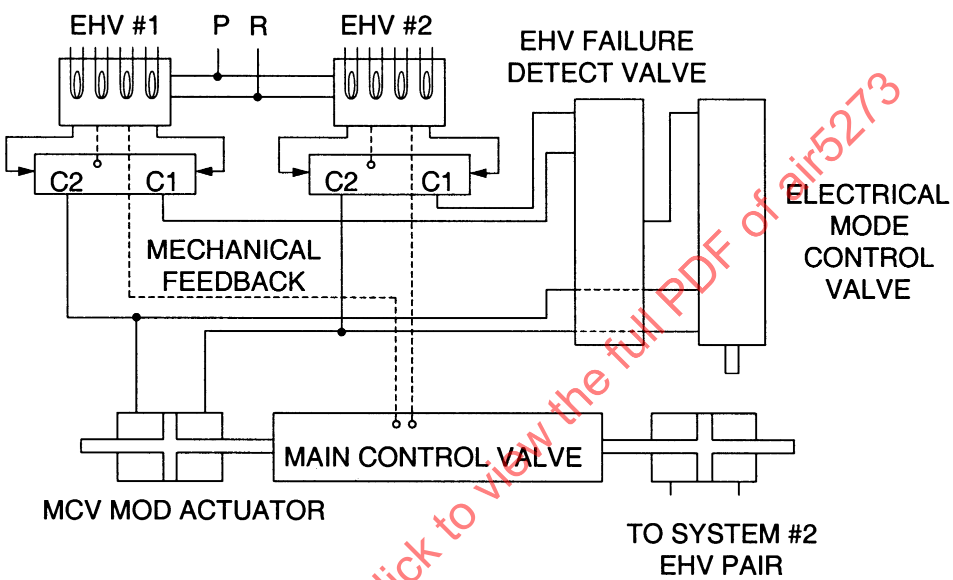

FIGURE 18 - C-17 Integrated Flight Control Module Schematic

5.10.1 Actuator Configuration: Each primary flight control surface is powered by two unequal-area, single-chamber actuators. A dual hydraulic system Integrated Flight Control Module (IFCM) supplies hydraulic pressure to each actuator pair.

5.10.2 Actuation Architecture: The IFCM has two principal modes of operation – electrical and mechanical. In electrical mode, the MCV is actuated by modulating pistons pressurized by flow from EHVs. The MCV is a dual hydraulic system, tandem design and there are two four-channel EHVs per hydraulic system. The mechanical input to the IFCM is decoupled from the MCV when the unit is operating in electrical mode.

Transition from the electrical to the mechanical mode of operation consists of shutting off hydraulic supply pressure to the EHVs and engaging the mechanical input to the MCV via a Mechanical Mode Coupler (MMC) device.

In the unlikely event that both hydraulic systems lose supply pressure or that the electrical and mechanical controls for both systems fail, the surface goes into a damped float mode.

5.10.3 Failure Detection: There are software monitors in the Flight Control Computers that perform a "servo fault detector" function. These monitors are operable when the surface is not at a position where it may be hinge moment limited and check actuator command versus surface movement. Additionally, the C-17 has some of the same fault detection monitors as the F-18 such as: cross-channel surface position monitor; cross-channel servo current monitor; servo-amp monitor (active-model comparison). Detection of a failure causes the EHV Failure Detect Valve to interconnect the hydraulic output of the EHVs, placing the MCV control input for that hydraulic system in bypass.

5.11 B-777:

The B-777 is a large commercial transport airplane. This section describes the failure detection employed for all of the full FBW servoactuators used for the elevator, rudder, flaperon and aileron primary flight control surfaces.

5.11.1 Actuator Configuration: The elevator, aileron, and flaperon control surfaces are each powered by two single-chamber servoactuators. The rudder control surface is powered by three servoactuators. Each servoactuator on a surface is supplied by a different hydraulic system.

5.11.2 Actuation Architecture: Each servoactuator is a single hydraulic system unit with a single electrical channel driving a single two-stage EHV. During normal operation, all the actuators on a surface are actively powering the surface. Most of the actuators have three modes of operation, normal, damped-bypass (or free bypass) and blocked. In the event of EHV failure the bypass solenoid valve is de-energized, forcing the mode select valve into damped bypass mode. If EHV failures are detected on all the actuators on a surface and the surface is near zero position, the blocking solenoid is de-energized, causing the mode select valve to revert to the blocked position. Most of the servoactuators also employ a differential pressure sensor for force equalization. This arrangement is shown in simplified form in Figure 19.

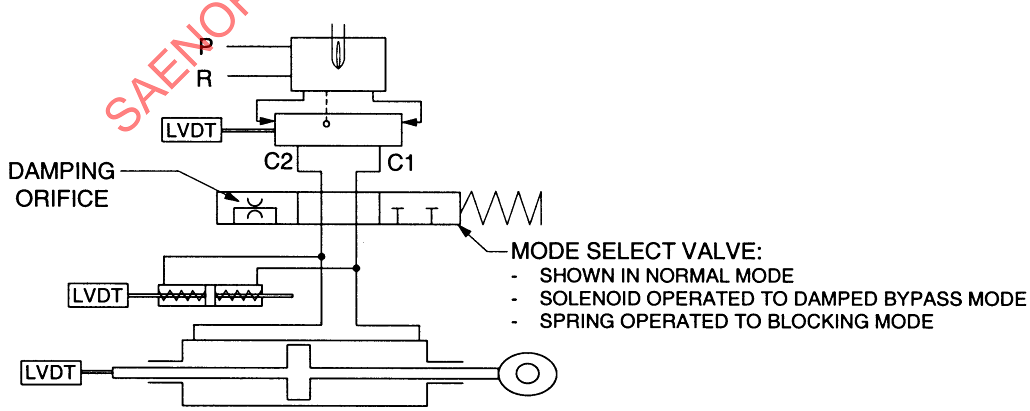

FIGURE 19 - B777 Servoactuator Schematic