

# HiMAT Onboard Flight Computer System Architecture and Qualification

Albert F. Myers\* and Michael R. Earls†  
*NASA Ames Research Center, Edwards, California*  
 and  
 Larry A. Callizo‡  
*Rockwell International, Los Angeles, California*

Two highly maneuverable aircraft technology (HiMAT) remotely piloted research vehicles (RPRVs) are being flight tested at NASA Dryden Flight Research Facility, Edwards, Calif., to demonstrate and evaluate a number of technological advances applicable to future fighter aircraft. Closed-loop primary flight control is performed from a ground-based cockpit utilizing a digital computer and up/down telemetry links. A backup flight control system for emergency operation resides in one of two onboard computers. Other functions of the onboard computer systems are uplink processing, downlink processing, engine control, failure detection, and redundancy management. This paper describes the architecture, functions, and flight qualification of the HiMAT onboard flight computer systems.

## Introduction

UNDER the management of the National Aeronautics and Space Administration and the U.S. Air Force, two highly maneuverable aircraft technology (HiMAT) remotely piloted research vehicles (RPRV) were built under contract and delivered to the NASA Dryden Flight Research Facility. The HiMAT vehicles are 0.44 scale versions of an envisioned full-scale fighter designed to have a sustained 8 g turn capability at Mach 0.9 at an altitude of 7620 m (25,000 ft). These vehicles were designed to incorporate technological advances in aerodynamics, advanced composite and metallic structures, and digital fly-by-wire active controls. The 1530 kg (3370 lb) HiMAT vehicle is powered by a J85-21 afterburning turbojet engine, which is controlled by a digitally implemented integrated propulsion control system (IPCS). These vehicles are currently undergoing research flight test at NASA Dryden.

## Flight System Description

Closed-loop primary flight control is performed from a ground-based cockpit utilizing a digital computer and up/down telemetry links. A backup control system (BCS) for emergency flight operation resides in one of two onboard computers. Other functions of the onboard computer system are uplink processing, downlink processing, engine control, failure detection, and redundancy management. The requirement for single-fault toleration and the flight objectives outlined below are the basis for the computer system architecture and qualification procedures described in this paper.

The operational concept for the HiMAT vehicles is similar to other RPRVs flown at Dryden. The vehicle is air launched from a B-52 aircraft at 13,700 m (45,000 ft) at Mach 0.68. The aircraft, which carries 286 kg (660 lb) of fuel, can conduct 20-45 min of flight test before horizontal landing recovery is made on the Edwards dry lakebed. The vehicle is flown under

the control of a NASA research test pilot located in a ground-based RPRV facility cockpit. Flight control laws for both the primary and a backup mode of operation are implemented by the use of two ground-based and airborne digital computers. The three-view drawing of the HiMAT vehicle (Fig. 1) shows the five pairs of hydraulically actuated control surfaces. All five pairs of surfaces are active during the primary mode of operation. The BCS controls only the rudders and elevons while the other three surface pairs are commanded to a hydraulically locked safe position.

A primary system design criterion for HiMAT was that no single failure would result in the loss of the aircraft. Redundant systems which provide independent primary and backup flight control systems are utilized to obtain a fail-operational (degraded) capability.

The HiMAT RPRV system utilizes a ground station, uplink telemetry, and downlink telemetry to control the vehicle. Major elements of the system are shown in Fig. 2. The ground-based control law computer interfaces with the downlink processor, the ground cockpit, and the uplink system. During normal operation, the primary control system (PCS) mode is active, utilizing the ground-based cockpit, control law computer, uplink system, airborne system (computers, engine, actuators, and sensors), and downlink system. The PCS provides for proportional control of the vehicle surfaces and the throttle. In most system failures, the BCS is utilized and the onboard computer executes the vehicle

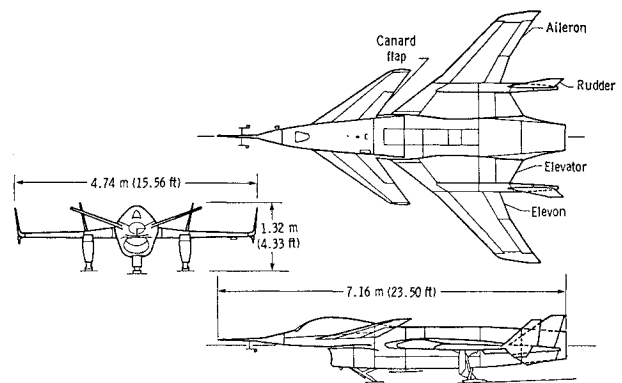


Fig. 1 HiMAT RPRV.

Presented as Paper 81-2107 at the AIAA Computers in Aerospace III Conference, San Diego, Calif., Oct. 26-28, 1981; submitted Oct. 1981; revision received Dec. 7, 1982. This paper is declared a work of the U.S. Government and therefore is in the public domain.

\*Chief, Control Branch, Dryden Flight Research Facility (currently with Northrop Aircraft Group). Member AIAA.

†Aerospace Technologist, Controls Section, Dryden Flight Research Facility.

‡Software Design Engineer.

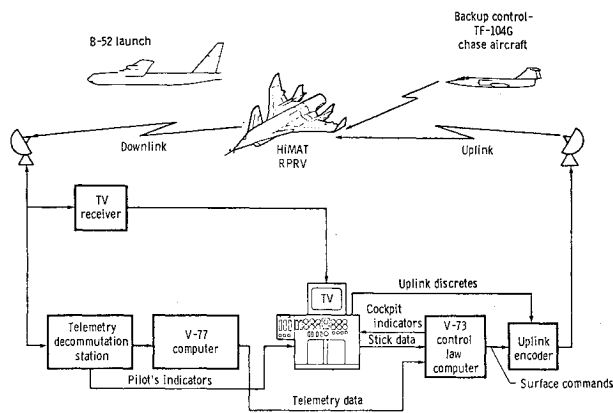


Fig. 2 HiMAT RPRV control system.

BCS control laws. During backup operation, the ground control law computer is bypassed. Pilot inputs, originating either from the ground cockpit or the TF-104G chase aircraft, supply backup control by way of uplink discrete commands, thus providing the capability for control of the HiMAT vehicle in the event of ground/vehicle communication loss. In case of total loss of uplink, the BCS automatically commands the aircraft to orbit at a preselected altitude until communication with the ground or chase aircraft is regained. A third mode of operation, degraded primary mode (DPM), can be utilized in certain failure modes. Ground-based systems are used as in the normal PCS in conjunction with the backup systems onboard.

The no-single-failure criterion is the basis for the extensive failure detection logic onboard the vehicle both in software and in the avionics and power system hardware. The most critical of the flight control sensors (rate gyroscopes and accelerometers) are triplicated, while other systems (power, hydraulics, uplink, air data, and computer) are dualized. Electrical power is provided by an engine-driven generator or an emergency battery. One hydraulic pump is engine driven; the other is electrically driven from the battery bus. The PCS requires both uplink systems as well as the primary side of

most of the dualized systems. Because of the system's mechanization, the duplex actuators (rudders and elevons) can be switched to the backup side while the vehicle remains under the control of the PCS. The BCS requires only one uplink system for proper operation since the uplink BCS command discretes are redundant; however, the remaining backup components of the dualized systems must be operational, as well as the No. 3 sensors of the triplex set, which are designated as backup and powered by the backup battery bus. If any of these necessary backup systems fail, logic residing in the primary computer inhibits any automatic transfer to the backup mode, even in the presence of a primary system failure. Uplink-commanded transfers to the backup mode are always accepted, regardless of the health of the backup system. DPM requires good uplink and downlink systems, as well as good backup elements of the triplicated and dualized sensors along with active backup hydraulic and actuator systems. A more complete description of the HiMAT flight control systems can be found in Ref. 1.

### Onboard Computer System

All critical onboard flight systems are controlled by two computers. Although the computers are designated primary and backup, they execute different software and both are normally active unless one has failed. The principal tasks performed by each of the computers are summarized in Table 1.

#### Airborne Computer/Aircraft Systems Interface

The airborne computer interfaces with the aircraft systems (Fig. 3) consist of three types: digital, discrete, and analog. Most computer-supplied information to be downlinked is transferred to the flight test instrumentation system (FTIS) digitally. Computer/FTIS synchronization is provided by three FTIS-generated pulses to the primary computer. Uplink commands to the vehicle, both proportional and discrete, are transferred digitally to both computers from the two uplink decoders. Discrete signals from the decoders are used as interrupts to synchronize reading of the 128 bits of uplink data and to indicate validity of those data. The third digital interface to the primary computer is with the system test

Table 1 Airborne computer functions

Function	Primary	Mode		
		Primary (backup com- puter failed)	Backup	Test
Primary computer				
Uplink processing	X	X		
Downlink processing	X	X	X	
Aircraft control via PCS	X	X		
Failure detection	X	X	X	
Computers				
Sensors				
Actuators				
Uplink				
Downlink				
Electrical system				
Intercom control	X		X	
Backup IPCS		X		X
Test mode control and I/O				X
Backup computer				
Uplink processing	X		X	
Aircraft control via BCS			X	
Failure detection	X		X	
IPCS sensors				
Radar altimeter				
Intercom response	X		X	X
Primary IPCS	X		X	
Test mode I/O				X

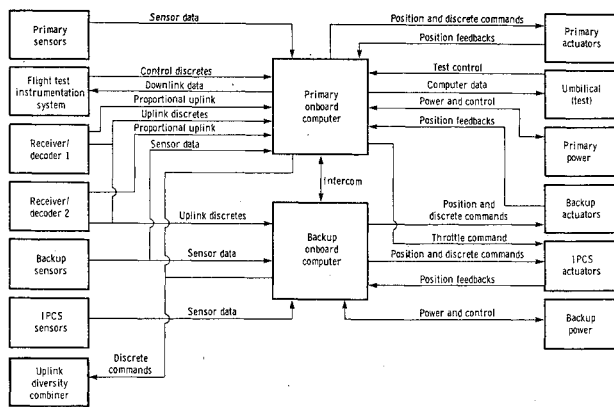


Fig. 3 Airborne computer/aircraft systems interface diagram.

console (STC) via the aircraft umbilical. Computer memory interrogation, interface test initiation and monitoring, and engine control and monitoring are among the functions of the STC interface. Information transfer between the primary and backup computers is via a digital intercom.

Discrete outputs are used to command many aircraft systems, such as fuel dump, landing gear, hydraulic system selection, electrical power distribution, engine on/off, and others. They are also used in watchdog timers, in which a missing pulse indicates to one computer that the other computer is no longer operating. Discrete inputs monitor the fire-detection system, hydraulic pressure and reservoir switches, engine oil pressure switches, whether the aircraft is captive on the B-52 launch vehicle or in-flight, and other discrete states.

Analog outputs command control surface actuators and engine actuators (throttle and nozzle). In addition, some parameters are passed to the FTIS via analog outputs for downlink. Analog inputs include flight control sensor data, surface positions, throttle and nozzle positions, engine temperatures and pressures, environmental control temperatures, and voltage monitors from the other computer and from aircraft power systems.

#### Airborne Computer Hardware

The airborne computer consists of two microcomputers packaged in a common chassis with separate circuit card sets and connectors. They are identical in computational and memory capacity; only the input/output interfaces differ. Each computer consists of an 8080A microprocessor, a 24 MHz clock, a maximum of 22K bytes of program memory, 1K bytes of random access memory, integer multiply hardware, and priority interrupt structure. Program memory is in 2708-type erasable programmable read only memories (EPROMs). All input/output (I/O) interfaces are memory mapped in the computers. The dual computer chassis weighs 18.1 kg (40 lb) and has a volume of 19,632 cm<sup>3</sup> (1198 in.<sup>3</sup>). Analog inputs use multiplexed analog-to-digital converters and a multiplexed synchro-to-digital converter. Analog outputs are by way of individual digital-to-analog converters. Digital input/output is transistor-transistor-logic (TTL), while discrete input/output is mixed TTL and 28 V logic. Most discrete outputs are 28 V relay drivers.

All mainframe and circuit card wiring is point-to-point. Electronic components, other than discrete resistors and capacitors, are mounted in sockets on the circuit cards. Each computer contains 15 circuit cards.

Computer power supplies are packaged separate from the computers. The primary and backup power supplies share a common housing, but have separate connectors and are electrically isolated. The power supply heat-sink temperature is monitored as part of the environmental control system.

#### Software Architecture and System Functions

Both computers are programmed entirely in Intel 8080 assembly language. The primary computer contains 21K bytes of code (including 8K bytes for ground test software) while the backup computer contains 16K bytes of code. The on-board software is organized as an interrupt-driven system, requiring both speed- and memory-efficient code. High-order programming languages, with all of their inherent benefits, could not achieve the required efficiency using the 8080A microprocessor.

Each computer contains an eight-level priority interrupt control unit (PICU). The PICU provides for vectored interrupts and for the capability of interrupts interrupting other interrupts on a prioritized basis. When an interrupt occurs, all interrupts of less or equal priority are disabled by the appropriate software interrupt handler. Interrupt signals are latched in the hardware, in case the computer interrupt system is disabled at the time of the interrupt, and must be reset by the appropriate software interrupt handler routine. With this mechanization, a low-priority task cannot interrupt a task of higher or equal priority.

The interrupts incorporated into the primary computer, ordered from highest priority to lowest priority, are: 1) power on, 2) watchdog timer, 3) downlink strobe, 4) downlink frame rate, 5) synchro-to-digital conversion complete, 6) intercom, 7) uplink, and 8) real time clock. The list for the backup computer is similar except that the downlink and synchro-to-digital conversion complete interrupts are omitted. This ordering gives highest priority to asynchronous tasks since they relate to external events which demand immediate attention. Lowest priority is given to those tasks which are not time dependent or, if time dependent, need only run at low frequencies.

#### Power-On Interrupt Processing

The power-on interrupt starts the computers in a known state whenever power is applied or the computers are reset. The initialization routine sets all discrete and analog outputs to known states, initializes random access memory (RAM), computes an initial memory checksum for each EPROM chip, and clears all interrupts. When initialization has been completed, interrupts are enabled and the background mode is entered. In the background mode, the EPROM checksums are continuously recomputed and compared to the initial checksums which are calculated during initialization. In the event of a miscompare the computer is declared failed and switched off line and information is stored in RAM to identify the failed EPROM. Background is the lowest priority task and runs only if no interrupts are pending. Depending upon computational demands on the computers, each computer spends about 20-40% of real time in the background mode (CPU utilization of 60-80%).

#### Watchdog Timer Interrupt Processing

The watchdog timer interrupt occurs only when the alternate computer fails. During normal operation, the software in each computer drives a heartbeat-type discrete output which goes through a missing pulse detector. Absence of this pulse causes the failed computer's outputs to be deactivated and initiates a watchdog timer interrupt into the opposite computer.

A watchdog timer interrupt into the primary computer initiates execution of the backup IPCS program residing in the primary computer. Intercomputer relay logic causes the engine to be driven by the primary computer instead of the backup computer.

A watchdog timer interrupt into the backup computer initiates execution of the backup flight control system code. In this case, relay logic is used to lock the simplex actuators, canards, ailerons, and elevators and to switch control of the duplex elevon and rudder actuators to the backup computer. A watchdog timer interrupt into either computer causes future

intercom and watchdog timer interrupts into that computer to be disabled. A failed computer, if still running, can do no harm because all of its outputs are deactivated and are ignored by the alternate computer.

#### Downlink Interrupt Processing

There are two interrupts and an input discrete generated by the FTIS and used by the downlink routines: frame rate interrupt, strobe interrupt, and subframe rate discrete. Coincidence of a frame rate interrupt and subframe rate discrete indicates the beginning of a major data frame, and is used to achieve initial synchronization with the FTIS. Synchronization is required because all downlink data is stored into the same 10-bit buffer register, from which the FTIS inputs the data at each strobe interrupt. Loss of synchronization is detected using the known sequence of 4 frame rate interrupts per major frame and 10 strobe interrupts between frame rate interrupts. All interrupts except the tenth strobe of each minor frame result in storing data into the FTIS buffer for transfer at the next strobe interrupt. At the tenth strobe, current midvalue data from the triplicated flight control sensors are input. Major frames occur at a 55 Hz rate; however, the midvalue flight control data (rates and accelerations) are output in each minor frame, at 220 Hz. Other sensor data and eight packed digital status words are output at the 55 Hz rate. The midvalue sensor of each flight control trio is selected in the downlink routine at a 55 Hz rate. Because of the relatively large amount of processing required within a narrow time frame, the downlink interrupts are assigned a high interrupt priority.

#### Synchro-to-Digital Conversion Complete Interrupt Processing

The synchro-to-digital conversion complete interrupt is used to sample the three-axis attitude gyro. Each axis (pitch, roll, and heading) is sampled 25 times/s. The gyro data are downlinked to the ground as a part of the 55 Hz data and are intercommuted to the backup computer at a 25 Hz rate. The backup computer uses the vertical gyro data in primary mode to initialize a direction cosine algorithm which synthesizes vehicle attitude for the backup flight control system.

#### Intercom Interrupt Processing

The intercom is a bidirectional digital communications link between the primary and backup computers. The primary

computer controls the intercom. Up to seven 8-bit bytes of data may be transferred each way per intercom message. One byte of the seven is used for the intercom message identity; the other six bytes are used for data. Typically, the primary computer sends seven bytes of information to the backup computer; this generates an intercom interrupt in the backup computer. The backup computer does any necessary processing on the data and sends seven bytes of data, including the echoed message identification, back to the primary computer; this generates an intercom interrupt in the primary computer. The primary computer then processes the data as required depending upon the particular message request. The intercom is used only by the uplink interrupt processor and the tasks running under control of the real-time clock processor. Since it is desirable to have intercom processing taking place in parallel with the routines that use it, the intercom is given a higher priority than these routines.

#### Uplink Interrupt Processing

The uplink interrupt is next in order of priority. The uplink data format is shown in Fig. 4. Four 16-bit words of data are available from each of the two decoders. The first 10 bits of each word are available to only the primary computer and are designated proportional data. The last six bits of each word are designated as manual command discretelys and go to both computers. Nominally, the uplink interrupts alternate between decoder 1 or 2. Each decoder produces an interrupt rate of 53.3 Hz for a total uplink interrupt rate of 106.6 Hz.

The processor reads the decoder status to see if the current data are from decoder 1 or 2. The decoded data are then placed in a buffer in RAM for later processing and fault detection by the uplink monitor logic which is under control of the real-time clock interrupt.

In the primary computer the proportional parity and uplink rate checks are accomplished, and the computer discretelys are filtered against noise spikes (five-frame persistence) and executed. Parity and rate failures cause selection of the backup flight mode. Actuator fault detection is also accomplished as part of this module.

#### Real-Time Clock (RTC) Interrupt Processing

The RTC interrupt occurs at 100 Hz in both computers. The routine increments a 24-bit clock counter used throughout the system for programming delays and time elapsed computations. The multitask executive is then executed.

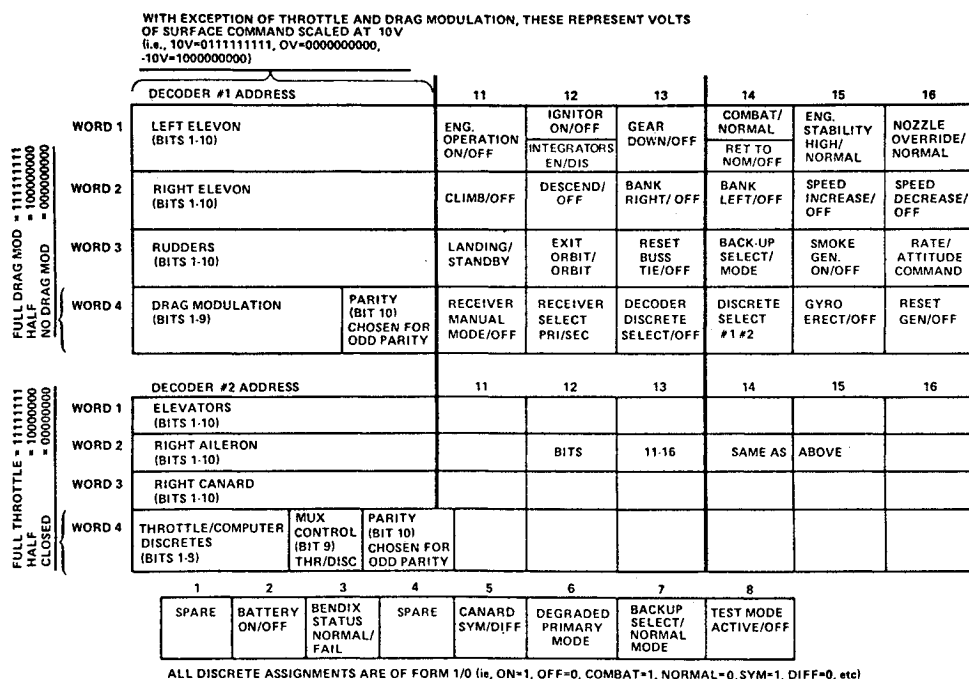


Fig. 4 Uplink format.

The multitask executive is the program which schedules, according to a preassigned priority, the running of all tasks under control of the RTC interrupt. In the primary computer, there are three timed loops under control of the multitask executive: 10 Hz (high priority, from which 1 Hz is derived), 50 Hz (from which 25 Hz is derived), and 10 Hz (low priority). In the backup computer, the multitask executive controls four timed loops: 10 Hz (high priority), 50, 33.3, and 10 Hz (low priority). In addition, the BCS fast loops run at 100 Hz in the backup computer; however, these tasks run serially with the multitask executive.

#### Failure Detection and Redundancy Management

To meet the primary design criterion that no single system failure shall result in the loss of the vehicle, several failure detection functions are incorporated within the onboard computer software. Normally, failures are downlinked for display on the ground master caution warning panel and a switch is made to an alternate or degraded mode of operation which bypasses the failed system.

Most of the uplink failure detection is done as part of the uplink monitor logic. In addition to uplink failure detection, the uplink monitor logic also performs a five-consecutive-frame persistence test on the command discretes. In the primary flight mode, both decoders must be operational so that a complete set of proportional commands can be available for outputting to the flight control surfaces. The uplink monitor logic in the primary computer tests for missing data from either decoder, and if a decoder is found failed, an entry into the BCS mode is commanded. If both decoders are operational, the logic compares the decoder 1 discretes with those from decoder 2 and downlinks any discrepancies to the ground for resolution. In case of a disagreement, the ground may command the onboard computer to use either decoder 1 or 2 discretes. No action is taken on uplink command discretes until the computer has passed the five-consecutive-frame persistence test. In addition, if both decoders are operational and there has not been a ground command to select the use of either decoder singly, a discrete will not be acted upon unless both decoders are in agreement for that discrete.

Fault detection for the simplex actuators (aileron, canard, and elevator) is accomplished by a cross-ship comparison algorithm. A cross-ship comparison is also used to test the rudders duplex actuators. A spool valve technique is used to test the elevons duplex actuator. The elevon testing is done by the servoactuator electronics system external to the computers. This system contains electronic circuits which model the elevon servovalve dynamics and send fault detection signals back to the primary computer. In the event of a simplex actuator failure, the primary computer commands a switch to backup mode; this commands all simplex actuators to the fail-safe locked position. A duplex actuator failure results in a switch to the alternate side of the actuator.

Hydraulic system failure detection consists of monitoring pressure transducers and low fluid level switches in both the primary and backup systems. A primary hydraulic failure results in an automatic transfer to backup flight mode, while a backup hydraulic failure inhibits automatic transfers to the backup mode.

Electrical system failure detection involves monitoring primary system (generator) and backup system (battery) voltages. A primary system failure results in a transfer to backup mode.

Triplex sensor failure detection consists of comparing the two nonmidvalue sensors with the midvalue sensor for each of the five triplicated sensors. Failure indications are downlinked to the ground; however no automatic action is taken since a failed sensor will have been voted out of the system by the midvalue selection process. If sensor 3 of a trio used by the backup flight control system has failed, automatic transfers to the backup mode are inhibited.

Air data sensor fault detection consists of comparing the primary static and impact pressure transducer outputs with those of the corresponding backup transducers. If a disagreement exists the state is downlinked for resolution on the ground. The static and impact pressures are also used to digitally compute predicted static and impact pressure rates. These predicted rates are then compared with the analog differentiated rates to determine if an air data pressure rate failure exists.

The computer intercom is tested by sending a diagnostic test message from the primary computer to the backup computer. The backup computer echos the message back to the primary computer, where it is checked for correctness. Two different messages are used so that all bits can be checked in both the on and off state.

Computer self-test software is utilized in each computer. These include memory (both RAM and EPROM), hardware multiplier, analog-to-digital and digital-to-analog, and instruction diagnostic tests. If a failure is detected, the failing computer will take itself off line by turning on its computer failure discrete output and freezing its watchdog pulse output. A primary computer failure causes a transfer to backup mode, while a backup computer failure inhibits automatic transfers to backup mode.

#### Integrated Propulsion Control System

The HiMAT aircraft utilizes a digitally implemented engine control system which replaces the mechanical control system of the J85-21 afterburning engine. This system, the IPCS, both emulates the conventional J85-21 mechanical controls and provides additional control modes not found on the standard engine. The primary IPCS control software runs in the backup computer as a 33.3 Hz task, while the backup IPCS software runs in the primary computer as a 50 Hz task. The backup IPCS software is functional only if the backup computer fails.

The primary IPCS control laws take the throttle command from uplink in primary flight control mode and from the backup flight control laws in backup mode. The multimode engine control system allows control of the propulsion system in either a normal or combat mode of operation and with either a high or normal compressor stability margin. In combat mode, the rate of thrust response is significantly greater than in normal mode; engine rpm is maintained at 100% for all power settings by modulating jet nozzle throat area in the dry power region and by modulating both the jet nozzle area and afterburner fuel flow in the afterburner region. In the high-stability mode, the engine is operated in essentially a normal manner, but at approximately 100°F lower exhaust gas temperature than in normal stability mode. Logic is also included for engine startup and shutdown, main burner flameout detection and annunciation, and engine sensor failure detection. In the event of an engine sensor failure, the IPCS automatically switches to an alternate path in the control logic and the failure is annunciated on downlink.

The IPCS program residing in the primary computer is much simpler than the backup computer version since it represents a backup mode of operation. The backup IPCS contains engine startup and shutdown logic, and throttle command logic only. The jet nozzle is maintained at a fixed area by intercomputer relay logic, unless overridden by a nozzle override command which commands the nozzle full open, and the throttle is limited to dry power operation.

#### Degraded Primary Mode Logic

The degraded primary mode is a ground selectable mode which utilizes only rudders and elevons for control. It is intended for use primarily in engine-out conditions; however, it may be used in the engine-powered mode (cases where there is a primary hydraulics failure, a simplex actuator failure, or a primary electrical failure). The simplex actuators are locked,

whereas the secondary sides of the duplex actuators are active and commanded via the uplink proportional commands. The backup static and impact pressures are output on FTIS, and the backup rate gyro and accelerometer data are downlinked if generator primary power voltage drops below 24.5 V.

#### **Backup Control System**

The backup control system provides the means for the pilot to fly the vehicle by way of discrete uplink commands. The ground cockpit contains an independent control panel for issuing BCS commands; this control panel is also duplicated in a TF104-G chase aircraft in the event all uplink command capability from the ground is lost.

The BCS is a multirate digital controller with stability augmentation and command functions residing in the backup computer. The stability augmentation loops are executed at the highest rate, 100 Hz, while the command functions are executed at a lower rate, 50 Hz. The BCS is designed to provide well-controlled vehicle dynamics throughout the flight envelope and provide adequate control modes and vehicle stability to land at a selected site. The BCS commands elevons for pitch and roll control and the rudders for yaw control and utilizes an auto throttle for speed modulation. The simplex actuators are commanded to their fail-safe locked positions. In the event of an uplink failure, the BCS will command the aircraft to orbit until uplink acquisition is regained.

The BCS is engaged automatically if failure is detected in any of the following systems: simplex actuators, primary hydraulics, primary electrical power, uplink, or the primary computer. The primary computer controls the flight mode, except in the case of primary computer failure. When the primary computer detects one of the above failures, it commands the backup computer to enter the backup mode by sending a message on the intercom. When the primary computer fails, the transfer to the BCS mode is initiated by a watchdog interrupt. The BCS may also be entered by an uplink command.

The BCS contains a recovery mode which brings the vehicle to a stable attitude following entry into the BCS. Following exit from recovery mode, the orbit mode is entered if there are no other pilot inputs. In orbit mode the vehicle climbs to the next highest altitude of 5000, 10,000 or 25,000 ft (or dives if altitude is greater than 25,000 ft) and then orbits at a bank angle of approximately 35 deg. When exit-orbit is commanded, the vehicle will fly straight and level until commanded otherwise. The pilot may command left bank, right bank, climb, dive, increase speed, or decrease speed. Climbing and diving turns are permitted. The bank angle is normally fixed at 0 deg for straight and level, or 35 deg for turns; however, the BCS contains a roll rate command mode which allows the pilot to control the roll attitude.

The BCS contains an automatic landing mode which commands airspeed, sink rate, and flare initiation as a function of radar altitude. On the fifth flight of HiMAT air vehicle 1, the aircraft was landed utilizing the BCS autoland system as the result of an inflight uplink decoder failure. The landing on the dry lakebed runway was quite satisfactory with a touchdown at 186 knots and a sink rate of less than 3 ft/s. The BCS also contains engine-out modes for both glide and autoland. A full description of the BCS is provided in Ref. 2.

#### **Ground Test Mode**

Selected ground tests may be executed when the system test console is interfaced to the onboard computers. The purpose of the ground tests is to verify proper operation of the computer interfaces and aircraft systems in a nonflight environment. The operator selects ground test mode and the desired test number through the STC. The go and no-go lights and a four-digit test data display on the STC are used to output most test results. Approximately 160 tests are resident in the onboard computer which verify STC interfaces, uplink

hardware, downlink hardware, input and output discretes, and flight control and engine sensors and actuators.

#### **Captive Test Mode**

Two test modes, designated PCS test and BCS test, can be selected from the cockpit. These test modes may be activated only while the vehicle is captive on the B-52 launch aircraft and are utilized to assure proper system performance prior to launch. In PCS test mode, the primary sides of the duplex rudders and elevons are activated and all flight control surfaces and the throttle may be cycled from the ground cockpit. In BCS test mode, the secondary sides of the duplex rudders and elevons are activated and these surfaces are commanded to fixed, predetermined positions depending upon the settings of the BCS command discretes in either the ground cockpit or the TF-104G chase aircraft.

### **System Qualification**

#### **Qualification Tests**

Extensive qualification testing of both the hardware and software was required to certify a HiMAT vehicle for flight. Onboard computer hardware was qualified environmentally by the use of components meeting military specifications and by environmental tests both before and after delivery. Computer hardware was tested to the requirements of NASA Dryden Process Specification 21-2, which defines altitude, temperature, and vibration test profiles.

Functional verification of the onboard computer interfaces was accomplished in four different test sequences (integrated systems, combined systems, iron bird, and preflight), portions of which are repeated any time a modification is required to the interface.

The integrated systems test sequence was conducted to demonstrate that each vehicle subsystem operated correctly. This test phase included signal interface and continuity checks, power system checks, the functional qualification of both the backup and primary hydraulic and servoactuator systems, vehicle telemetry uplink and downlink system testing, and engine test runs with the engine both installed and uninstalled.

Combined system testing was conducted with the HiMAT vehicle operating in combination with the RPRV facility. All ground and airborne systems are active in these tests, with the exception of the radio frequency links, which are hard lined with cables. This test sequence included end-to-end signal verification, closed-loop total system and subsystem time delay measurements, ground resonance tests, and automated preflight testing, both onboard and ground based. Open-loop failure modes and effects tests were conducted to validate the proper system response to component and subsystem failures.

The iron bird simulation test sequence expands on the combined systems test configuration to include real-time simulation of the vehicle dynamics. Tests conducted during this phase include dynamic response tests for both the PCS and BCS flight modes, limit cycle tests, closed-loop failure modes and effects tests, piloted evaluation and training, and a complete mission simulation.

Vehicle preflights are a final check of all vehicle subsystems and are performed as close to each flight day as possible. This test sequence uses the interface test capability resident in the onboard computers to verify interface and subsystem operation. Upon completion of the preflight, all subsystem configurations are frozen and cannot be changed without violating the preflight. If removal of hardware is required, a preflight must be performed again on that item.

#### **Simulation Systems**

Four types of simulations are used to qualify onboard computer software. In each of these systems, the vehicle dynamics are simulated in the Dryden Cyber 73-28 computer. The four HiMAT simulation systems, termed all-Cyber,

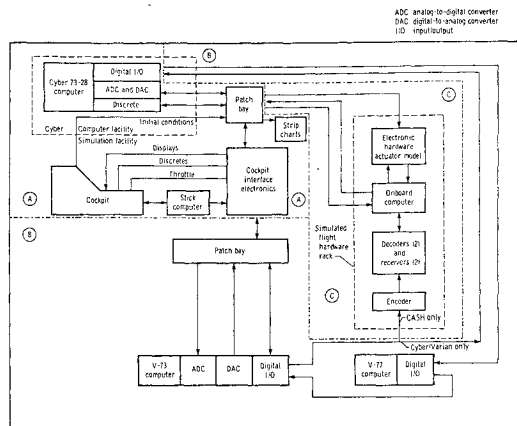


Fig. 5 HiMAT nonaircraft simulation configurations (A = all Cyber, A + B = Cyber-Varian, A + B + C = CASH).

Cyber-Varian, CASH (computation and simulation for HiMAT), and iron bird are described below. In the order presented, each includes more actual HiMAT hardware in the loop than the previous one.

The all-Cyber simulation (Fig. 5, part A) is the principal tool in the design and development of both the BCS and PCS software since it permits designs to be verified in a dynamic environment before they are implemented in the ground and airborne flight computers. In this simulation the HiMAT servoactuator system and the uplink and downlink systems are all modeled, along with HiMAT vehicle dynamics, using a Cyber 73-28 computer. This simulation is interfaced by way of the Cyber computer's real-time input/output system with a HiMAT simulation cockpit.

The Cyber-Varian simulation (Fig. 5, parts A and B) allows much of the HiMAT PCS software to be validated in the simulation facility with ground computers identical to those used for flight and with a full simulation of the HiMAT vehicle dynamics. Simulation cockpit, uplink and downlink interfaces are such that ground-based software can be identical to the software for the RPRV facility computers. This simulation method is the least useful for design or verification of onboard software.

The CASH system (Fig. 5, parts A, B, and C) goes a step further than the Cyber-Varian simulation just described. In this simulation, an actual HiMAT onboard computer is interfaced with the Cyber and simulation facility ground computers. An uplink encoder is hard lined to an uplink decoder, bypassing only the transmitter/receiver radio frequency link. The decoder is interfaced with the onboard computer, just as in the flight configuration. A high-fidelity electronic model of each of the HiMAT servoactuator channels is interfaced with the onboard computer, and the output of these actuator models is monitored by the Cyber computer which calculates vehicle response. This configuration is used extensively for both ground and airborne software validation and verification, since both the BCS and PCS software are executed in computers identical to those used for flight.

The iron bird simulation (Fig. 6) represents the most sophisticated of the HiMAT ground test phases, making maximum use of actual flight hardware by incorporating the flight vehicle in the loop. In this configuration, the aircraft and RPRV facility systems can be made to function as if the HiMAT vehicles were in flight. With the HiMAT vehicle in the hanger, the telemetry downlink is hard lined to the RPRV facility, as is the uplink command system to the vehicle; all vehicle control loops are active. The simulation of the vehicle dynamics is similar to that used in the CASH system, except that actual surface positions are interfaced with the Cyber 73-28 computer. Vehicle response data are trunked to the vehicle,

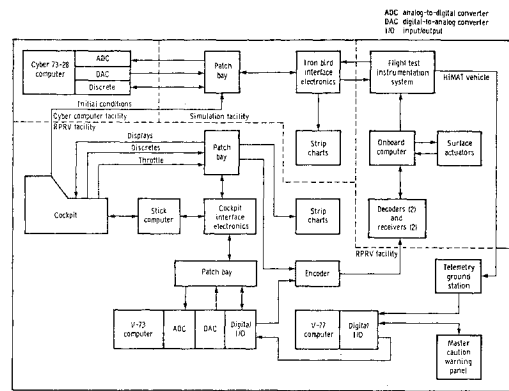


Fig. 6 HiMAT iron bird simulation.

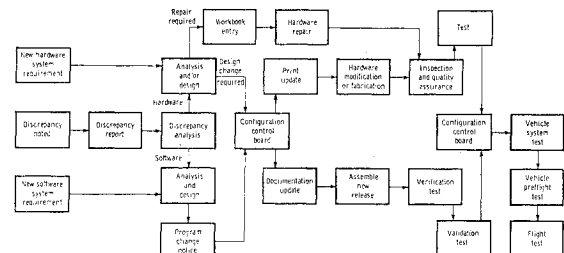


Fig. 7 HiMAT configuration control process.

summed with the actual vehicle transducer outputs, and input to the telemetry downlink system. The iron bird simulation provides for a full system validation of both the BCS and PCS.

#### Software Qualification

Flight software undergoes two types of testing activity during the process of flight qualification: verification and validation. Verification is the process by which it is determined that the software performs as specified. It is accomplished by devising individual tests for each specified software task, conducting the test, and observing that the task was accomplished according to the specification. Validation is the broader task which seeks to determine if the system, of which the software is a part, performs adequately to accomplish the flight requirements. Failure modes and effects tests (both open loop and closed loop) are among the techniques used in software validation. In these tests, failures are artificially induced and a proper system response to those failures is verified.

The onboard flight software is developed and verified using a microprocessor development system (MDS) and the airborne computer test set, a stand-alone bench facility which simulates the HiMAT systems/computer interfaces. Software validation is done primarily with CASH and iron bird simulations.

#### Ground Test Requirements

Adequate ground test and computer interface equipment is essential for the proper qualification of the airborne system in the operational configuration. As delivered, computer memory display consisted of a three-digit octal display addressable by thumbwheel switches. Only one byte of RAM memory at a time could be interrogated, while many parameters are stored as 16-bit (two-byte) quantities. This minimal capability was inadequate for verification of hardware interfaces or of software.

As a result the aircraft interrogation and display system (AIDS) was developed to provide increased onboard computer system visibility. The AIDS is an independent



microprocessor-based system that interfaces with the HiMAT onboard computer through the same data port that services the STC. Any data available in the onboard computer memory can be displayed on a dynamically refreshed cathode ray tube (CRT) monitor. Up to 20 individually labeled parameters may be displayed at a time in either raw input form or engineering units. This system also contains a printer which can be used to provide hard copy of any CRT display. The AIDS has greatly reduced the manpower required to conduct failure modes and effects testing and systems hardware and software validation.

#### Configuration Control

Rigorous configuration control procedures are utilized to track onboard flight computer hardware and software changes. An outline of the configuration control process is shown in Fig. 7. Hardware and software changes result from changes in requirements or from system discrepancies. Procedures are provided for documenting and tracking all discrepancies and changes. All changes, including those associated with discrepancies, must be approved by a configuration control board before they can be implemented for flight. Hardware changes are tracked by the NASA work order system and, if applicable, by the HiMAT discrepancy report system. Software changes are tracked by the program change/program verification and validation paperwork and procedures. Verification/validation procedures must be accomplished for each change and software documentation updated before that change is approved for flight.

Changes to onboard software require the manufacture of a new flight release. Source code changes are incorporated in a source file maintained on the Cyber computer; then the new total program is assembled by the cross-assembler on the Cyber computer. The Intel hexadecimal format object code is transported to the MDS, into which it is loaded for the purpose of programming the EPROMs used in the flight computer. An octal memory checksum is computed from the assembled output on the Cyber computer and compared with that computed in the HiMAT onboard computer as part of its self-test; this is part of the verification that the cross-assembler output has been accurately transferred to the flight computer. Software verification and validation test procedures use the flight release. These tests may be per-

formed in a laboratory environment using the in-circuit emulator and the computer test set, in the simulation laboratory using the CASH simulation, or on the aircraft using the iron bird simulation or a stand-alone configuration. Primary and backup onboard computer flight releases are manufactured independently, although in practice both computers are updated in the same time period. Further information on the qualification procedures used for HiMAT can be found in Ref. 3.

#### Conclusion

The HiMAT vehicle development has demonstrated that microprocessor technology is capable of accomplishing complex onboard digital flight control tasks. The development and qualification procedures used on this program, while rigorous, have provided an orderly and efficient environment in which systems can be developed and modification can be made to both hardware and software with reliable results. The authors believe that the formal configuration control imposed on the development and qualification of the HiMAT onboard computer software actually reduced the time and manpower required before the first flight of the vehicle. During the final development and qualification tests, the software tasks were never on the critical path as has been the case for several sophisticated software-driven systems.

The original ground test equipment was very inefficient in that it provided extremely limited human readable output. This was corrected by the development of additional ground test equipment based on commercially available microprocessor hardware. This equipment, which provided dynamically refreshed human readable output in real time, allowed tremendous savings of time and manpower.

#### References

- <sup>1</sup>Petersen, K.L., "Flight Control Systems Development of Highly Maneuverable Aircraft Technology (HiMAT) Vehicle," AIAA Paper 79-1789, Aug. 1979.
- <sup>2</sup>Hoyt, C.E., Kempel, R.W., and Larson, R.R., "Backup Flight Control System for a Highly Maneuverable Remotely Piloted Research Vehicle," AIAA Paper 80-1761, Aug. 1980.
- <sup>3</sup>Myers, A.F. and Sheets, S.G., "Qualification of HiMAT Flight Systems," Paper presented at 7th Annual Symposium of Association for Unmanned Vehicle Systems, June 1980.

### Reminder: New Procedure for Submission of Manuscripts

*Authors please note:* If you wish your manuscript or preprint to be considered for publication, it must be submitted directly to the Editor-in-Chief, *not* to the AIAA Editorial Department. Read the section entitled "Submission of Manuscripts" on the inside front cover of this issue for the correct address. You will find other pertinent information on the inside back cover, "Information for Contributors to Journals of the AIAA." Failure to follow this new procedure will only delay consideration of your paper.