Impact of CCV Requirements on Flight Control System Design

J. A. Boudreau*
Grumman Aerospace Corporation, Bethpage, N. Y.

The advent of Controlled Configured Vehicle (CCV) design approaches has imposed severe reliability and fault tolerance requirements on aircraft flight control and supporting systems. This paper establishes the requirements for, and develops the configuration of, an integrated fly-by-wire (FBW) flight control system suitable for an unstable CCV fighter/attack aircraft design. The hydraulic and electric power systems are an integral part of the design problem, since their functions are essential to safety of flight. A three-channel FBW system configuration was chosen as optimum. The system features in-line monitored active/on-line secondary actuators, skewed rate gyros, triplex digital computers, accelerometers, and pilot input transducers.

I. Introduction

THE advent of Controlled Configured Vehicle (CCV) design approaches has imposed severe reliability and fault-tolerance requirements on aircraft flight control and supporting systems. The objective of the study reported in this paper was to establish the requirements for, and to develop the configuration of, an integrated fly-by-wire (FBW) flight control system suitable for an unstable CCV fighter/attack aircraft design. The sensor, computer, and actuator subsystems were addressed, as well as the hydraulic and electric power sources. The hydraulic and electric power systems are an integral part of the design problem, since their functions are essential to safety of flight.

Several advanced fighter/attack aircraft designs were examined to establish generic characteristics and mission requirements. A typical control surface complement was selected and multimode control law requirements were formulated. This enabled determination of the flight control system design requirements, including flight safety, mission reliability, and failure tolerance.

The study approach was twofold. First, several design tradeoffs were performed to examine specific details of the system design for which the optimal approach was not well established. These investigations examined the following areas: 1) hydraulic system configuration, 2) electric power system configuration, 3) self-test/in-line monitoring considerations, and 4) command (secondary) actuator approach. Upon completion of the design tradeoffs, an overall FBW system configuration study was performed. It investigated redundancy requirements, cross-strapping/voting locations, and cost-weight-power tradeoffs.

A significant aspect of this paper is that it examines the applicability of the various redundancy techniques to each subsystem of a FBW system. A blend of these techniques, different for each subsystem, was found to achieve the optimum FBW system configuration.

II. CCV Design Features and Requirements

Several advanced-fighter-type aircraft designs were examined, including the Grumman Advanced Development Composite Aircraft (ADCA) and HiMat designs, the Fairchild-Republic AFTI design, and the Grumman Design 623 V/STOL. All of these designs are statically unstable longitudinally. They are intended to use multimode control laws including direct lift/sideforce control, fuselage pointing, and maneuver load control, to name a few. These designs tend to have more movable surfaces than older more conventional fighter/attack aircraft, but they all have the capability to fly safely on a minimum set of primary control surfaces. A typical set of primary flight controls could be differential and collective horizontal stabilizers (or elevons) for roll and pitch control, and one or more rudders for yaw axis control. Additional secondary flight control devices would be provided for direct force control and to augment control moments for attitude control. Therefore, it seems reasonable to assume that a typical advanced fighter/attack aircraft would require three tail control surfaces for safe flight and additional devices such as maneuver flaps, canards, ailerons, vectorable nozzles, ect., which are required for mission completion. In addition, since the airframe would be unstable, vehicle motion feedbacks would be required.

Control performance studies of unstable CCV designs have revealed that a fixed gain system using rate gyros and accelerometers should be adequate for backup-level flying qualities. Mission requirements, however, dictate variable gains scheduled as a function of air data or calculated using some form of self-adaptive approach. Also, the extensive signal processing and flexibility required by the multimode control laws and the FBW system redundancy management dictate a digital system mechanization. The ready availability of digital air data suggests gain scheduling over self-adaptive techniques; thus it was assumed that air data would be required for mission success.

Reliability goals were established for the complete integrated flight control system based in part on U.S. Navy experience.[1] The goal for flight safety was set at 3.5 failures per million hours; for mission success, it is 350 failures per million hours. These figures include allowance for the electric and hydraulic power systems. Failure tolerance requirements were then formulated based on component reliability data and vulnerability to combat damage. The requirements were set as given below:

Failure tolerance – primary flight controls:
for electrical components, 2 FO/(FS)
for hydraulic components, FO/(FS)
for mechanical components, (FS)

Failure tolerance – secondary flight controls:
for electrical/hydraulic, FO/FS
for mechanical, FS

where FO is fail operative: full capability still available; FS is fail safe: for secondary flight controls, mission completion

Presented as Paper 76-941 at the AIAA Aircraft Systems and Technology Meeting, Dallas, Texas, Sept. 27-29, 1976; submitted Oct. 20, 1976; revision received July 7, 1977.

Index categories: Guidance and Control; Reliability, Maintainability and Logistics Support.

*Group Leader, Guidance and Control. Member AIAA.

not possible, aircraft returns to base; (FS) is fail safe: for primary flight controls, anything less than operational implies loss of control, therefore (FS) implies safe ejection for the crew. These failure tolerance requirements were considered soft requirements, in that if a system met the reliability goals but not the failure tolerance requirements, it could still merit consideration.

Having established requirements for reliability and failure tolerance of the FBW system, certain other requirements were needed to proceed with the configuration definition. The hypothetical fighter/attack aircraft design was assumed to have twin engines. This assumption was necessary to permit selection of the hydraulic and electric power system configurations. Failure transient requirements were needed since the allowable failure transients impact the redundancy management techniques that may be employed, particularly for the command actuators. The failure transient requirements were established according to MIL-F-8785. Level 2 flying qualities require acceleration transients of 0.5 *g* or less, which seems reasonable for the first failure of a FBW system. Note that the actual flying qualities would be expected to remain at Level 1 after the first failure.

The failure transient requirements must be translated into allowable failure reaction times in order to select suitable redundancy management techniques (voting, failure detection, and failure isolation). To do this, time-history simulations were performed using aerodynamic data from the Grumman HiMat, Design 623, and the F-14. The results bracketed the range of response times expected for the hypothetical fighter/attack aircraft. For the case of a stabilizer actuator hardover failure, failure detection and reversal must occur in about 65 msec to meet the first failure requirement. This is the Level 2 requirement in Fig. 1. These results were found to be not strongly dependent on static margin in the region of 0-20% unstable. Controls locked failures in the presence of turbulence are considerably less severe, as shown in Fig. 2. The data in this figure suggests that when such a failure occurs at least 200-300 msec should be available to isolate the failed component.

III. Design Tradeoffs

A typical FBW flight control system is illustrated in Fig. 3. At the beginning of this study, the optimal design approach had to be established in several areas. Specifically, the requirement for ultrareliable hydraulic and electric power sources needed to be addressed. Also, questions concerning the most desirable type of command (secondary) actuator and self-test/in-line monitoring capabilities, had to be answered.

Hydraulic Power System

The purpose of this design tradeoff study was to select the most practical and cost-effective hydraulic system configuration for a FBW, CCV-type aircraft. Since a twin-engine aircraft had been postulated, a configuration with at least two main hydraulic systems was assumed. Duplex power actuators have demonstrated satisfactory reliability in the past and were therefore postulated. Three, 2-failure tolerant command actuators would be used for the fight critical tail surfaces. Because it was not known whether a three- or four-channel command actuator would be chosen, the more general case of four channels was addressed in this study. (Any of the configurations examined can be reduced to three channels by removal of one auxiliary pump or one or more transfer valves.)

The basic approach to formulating configurations was to assume that each main, engine-driven hydraulic system would supply one channel of the command actuators. The remaining command channels would be supplied by electrically driven pumps or by hydraulic transfer valves connecting the main systems. Each command channel must have an independent hydraulic source and no failure may cause the loss of more than one channel. This guideline dictates that the transfer valves must provide downstream leak detection, and be able to prevent loss of fluid from more than one hydraulic system. Four configurations evolved and are shown in Fig. 4.

Referring to the figure, and bearing in mind that reliability and cost are the most important elements in this tradeoff, it is clear that configurations 1 and 2 offer the best compromise. The reliability/vulnerability ratings are lower for configurations with transfer valves because these devices are potentially a single-point failure item. Therefore, configuration 1 is favored. See Sec. V, Selected Configuration Description for more information on the selected configuration.

The reliability analysis performed on these hydraulic configurations uncovered an unforeseen problem. None of the proposed configurations met the mission reliability goal of 350 failures per million hours. The duplex power actuators with a single hydraulic source supplying each half caused the mission abort rate to be 600/million hours. This is based on the ground rule that an abort must occur when one additional failure can result in loss of the aircraft. The proposed solution to this problem for configuration 1 is to supply one side of the

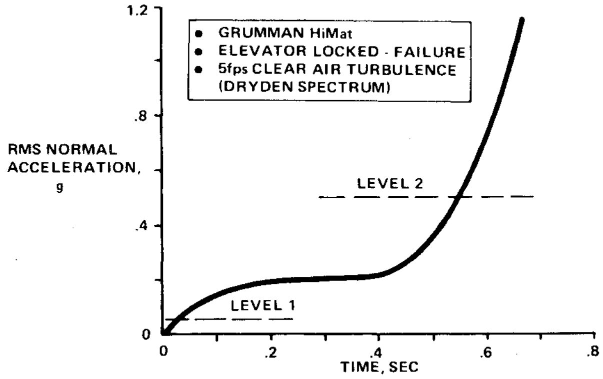


Fig. 2 Normal acceleration propagation with controls locked.

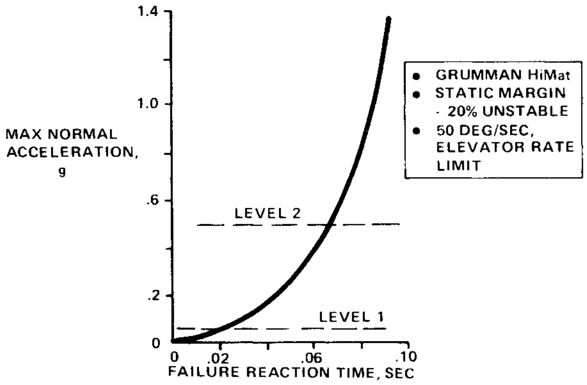


Fig. 1 Elevator hard-over failure transient.

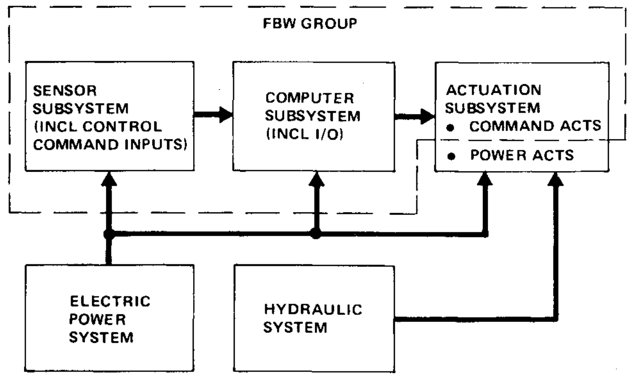


Fig. 3 Typical FBW system.

duplex power cylinders via a transfer valve from one of the auxiliary pumps. With this modification, the approximate reliability numbers for configuration 1, configured for either a three- or four-channel FBW system are: mission reliability, 20 failures/10^8 hr; safety reliability, 20 failures/10^{12} hr.

Electrical Power System

Three electric power configurations (configurations A through C) were developed to support a three- or four-channel, FBW flight control system. Particular emphasis was placed on the electrical power interface, with the goal of transient free power delivery to the FBW components. In addition, it was desired to eliminate the need for batteries, if possible. Configuration A utilizes the aircraft main power distribution system, supplying d.c. power to all the FBW channels. It can employ small dedicated batteries to ensure transient free service. Configurations B and C employ dedicated d.c. power sources for each flight control channel, thereby eliminating bus switching, which is a major cause of power transients. Figure 5 illustrates these configurations for a three-channel FBW system.

Configuration A features dual redundant transformer-rectifiers "T-R's" and dual engine-driven a.c. generators. It incorporates separate a.c. and d.c. bus-tie contactors which inhibit bus transfer subsequent to a bus fault (short). A hydraulic driven, combination a.c./d.c. emergency generator provides sufficient power for safe flight and thus a two-fail operational capability. With this configuration, all channels remain fully operational subsequent to single or dual generator, T-R, or feeder failures. This is because each FBW control channel is supplied power through triple redundant, diode isolated feeders powered from separate buses. This approach also ensures transient-free power for the first generator or T-R failure.

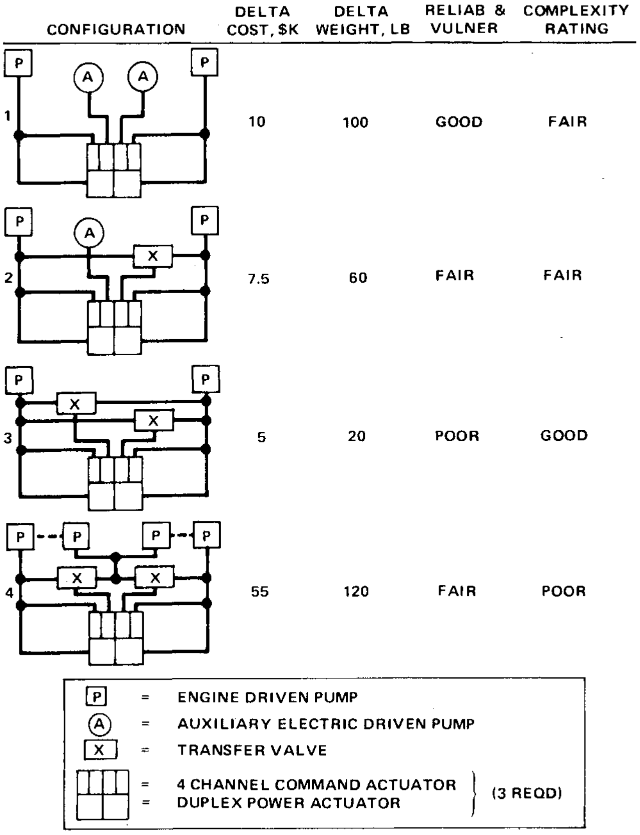
The hydraulic driven emergency generator requires approximately 1 sec to come up to speed following activation. If it is armed (brought on the line) after the first failure, it can then provide power essentially instantaneously after a second failure. However, due to the low design capacity of the emergency generator, a transient low voltage will occur. This transient will cause temporary shutdown of the FBW system, and is therefore unacceptable. The inclusion of a small battery in each channel could enable continuous operation for the fraction of a second duration of the transient. Another option would be to provide a specialized power regulator in each FBW channel which could handle the low voltage level. This device would be considerably heavier, more expensive, and draw more power on a continuous basis than would otherwise be required.

Table 1 Probability of no power to all FBW channels

Configuration	Failures/hr
A (with batteries)	166×10^{-12}
A (no batteries)	6×10^{-12}
B	184×10^{-6}
C	106×10^{-6}

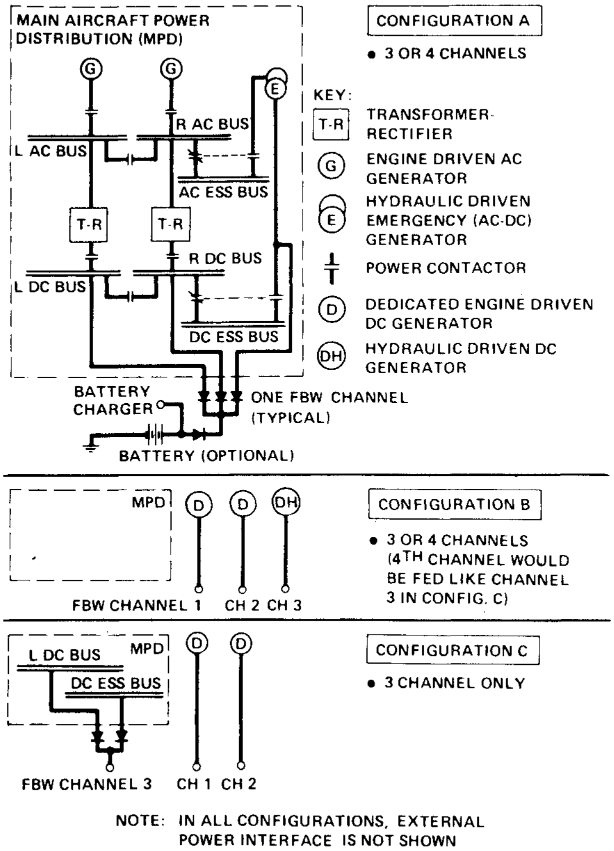
Configurations B and C use dedicated engine driven d.c. generators for two of the FBW channels. Configuration B provides a separate hydraulic driven d.c. generator for the third channel, whereas configuration C supplies the third channel from the main power distribution system. Configuration C, as shown, does not incorporate a battery resulting in an approximate one-second power interruption in the third channel during emergency generator activation. However, the other two channels are not similarly affected during this sequence.

The advantage of configuration B and C is that continuous transient free power is available to at least one FBW channel until a third failure occurs, without the requirement for batteries. The disadvantages associated with these configurations include: 1) loss of a dedicated power supply causes loss of the associated FBW channel; 2) increased system



CONFIGURATION	DELTA COST, $K	DELTA WEIGHT, LB	RELIAB & VULNER	COMPLEXITY RATING
1	10	100	GOOD	FAIR
2	7.5	60	FAIR	FAIR
3	5	20	POOR	GOOD
4	55	120	FAIR	POOR

Fig. 4 Hydraulic system configurations.



MAIN AIRCRAFT POWER DISTRIBUTION (MPD)
G
G
E
R AC BUS
L AC BUS
AC ESS BUS
T-R
T-R
R DC BUS
L DC BUS
DC ESS BUS
BATTERY CHARGER
ONE FBW CHANNEL (TYPICAL)
BATTERY (OPTIONAL)
CONFIGURATION A
• 3 OR 4 CHANNELS
KEY:
T-R TRANSFORMER-RECTIFIER
G ENGINE DRIVEN AC GENERATOR
E HYDRAULIC DRIVEN EMERGENCY (AC-DC) GENERATOR
POWER CONTACTOR
D DEDICATED ENGINE DRIVEN DC GENERATOR
DH HYDRAULIC DRIVEN DC GENERATOR
MPD
D
D
DH
FBW CHANNEL 1
CH 2
CH 3
CONFIGURATION B
• 3 OR 4 CHANNELS (4TH CHANNEL WOULD BE FED LIKE CHANNEL 3 IN CONFIG. C)
L DC BUS
MPD
DC ESS BUS
D
D
FBW CHANNEL 3
CH 1
CH 2
CONFIGURATION C
• 3 CHANNEL ONLY

NOTE: IN ALL CONFIGURATIONS, EXTERNAL POWER INTERFACE IS NOT SHOWN

Fig. 5 Electric power system configurations.

complexity due to the additional generators required; 3) incompatibility with existing engines/accessory gear box arrangements – major redesign of gear box or accessories may be required to incorporate the additional generators.·

A reliability analysis was performed to determine the relative reliability for these configurations as well as the absolute failure rate data necessary for the overall FBW configuration analysis. The results indicate that all the electric power configurations have essentially the same total system failure rate for both mission success and flight safety. However, on a per-channel basis, the reliability data show significant differences. Since the FBW electronics depend completely on ship's power in configuration A, channel redundancy is not a consideration. All channels benefit from the redundancy in the ship's power configuration; even in the most degraded ship's power mode, all channels receive power. This is not the case for the other configurations; therefore, it is useful to compare the probability of having power to all FBW channels. Table 1 shows the comparison in terms of the number of losses of power to one or more channels.

Examination of the data presented suggests selection of configuration A; however, further study is required to establish the better choice between batteries or increased power regulator requirements. Pending such a study, configuration A with batteries is selected.

Self-Test/In-Line Monitoring Considerations

Comparison monitoring has typically been used in the past to obtain failure tolerance in full authority redundant flight control systems. Since this technique depends on majority voting schemes, three channnels are required to provide single-failure tolerance; four channels enable two-failure tolerance. Self-test (or in-line monitoring) has been used in limited authority systems, and, since each channel can separately establish its own failure state, only three are required for two-failure tolerance. Based on this, a study was undertaken to establish where self-test would be desirable in a FBW system.

The three areas considered for self-test implementation were the digital computers, sensors, and actuators. The issue of self-test for actuators was addressed as part of the more comprehensive secondary actuator tradeoff evaluation summarized in the next section.

An essential characteristic of self-test is the so-called coverage that can be obtained for any given component. Coverage will be defined here as the probability of detecting a failure, given that a failure exists. This definition is applicable because the self-test capability would generally be used when two redundant components are available. A comparison of the two outputs from these components will indicate the existence of a failure; the self-test features are then exercised to determine which component has failed. An interesting feature of this definition is that 50% self-test coverage can be achieved by arbitrarily choosing one of the two components (flipping a coin).

A coverage of 95% offers a reliability improvement of a factor of ten over the 50% coverage level. In terms of failure tolerance, only one in 20 failures go undetected. This seems adequate for the second failure in a two-fail operational system. If the cost of implementing self-test functions is less than the cost of an additional channel, then self-test is worthwhile, provided that it enables meeting reliability or fault tolerance goals which would have required adding another channel if comparison monitoring were used.

The implementation of inflight self-test in the digital computer system will make use of the built-in-test (BIT) features. These must be supplied for maintenance troubleshooting. Additional self-test functions will probably be required over the normal BIT, but it seems reasonable to expect that 95% self-test coverage can be achieved. Allen indicates that somewhere between 90% and 99% is practical.[2] That paper also contains additional information on computer self-test capabilities and limitations.

Another aspect of self-test that must be considered is the length of time required to perform the tests. That is, once a failure has been indicated by comparing two redundant signals, how much time is required to isolate the failed component? The failure transient requirements established earlier suggest that for hardover failures only about 50 msec are available. However, an advantage of using digital computers is that they can delay issuance of faulty commands until the causative failure has been isolated. Therefore, the last good command may be held fixed, allowing the controls locked reaction time of about 200 msec to apply.

Self-test for sensors was examined in some detail. It is not easy to achieve a really complete test for vehicle motion sensors since they would have to be physically moved. In lieu of this, electrical stimuli may be applied to the sensing element and/or other forms of electrical monitoring may be implemented to evaluate sensor performance. This generally requires additional hardware, making the sensor more complex and expensive. Furthermore, coverage levels of 95% may not be practically attainable. Hooker et al.[3] suggests that 74% coverage can be achieved for rate gyros and that 97% should be possible of accelerometers. Thus, the development of accelerometers with self-test features seems worthwhile, but the cost effectiveness of self-test for gyros may be questionable.

The last type of sensor that is of interest is the pilot command input transducer. A reliability and cost comparison of the various candidate devices indicates that the linear variable differential transformer (LVDT) and rotary variable differential transformer (RVDT) are the best choices for this function. These devices are functionally similar. They output an a.c. voltage proportional to a position input. This output is the difference of the voltage in two coils. The sum of the voltages from these coils may be used as a self-test signal. It is a constant and can be monitored continuously. By spring-loading the movable element, even mechanical failures may be detected. It appears that virtually 100% self-test coverage can be achieved for these devices.

Secondary Actuator Tradeoff Evaluation

A tradeoff evaluation of four FBW secondary actuator concepts was conducted. The concepts considered were as shown in Fig. 6. All are electrohydraulic, two-failure tolerant approaches. A single-failure tolerant version can be achieved by deleting one channel in any approach.

These concepts were judged using the following criteria: 1) threshold performance, 2) failure behavior including tran-

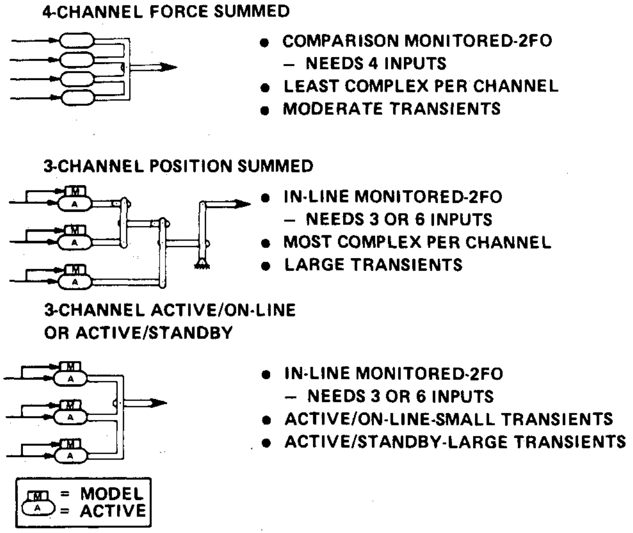


Fig. 6 Secondary actuator configurations.

sients, and 3) overall system complexity. A discussion of each concept follows:

Four-Channel Force Summed

This actuator employs four hydraulic cylinders (channels). Each channel employs a pressure feedback loop which provides a means of failure detection. A channel sustaining an active failure will increase its level of output force, thereby driving the pressure feedback signal beyond a preset failure threshold level. If the threshold is exceeded for a predetermined time-delay period, the affected channel is declared failed and shuts down.

The failure detection approach utilizes the principle that if the force output of one channel is considerably larger than the others, the channel must be failed. Therefore, it is based on comparison monitoring. The mechanization of this technique in the force summed actuator requires time delay settings of the order of 0.5 sec. Test data has shown that this relatively long delay is necessary to minimize false failure indications (nuisance trips). The effect of the long delay is to increase the magnitude of the failure transients.

The failure detection/isolation electronics for this concept are relatively simple; however, four independent hydraulic supplies are required to ensure two-failure tolerance. Threshold performance is marginally acceptable, being the worst of the four concepts evaluated.

Three-Channel Active On-Line

This actuator employs three channels: one in an active mode and the remaining two engaged, but operating in an online mode. The on-line channels employ a high-gain force feedback loop enabling them to track the active channel's position. If the active channel were to fail, it would shut down, and simultaneously the next on-line channel's feedback would switch, making it the active controlling channel. The authority of pressure feedback is limited so that, in the event of a failed active channel, the on-line channels can statically load share and thus oppose the failure transient.

Each channel employs an active and model servo loop path as part of its failure detection network. The active and model outputs are compared. If the comparator signals were to exceed a predetermined threshold for an established time-delay period, the channel is shut down. This in-line monitoring technique provides a sensitive, accurate failure indication, and therefore time-delay settings may be of the order of 50 msec. Laboratory test data have verified these settings. For the active/on-line actuator this results in small failure transients. In fact, for hardover failure conditions, the expected normal acceleration transient will be approximately 0.25 g, well within the previously stated limit of 0.5 g.

The active/model failure detection technique results in fairly complex actuator electronics and a requirement for six command inputs. The six inputs can be obtained from three or four channels of FBW electronics via a suitable interface. Threshold performance is the best of four concepts. This actuator concept is the only one that can tolerate most dual failure combinations. For instance, simultaneous failure of two channels presents no problem. Also, failure of both the active and model inputs to one channel can be tolerated, except that in this case performance will be degraded because a continuous force fight condition will exist.

Three-Channel Active Standby

This actuator employs three channels: one in an active mode, and the other two engaged, but operating in a standby mode. The two standby channels are operational for tracking purposes; however, the cylinders are bypassed, thereby adding no load to the system. Each channel employs an active and model servo loop path with failure detection and correction logic similar to the active on-line concept. If the active channel were to fail, it would shut down and the piston would bypass. Simultaneously the next standby channel would become the active controlling channel.

Failure transients with this type of actuator tend to be large because, unlike both of the concepts discussed previously, no force fight capability is possible. The level of complexity is similar to the active/on-line actuator, and threshold performance is almost as good.

Three-Channel Position – Summed

This actuator employs three active channels. In a full-up condition, each channel supplies one-third of full output stroke. A centering spring is employed in each actuator to neutralize position and hold a failed channel, providing a hard point about which the remaining channel linkage can rotate. A channel failure will result in the failed channel shutting down: the piston being bypassed, and the output ram being positioned to neutral by the centering spring. Simultaneously, the gain and the threshold values of the two remaining channels must be increased 1.5 times their original value to maintain full authority. A second failure requires an increase in gain and threshold value of the remaining channel 3 times the original value.

Each channel employs an active and model servo loop path with failure detection and correction logic similar to the active/on-line and active/standby concepts. As with the active/standby, no force fight capability exists; therefore failure transients are large. Due to the output linkage requirements and gain switching, this concept is the most complex to implement. Threshold performance is slightly degraded relative to the active/standby concept, being approximately the same as the force summed actuator.

The active/on-line actuator was rated far superior to the other three concepts evaluated because of its tolerance to dual failures. It also demonstrated the smallest failure transient profiles and lowest threshold values. The other concepts demonstrated several critical faults, which in most cases could be improved with additional failure logic or compensation circuitry. The force summed actuator should benefit most from additional improvements placing it in contention with the active/on-line concept.

In line with these conclusions, the active/standby and position summed concepts were dropped from further consideration. The active/on-line and force summed concepts were carried on to the next phase of the study, namely, the system configuration analysis. Failure rate data were estimated for each of these command actuator concepts. Per channel failure rates are as follows: active/on-line, 150 failures/10^6 hr; force summed, 100 failures/10^6 hr. Failure rates for the complete command actuator are, of course, much smaller, since with the force summed actuator two of four channels are required for safe flight, and with the active/on-line actuator one of three channels are required.

IV. System Configuration Analysis

The purpose of this phase of the study was to examine in detail the impact of different FBW system configurations on system reliability and cost. Some 26 candidate configurations were formulated and evaluated for failure tolerance and reliability. The most interesting of these were then evaluated from a cost, weight, and power required standpoint. It was felt that the key cost parameter is life-cycle cost; however, only initial cost estimates could be made. Therefore, each configuration was also given a complexity rating that is a primary indicator of relative life-cycle cost. The assumption was that the more complex configurations will require more maintenance actions, need greater spares inventory, and/or be harder to troubleshoot.

Candidate Configurations

Formulation of the candidate configurations was based on the previously established failure tolerance goals. In general, two-fail operational capability was required for the FBW electronics including the secondary actuators; thus, three-channel in-line monitored (self-tested) or four-channel comparison monitored systems provided the bases for configuration development. The significant variables were the level and type of redundancy applied in each of the sensor, computer, and command actuator areas.

A dedicated interface was used between the digital computers and command actuator channels for most configurations. If a cross-strapped interface (all computers cross-connected to each actuator channel) is used, analog voting and failure detection would be required in the actuator electronics. This would add additional hardware and complexity to the system; if two-failure tolerance has been provided, it does not significantly improve the system reliability. Also, for most configurations, the assumption was made that the computers were cross-strapped with digital data links. Sensor input data and actuator commands would be exchanged among computers for voting and failure detection. Digital computers are inherently suited to this function, and the same software algorithm may be used for processing different sets of redundant data. Therefore, little or no increase in complexity is introduced. This digital cross-strapping is similar in nature to the analog cross-strapping of both sensor data and actuator commands and thus can significantly increase system reliability.

Table 2 FBW system component reliability

Unit	Failure rate x 10^{-6}/hr
Gyro	80
Accelerometer	35
RVDT	10
LVDT	10
Digital computer	330
Computer interface	
Analog input section (dedicated sensors)	100
Analog input section (cross-strapped sensors)	150
Analog input section (hybrid)	125
Analog output section (active/on-line act.)	150
Analog output section (force summed act.)	100
Command (secondary) actuators (per channel)	
Active/on-line	150
Force summed	100
Analog dissimilar backup (2 channel)	1000
Fluidic dissimilar backup (1 channel with self-test)	40
Air data system (dual with self-test)	50
Power actuator (duplex)	0.5
Hydraulic system (per channel)	300
Electric power system	0.0002

Sensor analog data cross-strapping does not introduce the requirement for additional analog hardware, since voting, etc., can still be performed in the computer. It does, however, require a multiplicity of wires and cross-connections, which seems undesirable from a maintenance standpoint. The reliability improvement due to sensor cross-strapping is small if two-failure tolerant sensor systems have been provided (especially when digital cross-strapping is used). In the case of skewed sensors, analog cross-strapping is required to achieve the two-failure tolerance inherent in the six skewed sensor set.

Reliability Analysis

The reliability analysis was conducted in considerable detail, including the effects of failure detection coverage and cross-strapping. A coverage value of 100% was used for comparison monitoring and 95% was used for self-test, with the exception of the command actuator in-line monitor which was assumed to provide 100% coverage. Both mission and safety reliability were calculated for each configuration. The following functions were required for safety: 1) FBW group (sensors, computers, I/O's, and command actuators), 2) one

Table 3 FBW system component cost/weight/power

Unit	Cost, $K	Weight, lb	Power, W	Comments
Digital computer	25	15	100	Data representative of Kearfott, IBM and Teledyne machines
Interface unit (IFU)	25	20	180	Includes A/D, D/A, power supplies & actuator electronics
Rate gyro	1.5	1	5	Includes packaging
Accelerometer	1.0	0.5	1	Includes packaging
LVDT	0.2	0.2	1	Rudder pedal transducers
RVDT	0.2	0.2	1	Side stick transducers
Command actuators:				
o 4-channel force summed	13	31	-	Flight critical actuators (2F0) - 3 req'd
o 3-channel force summed	10	24	-	Mission critical actuators (1F0)
o 3-channel active/on-line	10	24	-	Flight critical actuators (2F0) - 3 req'd
o 2-channel active/on-line	7	16	-	Mission critical actuators (1F0)
Hydraulic system				
o Electro-hydraulic module	5	50	8000	An additional one of these is required for 4-channel force-summed actuator
o Transfer valve	2.5	10	-	
Dissimilar backup				Approximate cost estimate includes R&D but not actuators
o 2-channel analog	25	16	160	Without sensors cost is $20K
o 1-channel fluidic	20	20	-	Requires on-line self-test

rudder and two stabilizer power actuators, 3) hydraulic supply, and 4) electrical power.

The following functions were required for mission completion: 1) FBW group, 2) rudder and stabilizer power actuators (4), 3) mission critical controls (ailerons and maneuver flaps in this analysis), 4) air data, 5) hydraulic supply, and 6) electrical power.

In addition, the mission would be aborted if an additional failure would result in loss of the aircraft.

The reliability analysis of the FBW group could not be accomplished by using simple series and parallel strings. This was because many configurations used cross-strapped computers; thus data and/or actuator channels accessible only to a failed computer are no longer available to the system. (It was assumed here that each I/O section was dedicated to, and controlled by, a specific computer.)

The method employed for the analysis required enumerating all acceptable combinations of operating equipments. Since many components are dedicated to specific computers, the computers are the logical place to start the enumeration process. Considering, for example, a configuration with three computers, the general form of the reliability equation is:

$$\begin{aligned} R = P\ & (\text{safe combination of remaining equipment exists} \mid 3 \\ & \text{computers operating}) \\ & \times P\,(3 \text{ computers operating}) \\ + P\ & (\text{safe combination of remaining equipment exists} \mid 2 \\ & \text{computers operating}) \\ & \times P\,(2 \text{ computers operating}) \\ + P\ & (\text{safe combination of remaining equipment exists} \mid 1 \\ & \text{computer operating}) \\ & \times P\,(1 \text{ computer operating}) \end{aligned}$$

where P denotes probability, R denotes reliability, and | denotes "given that."

Failure rate $(=1-R)$ was generally used in the actual computations. Failure rates for each equipment item were estimated from past Grumman experience and various reference material including Refs. 3 and 4. Table 2 tabulates the failure rate data for each component of the FBW system necessary for the analysis. Note that the computer I/O was treated in two separate sections, the assumption being that the analog input section was partially independent from the analog output section.

Cost/Weight/Power

Table 3 provides the estimated component cost, weight, and power data that were used for the FBW group equipment. These data are based on Grumman and vendor estimates. The computer is assumed to have 16,000 16-bit words of semiconductor memory and an equivalent throughput rate of about 300,000 operations per second.

Results and Anomalies

Figure 7 summarizes the results for five typical configurations. The complexity rating given in the figure is based on a scale of 0 to 10, with 10 being the most complex and 1 corresponding to a single channel.

The three configurations with essentially the same safety reliability failure rate (1.5×10^{-6}) demonstrate an interesting anomaly, namely, that the total system reliability is insensitive to the reliability of the FBW group for a good design. The failure rate of 1.5×10^{-6} is entirely the result of the three dual-tandem power actuators necessary for safe flight. The failure rate for the rest of the system is smaller by a factor of 10 or more.

The third configuration does not meet the mission reliability goal but is interesting in that it shows that a three channel purely comparison monitored system can meet the flight safety goal. The fourth configuration fails to meet the safety reliability goal because the dual digital computers must use self-test with 95% coverage to detect and isolate the first failure. One out of 20 times that the first computer fails, the aircraft is lost. This points out that if a dissimilar backup channel is desired it should be used with at least three primary digital computers.

The configuration selected as a result of this study (shown at the bottom of Fig. 7) meets the reliability goals and is close

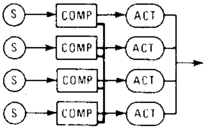
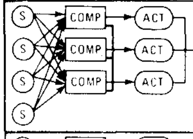
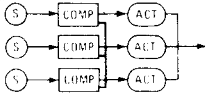
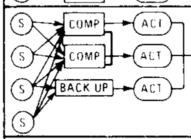
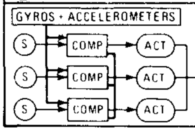
CONFIGURATION (FBW GROUP)	RELIABILITY GOALS: SAFETY – $3.5/10^6$ HR MISSION – $350/10^6$ HR	SYSTEM FAILURE RATE PER 10^6 HR		FAILURE TOLERANCE	COMPLEXITY RATING	COST, $K	WEIGHT, LB	POWER, W
		SAFETY	MISSION					
	4-CHANNEL • QUAD VEHICLE MOTION SENSORS • QUAD PILOT INPUT SENSORS • QUAD COMPUTERS • FORCE SUMMED CMD ACTUATOR	1.5	66	2	8	302	373	1200
	3-CHANNEL (I) • QUAD VEHICLE MOTION SENSORS • QUAD PILOT INPUT SENSORS • TRIPLEX COMPUTERS – SELF TEST • ACTIVE/ON-LINE CMD ACTUATOR	1.5	58	2	7	229	243	920
	3-CHANNEL (II) • TRIPLEX SENSORS • TRIPLEX COMPUTERS • ACTIVE/ON-LINE CMD ACTUATOR	2.3	2360	1	5	222	239	903
	2-CHANNEL (WITH BACK-UP) • QUAD SENSORS • DUPLEX COMPUTERS – SELF TEST • ANALOG BACKUP • ACTIVE/ON-LINE CMD ACTUATOR	35	98	2	7	204	224	800
	SELECTED 3-CHANNEL • SKEWED GYROS, TRIPLEX ACCEL • TRIPLEX PILOT SENSORS – SELF TEST • TRIPLEX COMPUTERS – SELF TEST • ACTIVE/ON-LINE CMD ACTUATOR	1.5	269	2 –	6	218	236	888

Fig. 7 FBW configuration tradeoff summary.

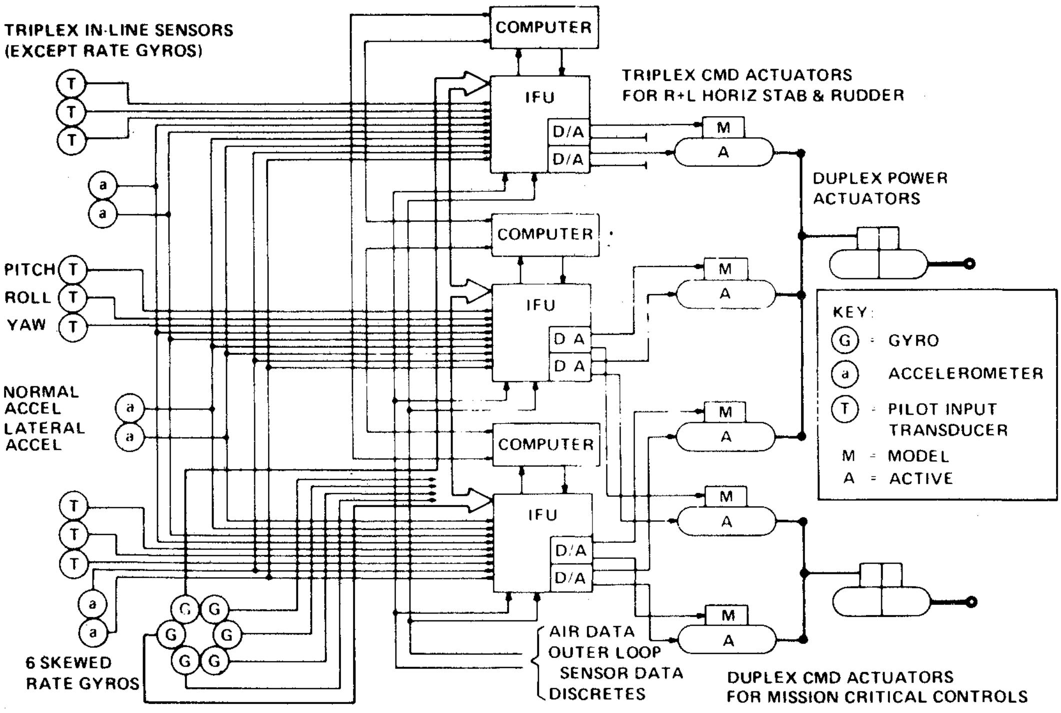


Fig. 8 Selected configuration.

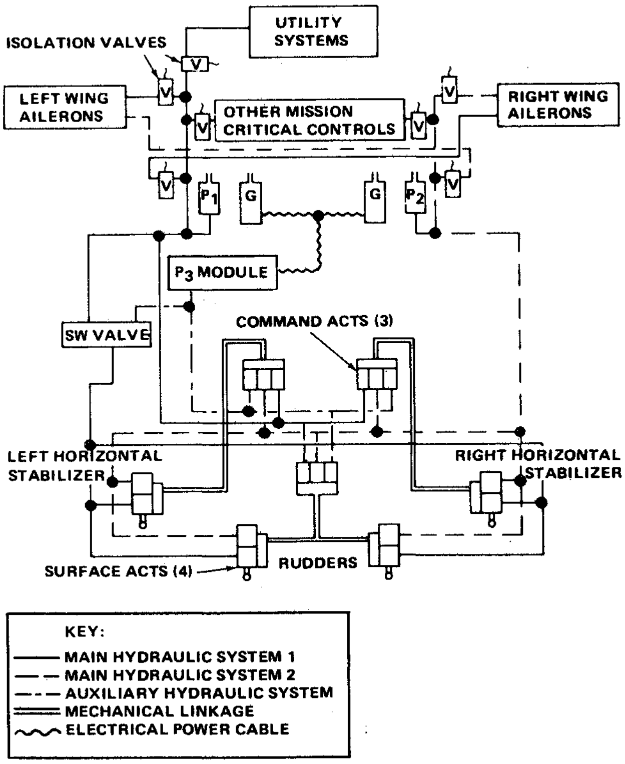


Fig. 9 Hydraulic system configuration.

to the best in all categories of complexity, cost, weight, and power. The configuration is two-fail operational for all components, except accelerometers; use of skewed accelerometers or accelerometer self-test would eliminate that drawback.

V. Selected Configuration Description

The selected configuration is shown in detail in Fig. 8. Note that triplex (2FO) active/on-line command actuators are used for safety critical controls; duplex (1 FO) active/on-line actuators are provided for mission critical controls.

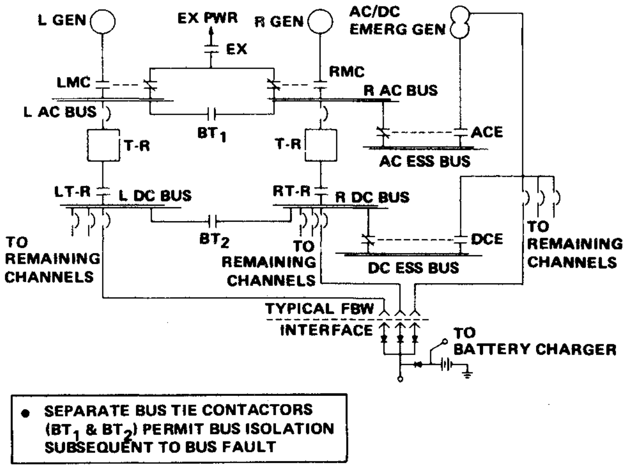


Fig. 10 Electric power configuration.

The interface unit (IFU) is a multifunction centralized analog I/O box. One is dedicated to each computer. It contains an analog input section – A/D conversion, multiplexing, etc.; and an analog output section – D/A conversion and actuator electronics. Separate D/A converters are provided for the active and model actuator channels. The actuator electronics include servo amplifiers, the electronic models, and failure monitoring electronics. Self-test functions for the I/O's must also be implemented in the IFU, since at the system level they must be two-failure tolerant. The self-test functions would be controlled by the computer as part of its self-test routine. Self-test is also provided for the dedicated pilot input transducers. 95% coverage has been postulated for all of these self-test functions.

Since the skewed gyros are two-failure tolerant, all flight critical components are 2FO except the accelerometers. A skewed accelerometer configuration would remedy this limitation with some increased software complexity. Skewed gyro technology is well in hand.[5] However, less development work has been done for skewed accelerometers. The skewed approach can provide 2FO with one less accelerometer, or for the same number of sensors it would provide full three-axis acceleration information. If accelerometer self-test with at least 95% coverage can be implemented, it would negate the requirement for cross-strapped accelerometers. This simiplified interface may offset the additional complexity introduced by the self-test features.

The hydraulic system configuration which resulted from the design tradeoff discussed earlier appears in Fig. 9. It has been adapted to the actuation system chosen for the selected FBW system. Similarly, the selected electrical power system configuration is shown in Fig. 10. The diode isolated interface and batteries would be contained in the IFU. Separate electrical interfaces are required for each gyro and accelerometer since they are cross-strapped and must not be dependent on a single IFU for power.

VI. Conclusions

A three-channel FBW system configuration was chosen as the optimum system configuration for a modern fighter/attack aircraft. The system features a three-channel, in-line monitored active/on-line command actuator. Skewed rate gyros are used, as are triplex digital computers, accelerometers, and pilot input transducers (LVDT's and RVDT's). Self-test features are included in the computers and in the pilot input transducers. This configuration, including the power actuators and hydraulic and electrical power supplies, meets the reliability goals set at the beginning of the study.

The selected configuration is the least complex of all the configurations that meet the reliability goals. It is two-fail operational for all components except the accelerometers. If this drawback is unacceptable, skewed accelerometer techniques or accelerometer self-test should be examined more thoroughly.

A series of design trade studies examined specific areas in question. The conclusions from these design tradeoffs are given in the following paragraphs.

Hydraulic and electric power supply configuration trades – Dual main (engine-driven) supplies were chosen for each system with auxiliary sources as required for redundancy. Separate hydraulic supplies are provided for each channel of the command actuators. An electrically driven auxiliary pump would be used for the third channel of the command actuator. One hydraulically powered auxiliary d.c. generator would be used in the d.c. electrical system.

In-line monitoring (self-test) versus comparison monitoring for failure detection – In-line monitoring is desirable if at least 95% of all failures can be detected and if it enables achievement of reliability or fault tolerance goals that would otherwise require increased redundancy. This conclusion is conditioned on the assumption that the self-test features do not significantly increase the system cost or complexity.

Command actuator concept tradeoff evaluation – This study examined four command actuator concepts: 1) active/on-line, 2) active-standby, 3) force summed, and 4) position summed. The three-channel active/on-line actuator was found to be superior. The four-channel force summed approach placed second.

References

[1] Helfinstine, R., Montague, L. and Seller, G., "Reliability and Redundancy Study for Electronic Flight Control Systems," Honeywell, Inc., Minneapolis, Minn., July 1972.

[2] Allen, J., "Digital Computer Design Guidelines for a Full Authority Fly-By-Wire Flight Control System," AIAA Digital Avionics System Conference, Boston, Mass., April 1975.

[3] Hooker, D., Pope, I., Smith, G. and Vetsch, G., "Definition Study for an Advanced Fighter Digital Flight Control System," AFFDL-TR-75-59, McDonnell-Douglas Corp., St. Louis, Mo., June 1975.

[4] Frazzini, R. and Vaughn, D., "Analysis and Preliminary Design of an Advanced Technology Transport Flight Control System," NASA CR-2490, Honeywell, Inc., Minneapolis, Minn., March 1975.

[5] Abrams, C. and Weinstein, W., "A New Concept for Angular Rate Flight Control Sensors," AIAA Mechanics and Control of Flight Conference, Anaheim, Calif., August 1974.