



**VLSI
ENCRYPTION/DECRYPTION
DEVICE DATA**

1993

**MYKOTRONX, INC
357 Van Ness Way, Suite 200
Torrance, California 90501
(310) 533-8100
FAX (310) 533-0527**

Table of Contents

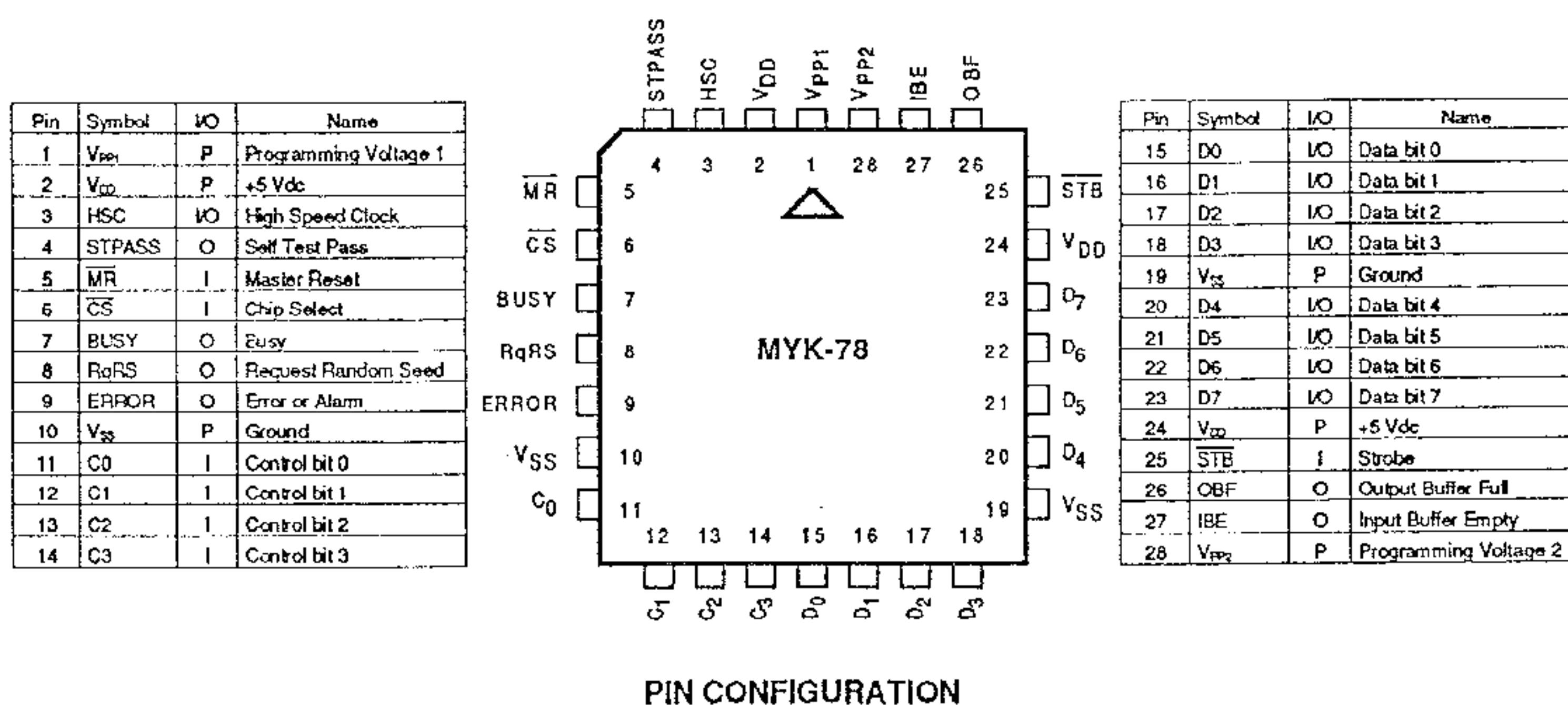
MYK-78 ENCRYPTION/DECRYPTION DEVICE	1-1
FUNCTIONAL DESCRIPTION	1-2
ENCRYPTION/DECRYPTION FUNCTION	1-2
DATA BUS BUFFER	1-2
CONTROLLER	1-2
ALGORITHM	1-3
SELF TEST LOGIC	1-3
INTERNAL OSCILLATOR	1-3
SECURITY FEATURES	1-3
SELF TEST	1-3
CV WRITE ONLY FEATURE	1-3
CV CHECK WORD TESTING	1-3
IV GENERATION	1-3
OPERATING STATES	1-3
INITIALIZATION	1-3
IDLE	1-4
PROCESS	1-4
REGISTERS	1-4
CONFIGURATION REGISTER	1-4
STATUS REGISTER	1-10
TEST/ALARM REGISTER	1-10
DEVICE COMMANDS	1-11
COMMAND DECODING	1-11
COMMAND DEFINITIONS	1-11
COMMAND AND DATA TRANSFERS	1-12
CV TEST	1-12
PIN DESCRIPTIONS	1-12
COMMAND, DATA AND DATA TRANSFER SIGNALS	1-12
CONTROL AND STATUS SIGNALS	1-13
HIGH SPEED CLOCK (HSC)	1-14
POWER AND GROUND	1-14
AC CHARACTERISTICS	1-15
DC CHARACTERISTICS	1-16
CAPACITANCE	1-16
RECOMMENDED OPERATING CONDITIONS	1-16
ABSOLUTE MAXIMUM RATINGS	1-16
 PLASTIC LEADED CHIP CARRIER (PLCC)	 A-1

MYK-78

ENCRYPTION/DECRYPTION DEVICE

- Supports Four Government DES Operating Modes
 - 64-Bit Electronic Code Book (ECB)
 - 64-Bit Cipher Block Chaining (CBC)
 - 8/16/32/64 Bit Cipher Feedback (CFB)
 - 64-Bit Output Feedback (OFB)
- Advanced Security Features
- Automatic Built-In Self Test (BIST) After Reset
- Performs Complete Algorithm Checks On Request
- On-Chip Initialization Vector (IV) Generator
- Automatic Crypto Variable (CV) Verification After Load
- Supports Clock Frequencies to 8 MHz
- 28-Pin PLCC Package
- TTL Compatible, Low-Power, 1-micron, 2-Layer Metal Bulk CMOS Insures High Reliability

The MYK-78 uses a Government Type II algorithm to encrypt and decrypt data under control of a microprocessor in the target system, which is referred to as the Control Processor (CP). The MYK-78 operates in one of four DES encryption/decryption modes, as selected by the CP. The MYK-78 insures the integrity of the crypto-algorithm using Built In Self Test (BIST) and off-line logic integrity checks. S-Box, check word, and crypto-variable (CV) parity tests are performed using a single algorithm test approach.



FUNCTIONAL DESCRIPTION

ENCRYPTION/DECRYPTION FUNCTION

The MYK-78 operates as a peripheral device to a control processor to encrypt or decrypt 8-bit bytes of data using a command strobe format. The MYK-78 accepts 16 commands via a four-bit command bus. These commands are used to configure the device, perform various security checks, process data, and monitor the status of the algorithm/device. The command sequence is restrictive. For security reasons, the MYK-78 rejects commands that are not submitted in the correct sequence.

During operation, a four bit command is strobed into the CP interface portion of the device. If the desired process requires a data input, one or more data bytes are then strobed into appropriate data registers. Depending on the command, the process is executed. If the process produces data, an appropriate command is used to read the data.

After the MYK-78 has been configured and security checks have been performed, encryption/decryption consists of repetitively writing input data and reading output data according to the selected DES mode. During multi-byte encryption/decryption process modes, an encryption or decryption command is issued and then the required number of data bytes are strobed in. After the last byte is input, the encryption/decryption process automatically begins. At the end of the process, the CP is notified, a read command is issued, the required number of data bytes are read out and the cycle repeats.

DATA BUS BUFFER

This is an eight-bit, bi-directional, tri state buffer that transfers CP data to and from the MYK-78 algorithm. The buffer is controlled by the controller.

CONTROLLER

The controller contains command decoding logic, registers and control logic. It functions as a peripheral interface circuit, controlling the transfer of data between the CP and the MYK-78 and controlling the operation of the MYK-78 based on commands provided by the CP.

The \overline{CS} and \overline{MR} inputs control the overall state of the MYK-78. Command bits C_0 through C_3 encode one of 16 commands. The controller latches these command bits using the STB input. The command bits are then decoded by the controller to determine the content of the command. Based on the decoded command, the controller establishes operating modes and controls the transfer of parallel data between the data bus buffer, the algorithm, the self test logic and internal registers and between the data buffer and the CP. The IBE output is provided by the controller for use by the CP in controlling the input of data to the data bus buffer. The OBF output is provided by the controller to indicate the output of data from the data bus buffer to the CP. The BUSY output notifies the CP when the MYK-78 is processing a command. During initialization, the RqRS output notifies the CP that a random seed input is required as the next initialization step.

The controller also controls the internal oscillator, enabling it during required processing sequences and disabling it when it is not required.

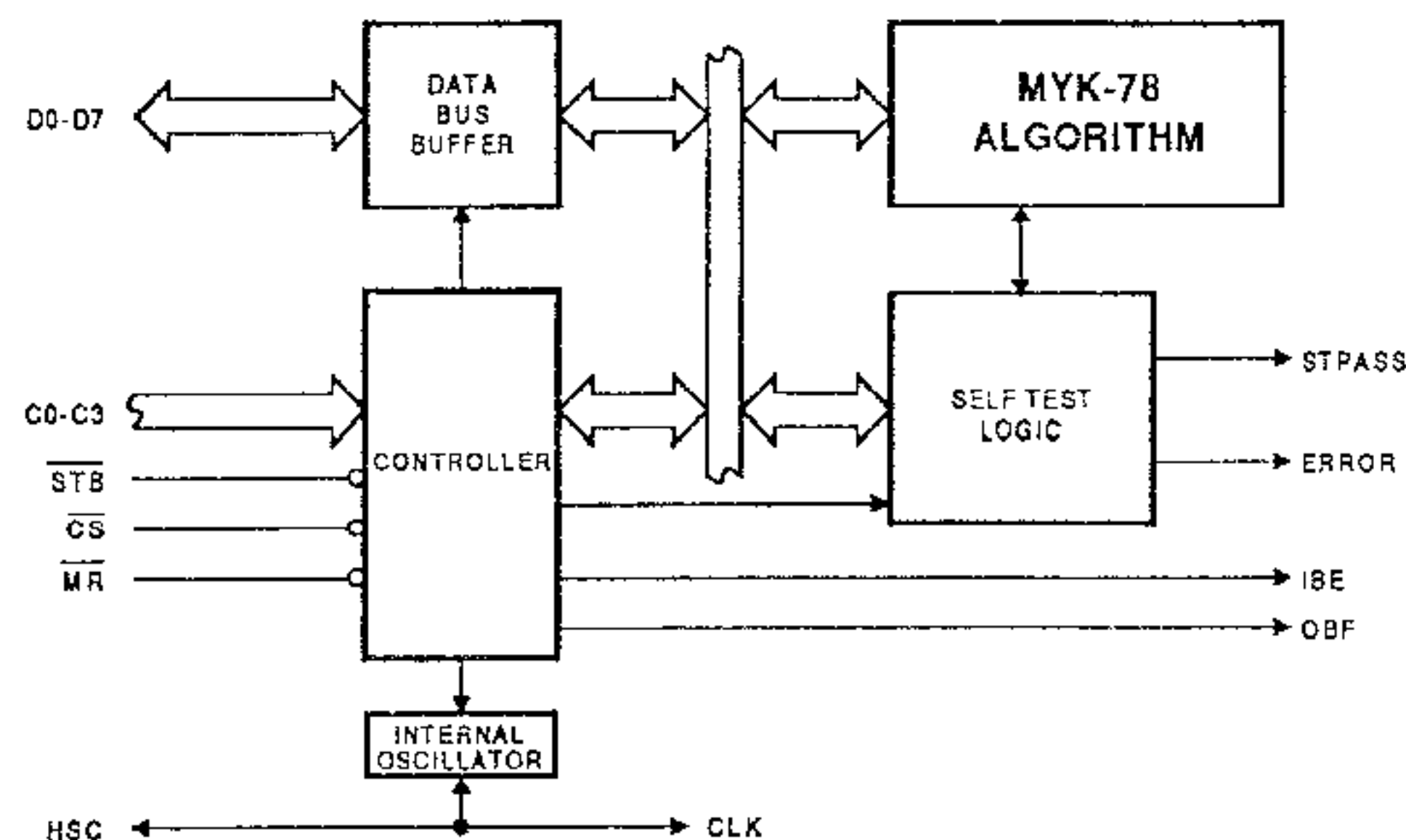


Figure 1. MYK-78 Simplified Block Diagram

ALGORITHM

The MYK-78 encrypts and decrypts data in one of the following DES modes:

- 64-Bit Electronic Codebook (ECB),
- 8/16/32/64 Bit Cipher Feedback (CFB),
- 64-Bit Cipher Block Chaining (CBC) and
- 64-Bit Output Feedback (OFB).

Refer to FIPS-PUB 81 for a detailed description of these DES modes of operation.

SELF TEST LOGIC

This logic operates with the algorithm to verify the integrity of the CV after it is transferred from the CP, to test the CV check word and to check for errors during operation. The self test logic can also be commanded to check itself to ensure that pass indications produced during normal self testing are valid. The self test logic provides two outputs to the CP (STPASS and ERROR) to indicate the result of testing and provides detailed test data to status and alarm registers in the controller.

INTERNAL OSCILLATOR

The internal delay oscillator is turned on either by the controller or by over-driving the feedback node with an external clock input on the HSC pin. The internal oscillator is active only during the encryption, decryption, initialization vector generation, self-test, algorithm tests and check word generation. When the oscillator is off, the HSC output is internally set to V_{DD} . The center frequency of the oscillator is 15 MHz. If the HSC pin is not overdriven and a capacitor is not connected, the HSC is an output and can be used by the CP for synchronization.

SECURITY FEATURES

There are four major security features embodied in the MYK-78:

- Self Test,
- CV Write Only Feature,
- CV Check Word Testing,
- Initial Vector (IV) Generation

SELF TEST

The self test achieves a fault grade of approximately 90% or better of the algorithm logic functions, depending on the crypto-variable and check word combination. The self test verifies proper operation of the control timing, CV transfers, algorithm testing and check word storage and comparison.

The MYK-78 powers-up using its own default CV and IV. A BIST starts after a reset is released and completes with a PASS or FAIL indicator showing the test result. The test pattern, CV and IV are chosen for the highest

possible fault coverage. During the power up BIST, no data exits the MYK-78.

CV WRITE ONLY FEATURE

Once the CV has been loaded, it cannot be read.

CV CHECK WORD TESTING

The integrity of the CV is verified after a CV is transferred from the CP. The CV is transferred along with a 24 bit check word that is stored on the chip. The check word is computed using the algorithm and the CV. The resulting value is then compared to the stored 24-bit check word that was loaded with the CV. In this way, the CV and the algorithm create a signature that should match the check word. This test also verifies the control timing since the test mode timing is the same as the operational mode timing except that the input plain text is a known pattern. A single error will set the error flag, disable the device outputs and inhibit normal algorithm operation. To resume normal operation, the CP must read out the signature and enter a CV with the correct check word.

IV GENERATION

The bits in the input register at the beginning of an encryption process are defined as the IV. To protect the key variable from crypto analysis, FIPS 140/FED-STD-1027 requires that the IV be derived from a random or pseudo-random source and that a new IV be used for each new transmission.

The MYK-78 has a new feature not found in current DES chips. A command can be issued that causes the MYK-78 to generate its own random IV based on a single input random seed and provide that IV to the target system. There is no limit to the number of initial vectors that can be generated based on a single random seed load. However, if the random seed is zeroized, a new seed value is requested (using the RqRS output).

The IV is generated by the MYK-78 device based on the supplied random seed. The random seed is generated by the CP by any means deemed adequate per the FED Standard. The random seed is loaded only once after a reset or a power-up state. The MYK-78 generates a new IV in response to a specific command. The IV is computed within 650 high speed clocks. The new IV is read out in response to another command from the CP.

OPERATING STATES

The MYK-78 operates in one of five states. These states are illustrated in Figure 2. The MYK-78 changes its operating state as a result of a reset, a valid command, or upon the completion of a process. See the *COMMAND DEFINITION* section below for a complete description of MYK-78 commands.

INITIALIZATION

The initialization state is entered when power is first applied or when the $\overline{\text{RESET}}$ input goes low. As shown in Figure 3, the MYK-78 first performs a BIST and then waits for the correct command from the CP. The MYK-78

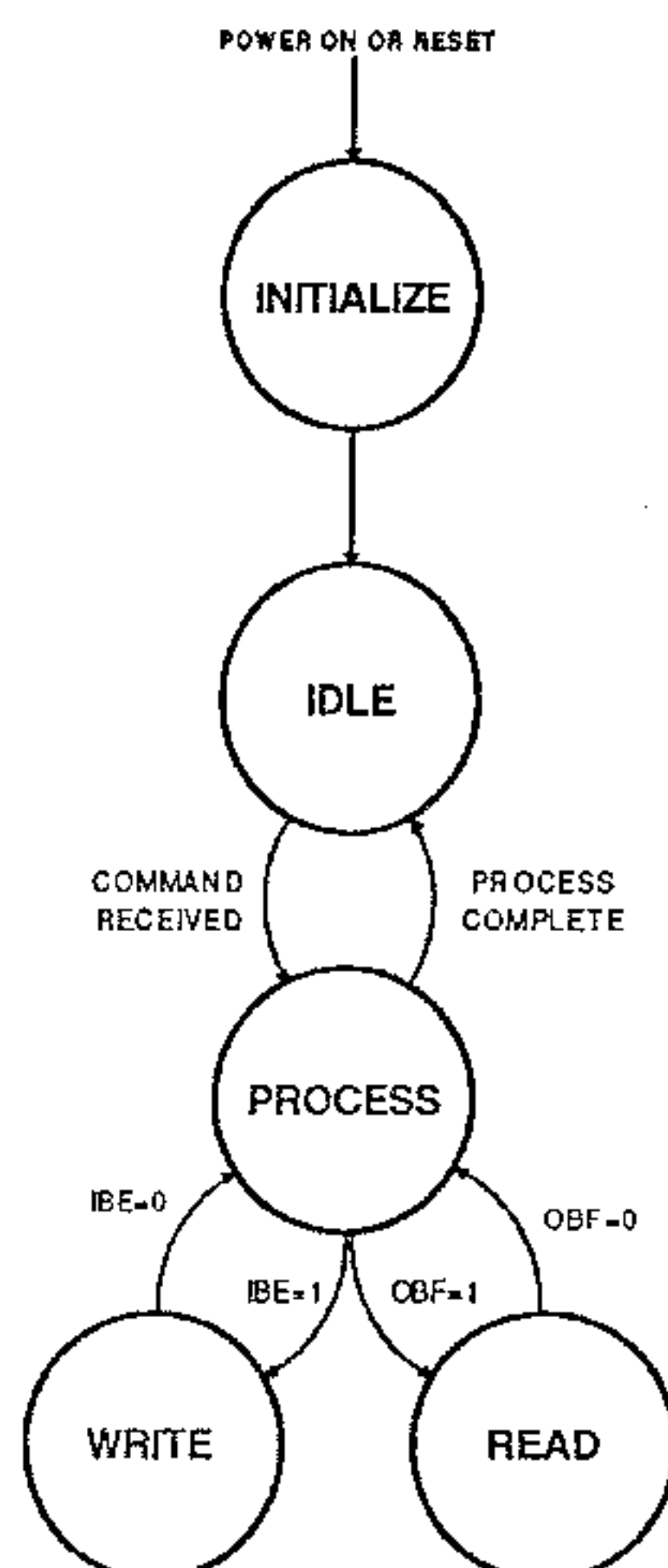


Figure 2. General State Diagram

must receive a series of commands in the proper order in order to successfully complete initialization and transit to the idle state. During initialization, the MYK-78 must first receive a random seed (RS) command, which inputs the random seed to the MYK-78. Next, the CP must provide a configuration word to the MYK-78 to establish the DES mode and testing options. Finally, the CP must provide the CV. The MYK-78 then tests the CV and check word and, if the test passes, enters the IDLE state. If an error occurs, the MYK-78 notifies the CP using the ERROR flag. Note that the CP can obtain detailed status information from the MYK-78 at any time during initialization. If other commands are issued by the CP or the sequence of the above commands is incorrect, an error will occur (as indicated by the ERROR flag).

IDLE

In the idle state, the MYK-78 simply waits for a command as shown in Figure 4. When a command is received, the MYK-78 enters the process state.

PROCESS

In the process state, the MYK-78 takes the action specified by the command. Figure 5 shows the flow for various commands and actions. If the command requires that data be transferred, the MYK-78 enters the write or read

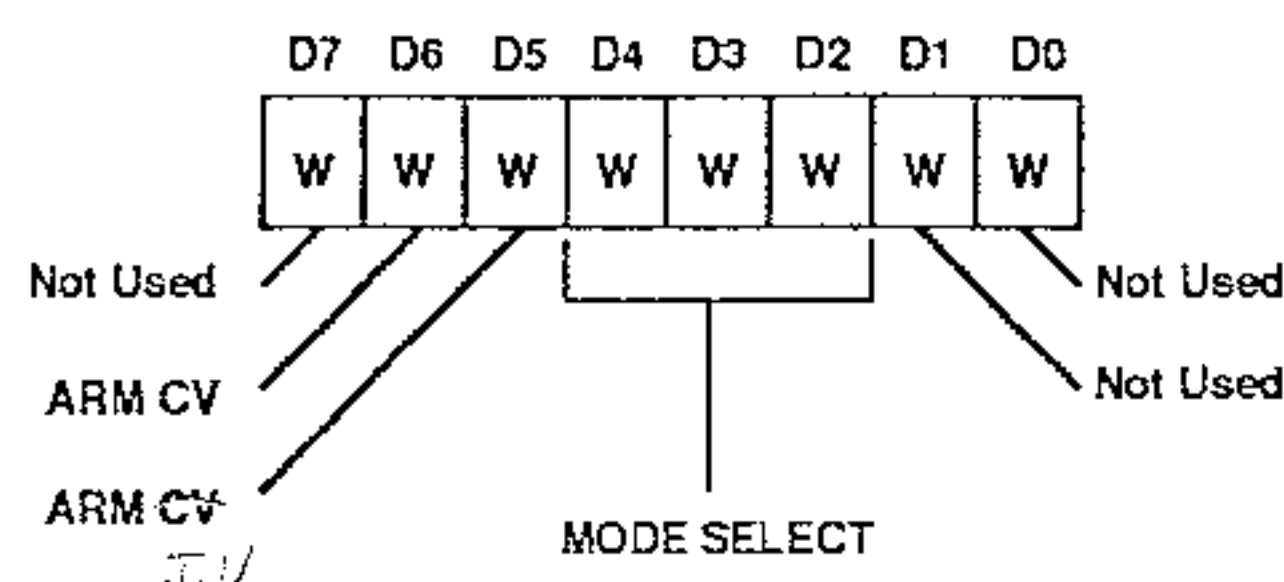
state, transfers a specified number of bytes and returns to the process state. When processing is complete, the MYK-78 returns to the idle state.

REGISTERS

The MYK-78 contains three registers. These registers are accessed by the CP to configure and test the device and to obtain status. These include a Configuration register, a Status register and a Test/Alarm register.

CONFIGURATION REGISTER

During initialization, this register is written by the CP using the WRITE CONFIGURATION REGISTER command to set-up the MYK-78 for modes of operation.



ARM IV LOAD

In order to load IV data into the MYK-78 while it is in the idle state, a WRITE CONFIGURATION REGISTER command must first be sent to set the ARM IV LOAD bit high and then a WRITE IV command must be sent. When the WRITE IV command is received, the ARM IV LOAD bit is automatically set low. If, while the MYK-78 is in the idle state, a WRITE IV command is received when the ARM IV LOAD bit is low or if a another command is received when the ARM IV LOAD bit is high, the MYK-78 will indicate an error.

ARM CV LOAD

In order to load CV data into the MYK-78 while it is in the idle state, a WRITE CONFIGURATION REGISTER command must first be sent to set the ARM CV LOAD bit high and then a WRITE CV command must be sent. When the WRITE CV command is received, the ARM CV LOAD bit is automatically set low. If, while the MYK-78 is in the idle state, a WRITE CV command is received when the ARM CV LOAD bit is low or if a another command is received when the ARM CV LOAD bit is high, the MYK-78 will indicate an error.

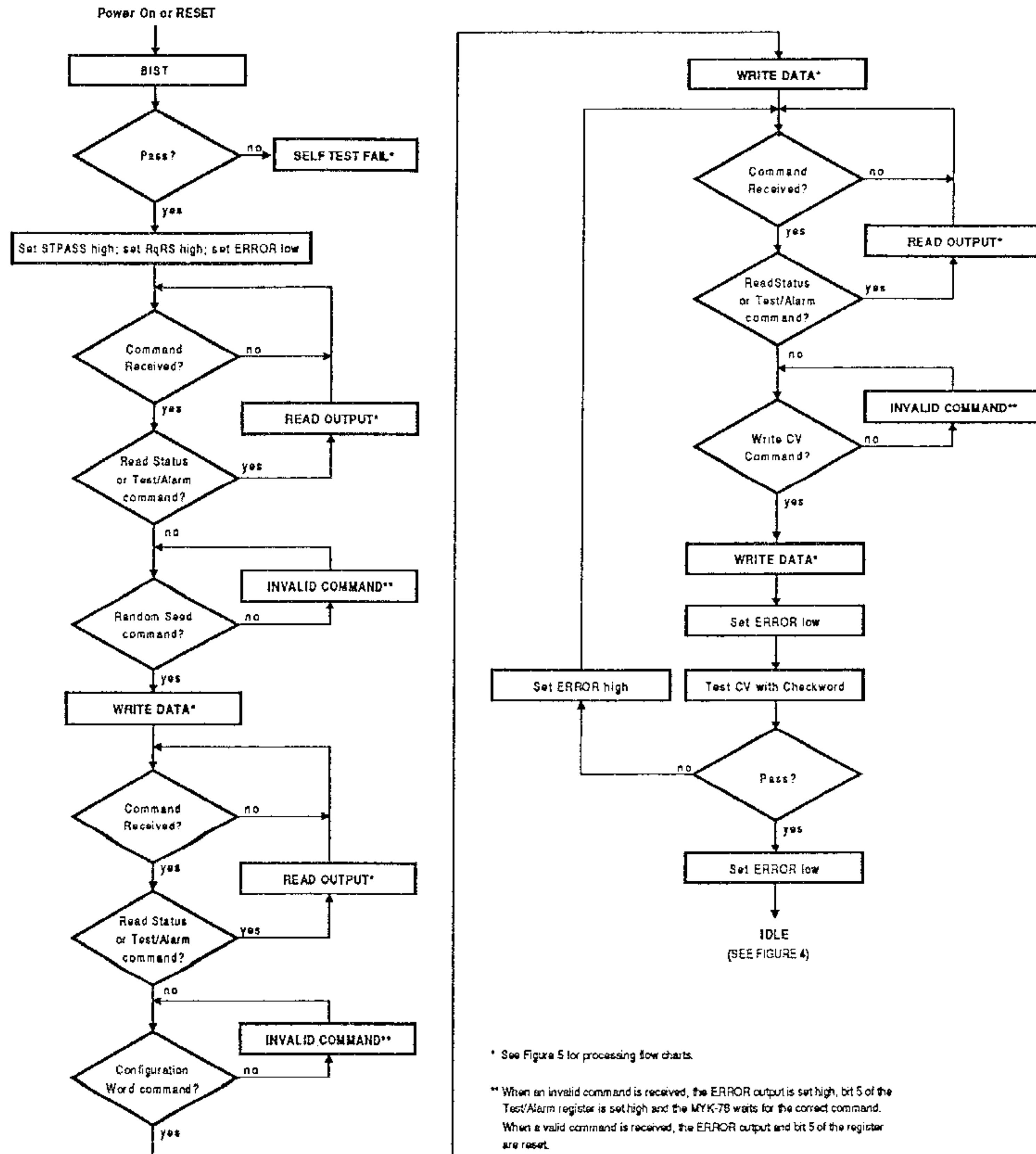
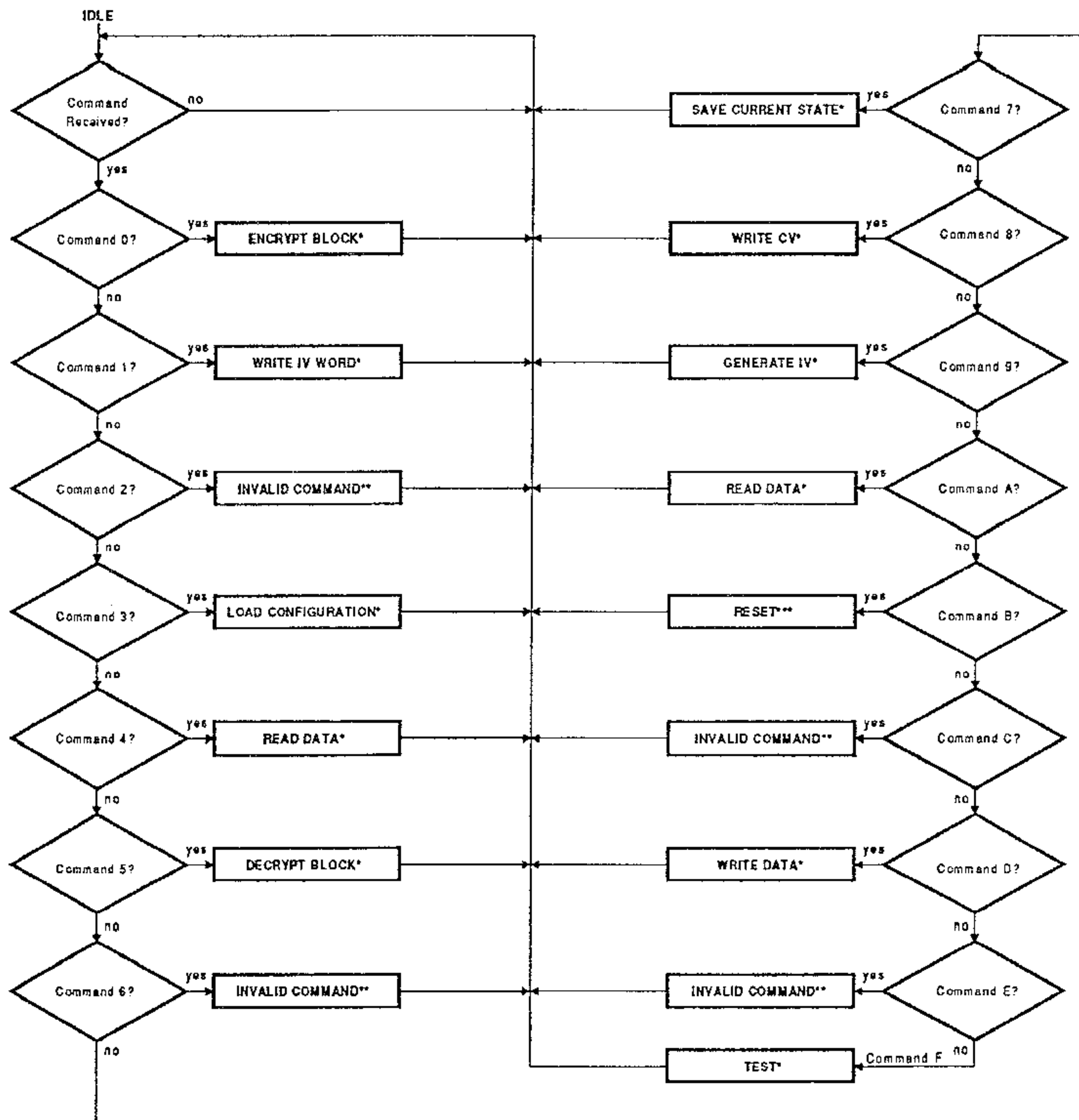


Figure 3. Initialization State Flow Chart

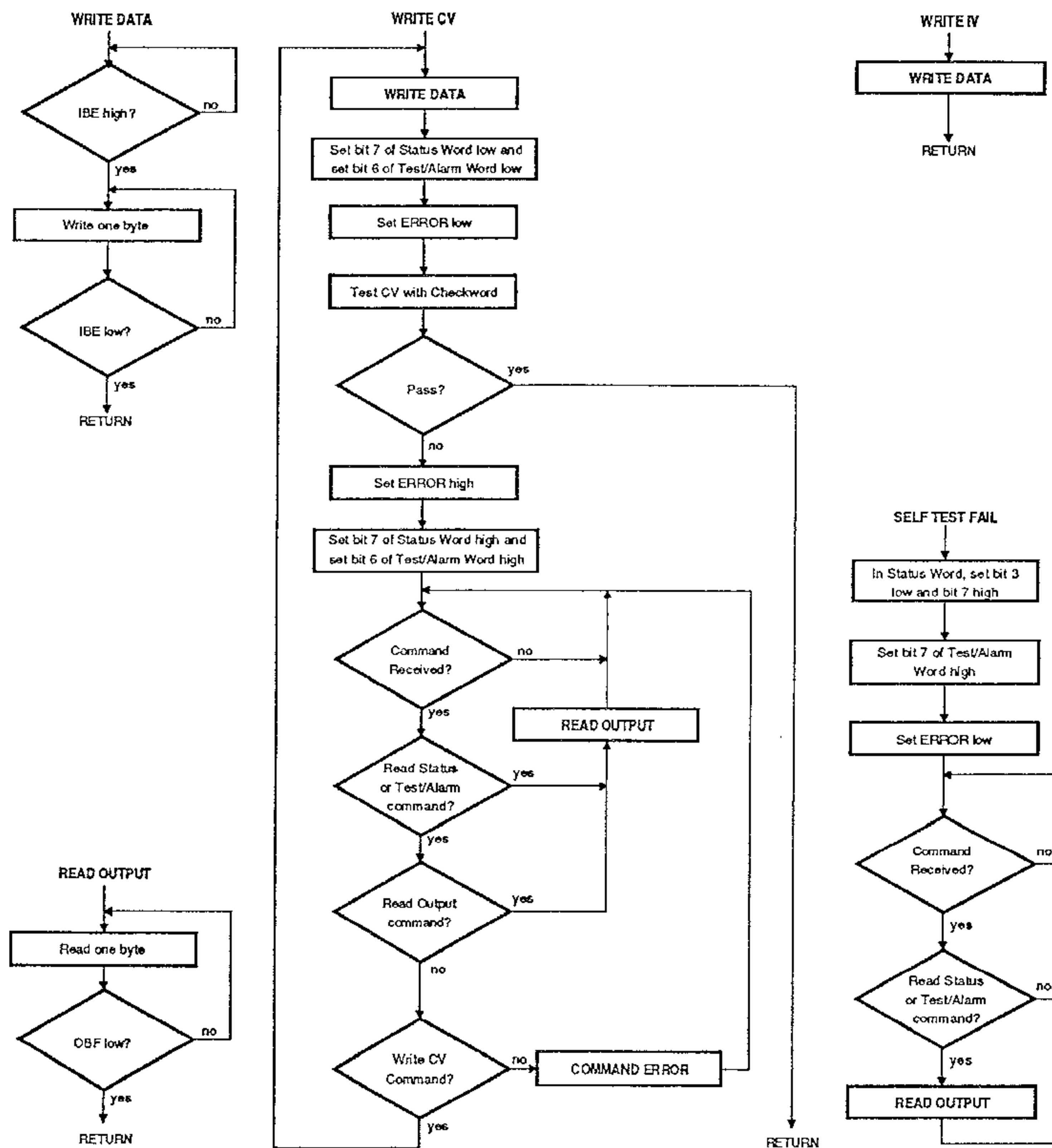


* See Figure 5 for processing flow charts.

** When an invalid command is received, the ERROR output is set high, bit 5 of the Test/Alarm register is set high and the MYK-78 returns to the idle state. When a valid command is subsequently received, the ERROR output and bit 5 of the register are reset.

*** See Figure 3 for processing flow chart.

Figure 4. Idle State Flow Chart



NOTE: At any time, setting MR low or sending a RESET command will cause the MYK-78 to reset (see Figure 3).

Figure 5. Processing, Read and Write Flow Chart (Sheet 1 of 3)

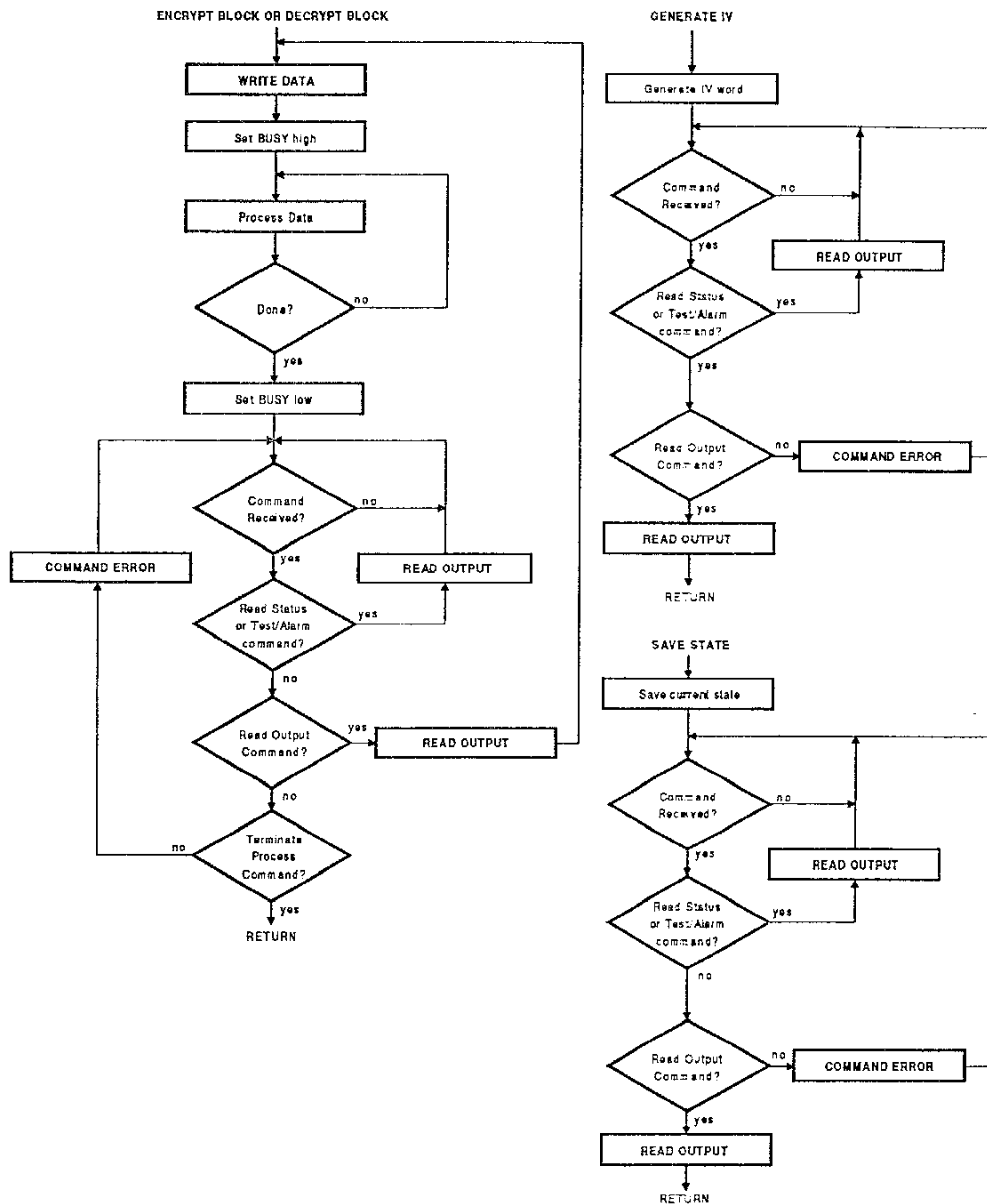


Figure 5. Processing, Read and Write Flow Chart (Sheet 2 of 3)

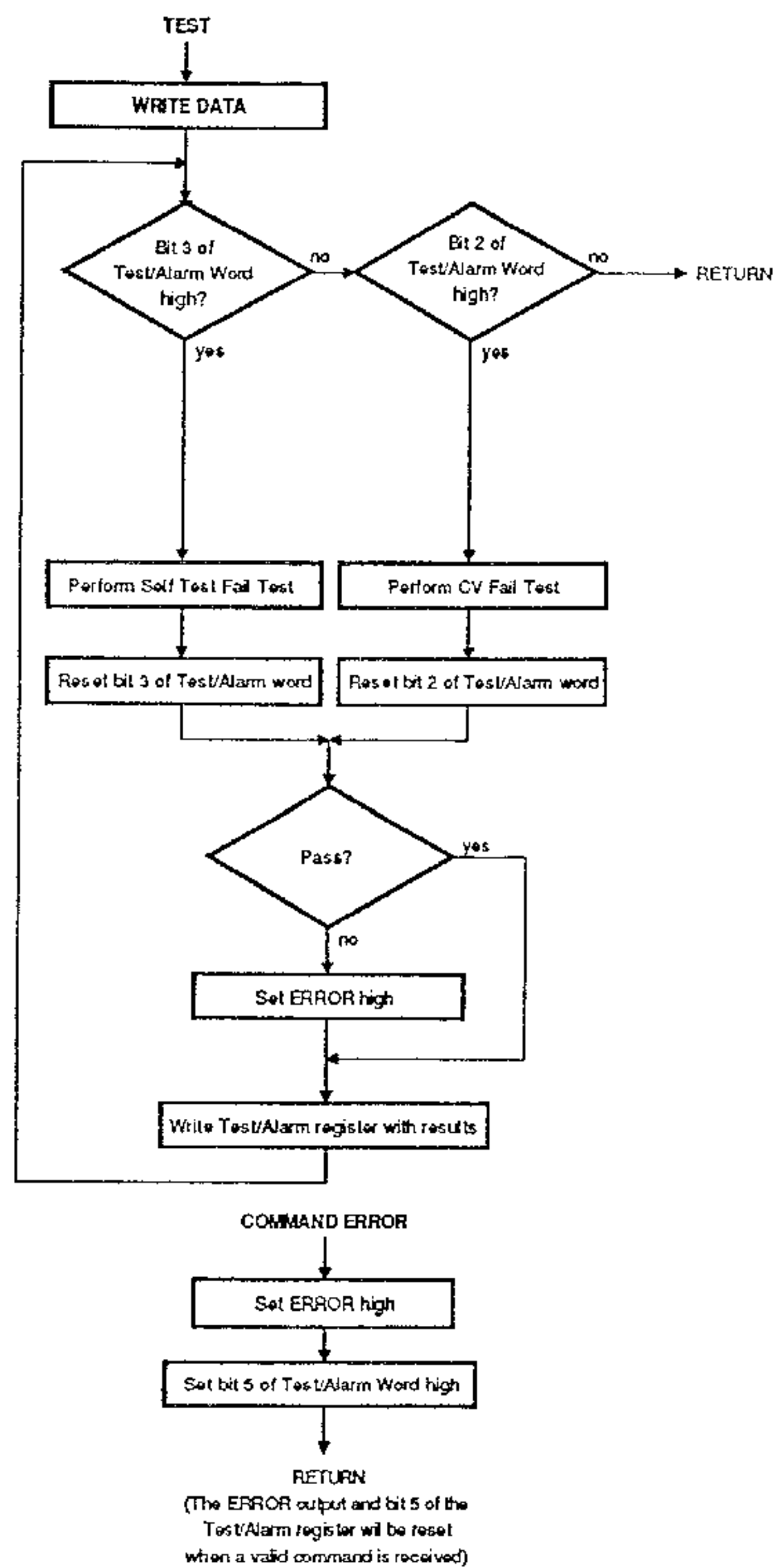


Figure 5. Processing, Read and Write Flow Chart (Sheet 3 of 3)

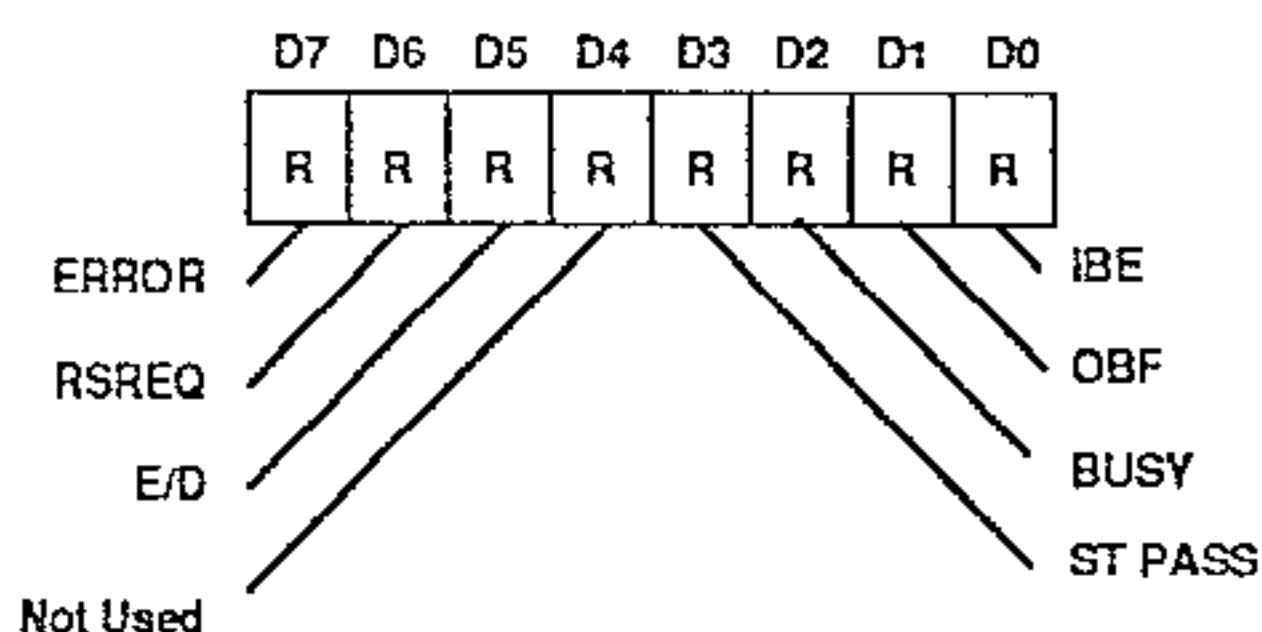
The mode select bits select the DES encryption/decryption mode as follows:

Bit			Mode
4	3	2	
0	0	0	ECB-64 bit
0	0	1	CBC-64 bit
0	1	0	OFB-64 bit
0	1	1	CFB-64 bit
1	0	0	CFB-32 bit
1	0	1	CFB-16 bit
1	1	0	CFB-8 bit
1	1	1	Not used

Refer to FIPS PUB 81 for a detailed description of the DES modes of operation.

STATUS REGISTER

This register is written by the CP using the READ STATUS REGISTER command to obtain the status of the MYK-78.



ERROR

This bit is set high when a failure occurs during the BIST, during an operational test or during a CV test (see the CV TEST section below). This bit is cleared by resetting the MYK-78 or by re-loading the CV. The ERROR bit will also be set high if an invalid command is received. In this case, the ERROR bit will be cleared when the correct command is received. To obtain the specific error status, use the READ TEST/ALARM REGISTER command.

RSREQ

This bit is set high after power up or reset to request the random seed from the CP (similar to the RqRS output). After the random seed has been successfully loaded, this bit is set low.

E/D

This bit indicates the encrypt/decrypt status MYK-78. When the START ENCRYPT BLOCK command is received, this bit goes high. When the START DECRYPT BLOCK command is received, this bit goes low. This bit defaults low on power up or reset.

ST PASS

This bit goes low when power is applied or when a reset occurs. During power up or reset, this bit goes high and the STPASS flag output goes high if the BIST passes.

BUSY

This bit goes high whenever the MYK-78 is processing data, loading a CV or performing a self test. This bit also goes high if an alarm condition occurs. This bit is low at all other times.

OBF

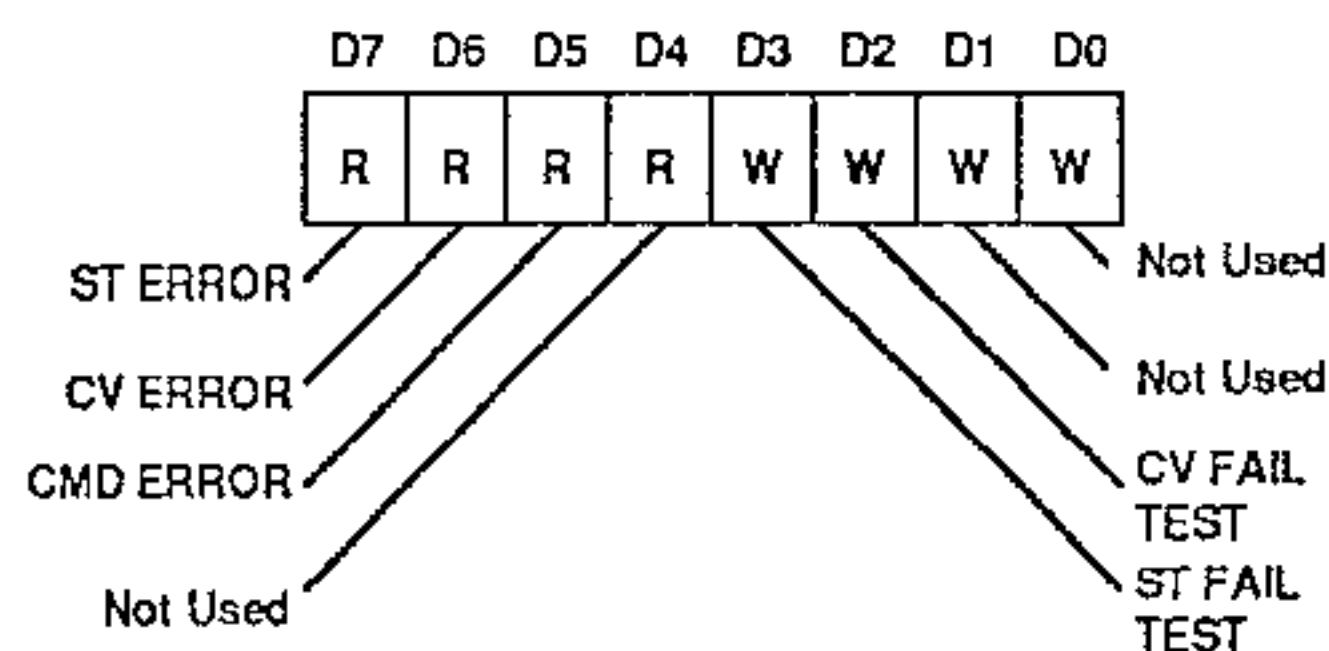
This bit goes high when the output data buffer is full and ready to be read out. After the buffer is read out, this bit resets to low. The default state is low.

IBF

This bit goes high when the input data buffer is empty or does not contain the specified number of bytes during a write operation. This bit goes low when input buffer is full. The default state is a low.

TEST/ALARM REGISTER

This register allows the CP to specify certain tests and to check for specific errors. Bits 7 through 5 are read-only and contain specific error flags which are set when an error occurs (as indicated when bit 7 of the Status register goes high). These bits are read using the READ TEST/ALARM REGISTER command. Bits 3 and 2 are write-only and allow the CP to define the test or tests to be performed. These bits are written using the WRITE TEST/ALARM REGISTER command. Bits 4, 1 and 0 are not used.



ST ERROR

This bit goes high when a BIST fails during initialization. This bit is cleared when reset occurs, when a WRITE CV command is received or when a the IV or CV is reloaded.

CV ERROR

This bit goes high when an error occurs during the CV test (see the CV TEST section below). This bit is cleared when the WRITE CV command is received. The default state of this bit is low.

CMD ERROR

This bit goes high if an illegal command is received. Once the error is detected, the MYK-78 halts until the correct

command is sent. This bit goes low again when the correct command is received by the MYK-78.

ST FAIL TEST

This bit is written by the CP using the WRITE TEST/ALARM REGISTER command. This command must also be written twice. If this bit is high, a self-test cycle is started and an error is injected in the algorithm. This test verifies that the ST TEST compare test logic is not stuck in the PASS state. If this test passes, bit 7 of this register (ST ERROR) goes high just as if an actual failure had occurred. If bit 7 remains low, this test has failed. The CV or IV is not altered during this test. To clear the simulated error condition, reset the chip.

CV FAIL TEST

This bit is written by the CP using the WRITE TEST/ALARM REGISTER command. This command must also be written twice. If this bit is high, a self-test cycle is started and an error is injected in the CV. This test verifies that the CV check word compare logic is not stuck in the PASS state. If this test passes, bit 6 of this register (CV ERROR) goes high just as if an actual failure had occurred. If bit 6 remains low, this test has failed. To clear the simulated error condition, issue the WRITE CV command.

DEVICE COMMANDS

COMMAND DECODING

Bit State				Function
C ₃	C ₂	C ₁	C ₀	
0	0	0	0	Start Encrypt Block
0	0	0	1	Write IV
0	0	1	0	Not used
0	0	1	1	Write Configuration Register
0	1	0	0	Read Status Register
0	1	0	1	Start Decrypt Block
0	1	1	0	Read Output
0	1	1	1	Save Current State
1	0	0	0	Write CV
1	0	0	1	Generate IV
1	0	1	0	Read Test/Alarm Register
1	0	1	1	Reset
1	1	0	0	Terminate Encrypt/Decrypt Process
1	1	0	1	Restore Saved State
1	1	1	0	Write Random Seed
1	1	1	1	Write Test/Alarm Register

COMMAND DEFINITIONS

Start Encrypt Block Command

This command causes the MYK-78 to repetitively encrypt plain text data words. When the command is received, the first byte of the first data word is supplied on the data bus by the CP. The number of bytes comprising the word is based on the operating mode selected by mode bits 1, 2 and 3 in the Configuration register. The MYK-78 reads the appropriate number of bytes, processes the data, and then waits for a READ OUTPUT command from the CP. When the command is received, the MYK-78 places the appropriate number of cipher text data bytes on the data bus, one at a time until the entire word is read out. The MYK-78 then returns to IDLE and waits for the next command.

Write IV Command

When configuration register bit 5 (ARM WRITE IV) is set high, the WRITE IV command causes the MYK-78 to load the IV data word. After the last byte is loaded, the MYK-78 returns to the idle state. If the MYK-78 is in the idle state, the bit 5 of the configuration register must be set high using the WRITE CONFIGURATION REGISTER command before issuing the WRITE IV command.

Write Configuration Register Command

This is the second command that must be received during initialization. This command is used to load one byte of data which determines the DES mode of operation (see the *CONFIGURATION REGISTER* section above). This command can only be used to select the DES mode during initialization.

Read Status Register Command

This command causes the MYK-78 to place the contents of the Status register on the data bus.

Start Decrypt Block Command

This command causes the MYK-78 to repetitively decrypt cipher text data words. When the command is received, the first byte of the first data word is supplied on the data bus by the CP. The number of bytes comprising the word is based on the operating mode selected by mode bits 2, 3 and 4 in the Configuration register. The MYK-78 reads the appropriate number of bytes, processes the data, and then waits for a READ OUTPUT command from the CP. When the command is received, the MYK-78 places the appropriate number of plain text data bytes on the data bus, one at a time until the entire word is read out. The CP then places the first byte of the next data word on the data bus and the cycle repeats until a TERMINATE ENCRYPT/DECRYPT PROCESS command or other legitimate command is received.

Read Output Command

This command is used to read out result data from the MYK-78 following the conclusion of an ENCRYPT DATA BLOCK, DECRYPT DATA BLOCK, WRITE CV or GENERATE IV command.

Save Current State Command

This command causes the MYK-78 to save all of the data defining its operational state (eight 8-bit bytes). When the command is received, the MYK-78 places the each byte on the data bus, one at a time until all bytes have been read out.

Write CV Command

When configuration register bit 6 (ARM CV LOAD) is set high, the WRITE CV command causes the MYK-78 to load and store the CV word (10 bytes) and the corresponding check word (three bytes). After the last byte has been loaded, the MYK-78 begins the CV test (see the CV TEST section below). If the MYK-78 is in the idle state, the bit 6 of the configuration register must be set high using the WRITE CONFIGURATION REGISTER command before issuing the WRITE CV command.

Generate IV Command

This command causes the MYK-78 to generate an eight-byte IV word. On completion, the MYK-78 waits for a READ OUTPUT command from the CP. When the command is received, the MYK-78 places the each byte on the data bus, one at a time until all bytes have been read out. After the last byte is read out, the MYK-78 returns to the idle state.

Read Test/Alarm Register Command

This command causes the MYK-78 to place the contents of the Test/Alarm register on the data bus. After the CP reads the byte, the MYK-78 returns to the idle state.

Reset

This command causes the MYK-78 to reset and begin the initialization process. This command has the same effect as setting MR low and then high.

Terminate Encrypt/Decrypt Process Command

This command causes the MYK-78 to terminate an encrypt or decrypt process. The command is ignored if no encrypt or decrypt process is under way.

Restore Saved State Command

This command causes the MYK-78 to load the state space of the MYK-78 directly and place the device in a known state. It is assumed that the CP has previously uploaded the state data (8 bytes) using the SAVE CURRENT STATE command.

Write Random Seed Command

This must be the first command issued during the initialization sequence (power up or reset) and is used only once. This command is ignored thereafter. This command causes the MYK-78 to load and store the eight-byte random seed value. After the last byte has been loaded, the MYK-78 waits for a WRITE CONFIGURATION REGISTER command, a READ STATUS command or a READ TEST/ALARM REGISTER command. An error will be generated if any other command is issued by the CP. If a READ STATUS or READ TEST/ALARM

command is issued, the MYK-78 supplies the required data and then continues to wait for a WRITE CONFIGURATION REGISTER command.

Write Test/Alarm Register Command

This command causes the MYK-78 to load one data byte into the Test/Alarm register. After the byte is loaded, the command must be repeated. The MYK-78 then performs the test or tests specified in bits 2 and 3 of the Test/Alarm register. The results are indicated in bits 6 and 7 of the Test/Alarm register.

COMMAND AND DATA TRANSFERS

Commands on the command bus (C₀-C₃) are clocked in on the falling edge of \overline{STB} (see Figure 6). If the command involves writing data, the data on D₀-D₇ are strobed in on rising edges of \overline{STB} . Depending on the command, the required number of data bytes are strobed. When the required number of bytes have been strobed, the IBE flag goes low. The command bits must be held at the correct value for the number of bytes strobed. After the last byte is strobed in, the specified process starts (if any).

During the specified process, the BUSY flag goes high. When the BUSY flag goes low, the process is complete.

If the command involves reading data, the OBF flag goes high. The CP then uses \overline{STB} to strobe the data out. When the last byte has been strobed out, the OBF flag goes low.

CV TEST

A CV test is always performed after a WRITE CV command is received and the CV data is loaded.

When this command is received, the CV plus the CV check word are loaded and stored. Then, the MYK-78 generates a new CV check word that is a function of the stored CV, a known IV and the selected algorithm. This new check word is compared to the stored CV check word. If the two check words do not match, bit 7 of the Status register (ERROR) and bit 6 of the Test/Alarm register (CV ERROR) are set high. These error flags are cleared when another WRITE CV command is received.

PIN DESCRIPTIONS

The MYK-78 is packaged in a 28-pin Plastic Leaded Ceramic Chip Carrier (PLCC). Refer to Appendix A for physical dimensions. The following list describes the signal on each pin.

COMMAND, DATA AND DATA TRANSFER SIGNALS**C₀-C₃**

These command bus bits encode the commands issued to the MYK-78 from the CP. They are latched on falling edge of \overline{STB} (see Figure 6).

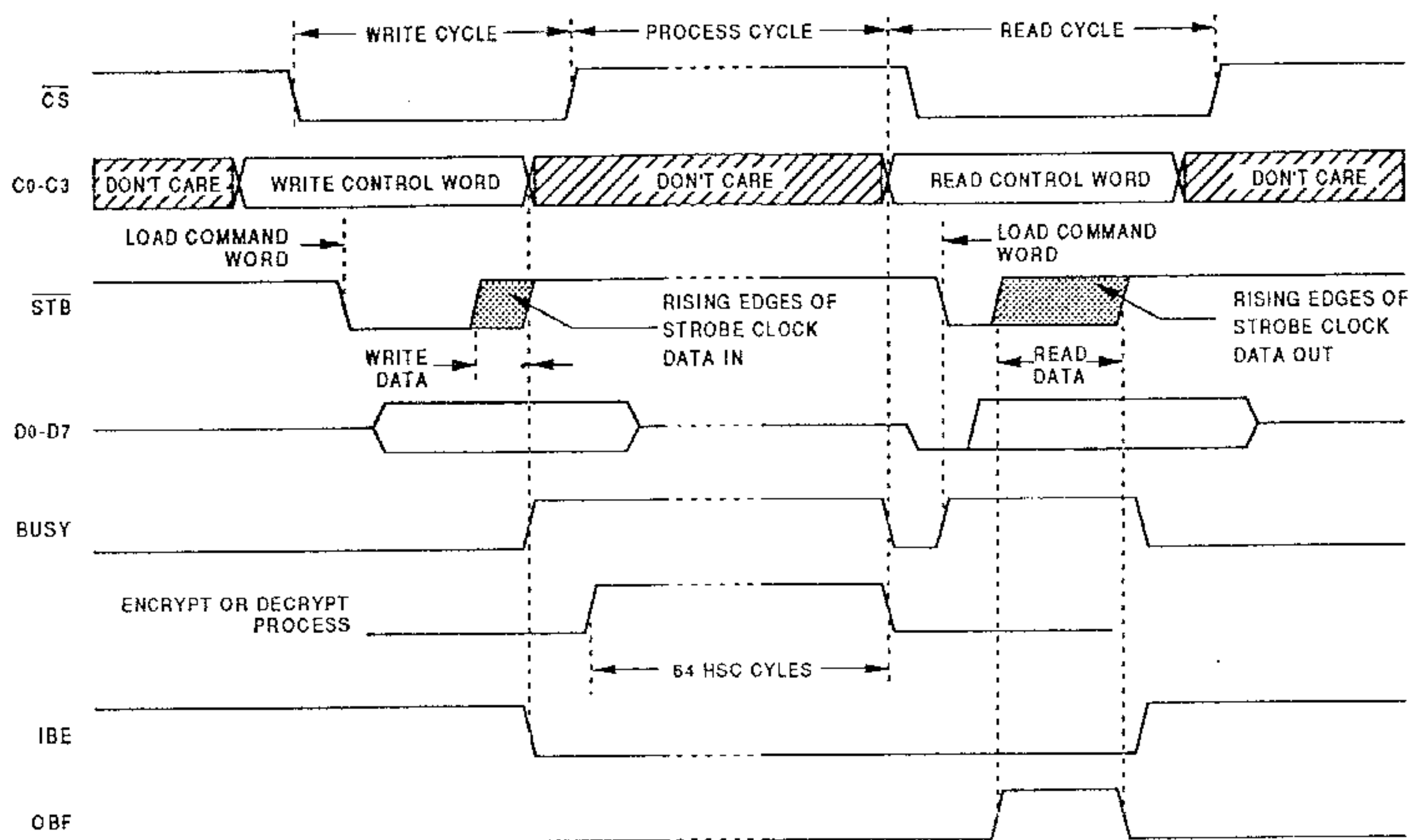


Figure 6. Command and Data Transfer Timing

D0-D7

These bi-directional data bus bits are used to transfer commands, status, IV data, IV check word data, CV data, CV check word data, plain text data and cipher text data. During a write operation, data are latched into the MYK-78 input buffer on the rising edge of \overline{STB} (see Figure 6). During a read operation, data are placed onto the data bus from the MYK-78 output buffer on the rising edge of \overline{STB} (see Figure 6).

\overline{STB}

The falling edge of this input latches command bus bits C0-C3 into the MYK-78 command buffer. During a write operation, the falling and rising edges of this signal latch the data present on the data bus (D0-D7) into the MYK-78 input buffer. During a read operation, the rising edge of this signal clocks data from the MYK-78 output buffer onto the data bus.

IBE

This output indicates the status of the MYK-78 data input buffer. A low indicates that the buffer is full and a high indicates that the buffer is empty.

OBF

This output indicates the status of the MYK-78 output buffer. A low indicates that the buffer is empty and a high indicates that the buffer is full.

CONTROL AND STATUS SIGNALS

\overline{CS}

Setting this input low enables the MYK-78 to access the command bus (C0-C3). Setting this input high causes the MYK-78 to set its command bus inputs to high impedance (tri-state).

\overline{MR}

Setting this input low causes the MYK-78 to reset all registers and storage elements, to tri-state the data bus (D0-D7) and to enter a quiescent, non-processing state. When the \overline{MR} input goes high, the MYK-78 enters the initialization state and begins its BIST.

BUSY

This output goes high when the MYK-78 is either processing data, conducting test or during the period when data is being read. This output is low at all other times.

STPASS

This output goes high after a BIST or other self test passes. This bit goes low immediately after a power up or reset (before and during BIST) or upon receipt of a WRITE CV command. See Figure 7.

ERROR

This output goes high after a BIST or other self test fails or when an illegal command is received. If an error occurred as a result of a test, this bit goes low immediately after a power up or reset (before and during BIST) or upon receipt of a WRITE CV command. If an error occurred as a result of an illegal command, this bit goes low when the correct command is received. See Figures 7 and 8.

RqRS

This output is low immediately after power up or reset and during BIST. If BIST passes, this bit goes high to

indicate that the next command issued by the CP must be a WRITE RANDOM SEED command (see Figure 7). When this command is received, the RqRS output goes low.

HIGH SPEED CLOCK (HSC)

High Speed Clock is a Schmitt trigger input/output with a minimum impedance of 250 ohms and maximum of 1 K ohm. A delay oscillator within the device is turned on by two means: an internal gate signal or an external clock input that over-drives the feedback node. The delay oscillator is active only during the encryption, decryption, IV generation, self-test, and check word tests. When the oscillator is off, the HSC output is internally set to V_{DD} . The center frequency of the internal oscillator is 15 MHz. The HSC pin can also be driven from an external source.

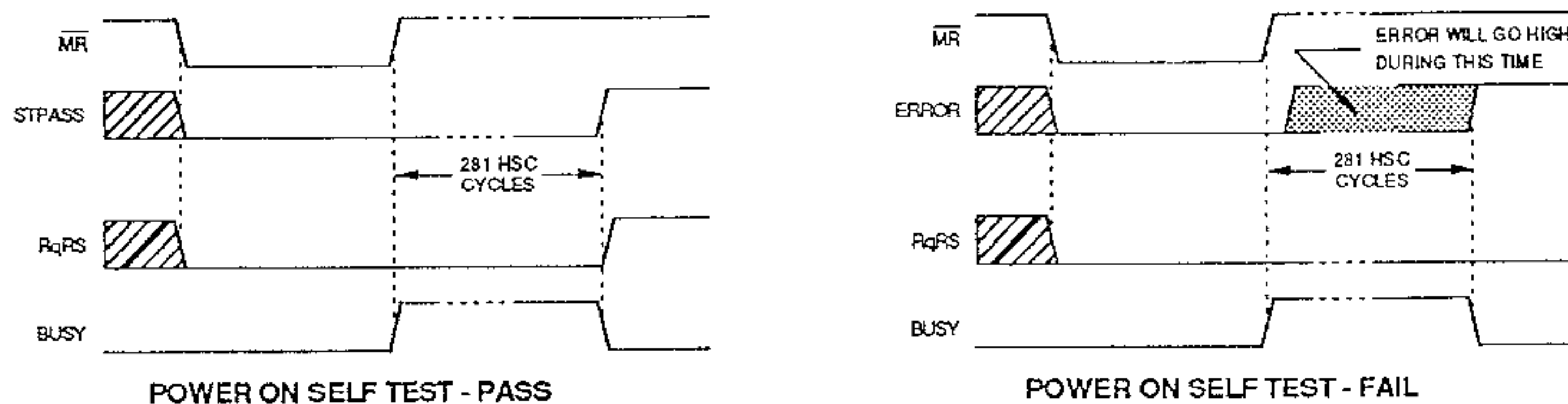


Figure 7. Power Up Self Test Timing

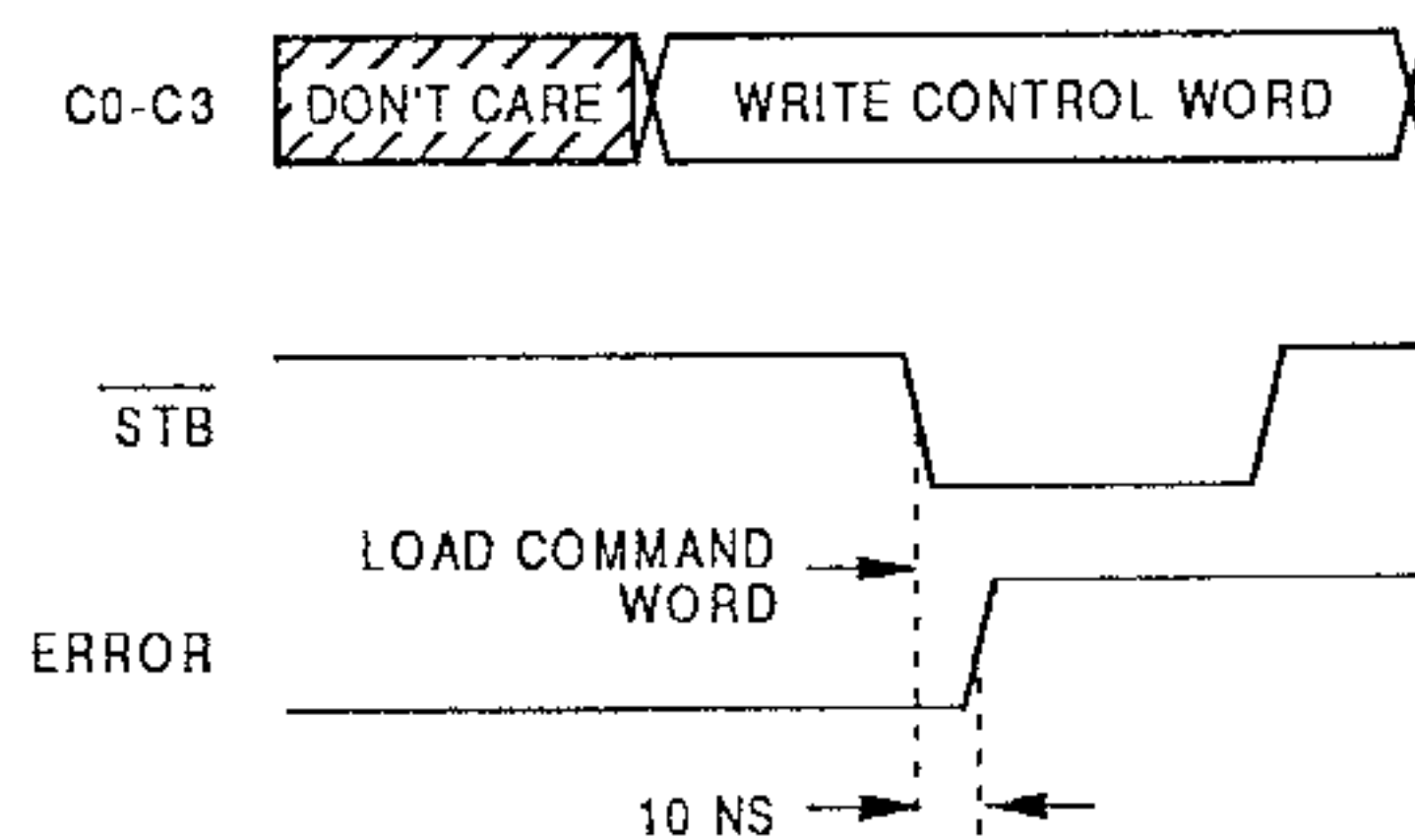


Figure 8. Command Error Timing

POWER AND GROUND

V_{DD} (Two Pins)

+5 Vdc input with a $\pm 10\%$ tolerance.

V_{SS} (Two Pins)

Negative power pins.

V_{PP1} and V_{PP2}

The MYK-78 requires two high voltage programming pins to program the internal non-volatile memory elements. These pins are open after programming.

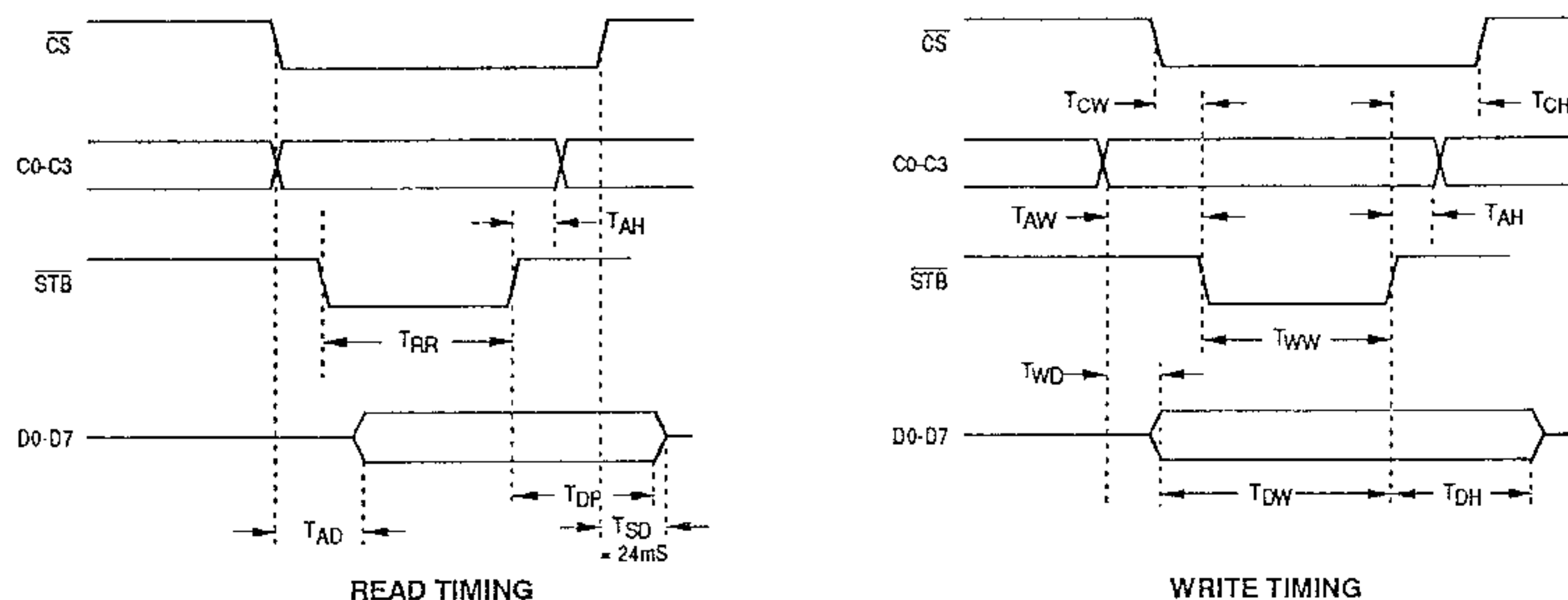


Figure 9. AC Characteristics

AC CHARACTERISTICS ($T_A = 0$ to $70\text{ }^\circ\text{C}$, $V_{DD} = 5V \pm 5\%$, $V_{SS} = 0V$)

Symbol	Parameter	Limits		Units
		Min.	Max.	
T_{AD}	Control bus stable and chip select low to data valid		40	ns
T_{AH}	Control bus hold after rising edge of \overline{STB}	-8		ns
T_{DF}	Rising edge of \overline{STB} to data invalid		30	ns
T_{RR}	\overline{STB} pulse width (read)	96		ns
T_{AW}	Control bus stable before falling edge of \overline{STB}	10		ns
T_{WD}	Data valid after Control bus changes to a write command	10		ns
T_{DW}	Data valid before rising edge of \overline{STB}	86		ns
T_{DH}	Data hold after rising edge of \overline{STB}	10		ns
T_{WW}	\overline{STB} pulse width (write)	130		ns
T_{CW}	Chip select stable before falling edge of \overline{STB}	10		ns
T_{SD}	Chip select to output = high impedance		24	ns

DC CHARACTERISTICS ($T_A = 0$ to $70\text{ }^{\circ}\text{C}$, $V_{DD} = 5\text{V} \pm 5\%$, $V_{SS} = 0\text{V}$)

Symbol	Parameter	Test Conditions	Limits		Units
			Min.	Max.	
I_{LH}	Input leakage current high	$V_{IN} = V_{DD}$		10	μA
I_{LL}	Input leakage current low	$V_{IN} = 0\text{V}$		-10	μA
I_{LR}	Input leakage current on $\overline{\text{RESET}}$ pin	$V_{IN} = 0\text{V}$		-100	μA
I_{LOH}	Output leakage current high	$V_{OUT} = V_{DD}$		10	μA
I_{LOL}	Output leakage current low	$V_{OUT} = 0\text{V}$		-10	μA
V_{IH}	Input voltage high		2.0	$V_{DD} + 0.3$	V
V_{IL}	Input voltage low		-0.5	0.8	V
V_{OH}	Output voltage high	$I_{OH} = -400\text{ }\mu\text{A}$	2.4		V
V_{OL}	Output voltage low	$I_{OL} = 2.0\text{ mA}$		0.4	V
	Supply current average operating	HSC freq. = 15 MHz		10	mA
	Supply current peak operating	HSC freq. = 15 MHz		35	mA
	Supply current standby	$\overline{\text{CS}}$ high		10	mA

CAPACITANCE ($T_A = 25\text{ }^{\circ}\text{C}$, $V_{DD} = 5\text{V} \pm 5\%$, $V_{SS} = 0\text{V}$)

Symbol	Parameter	Test Conditions	Limits		Units
			Min.	Max.	
C_{IN}	Input capacitance	Unmeasured pins		7	pF
C_{OUT}	I/O capacitance	Returned to V_{SS}		10	pF

RECOMMENDED OPERATING CONDITIONS

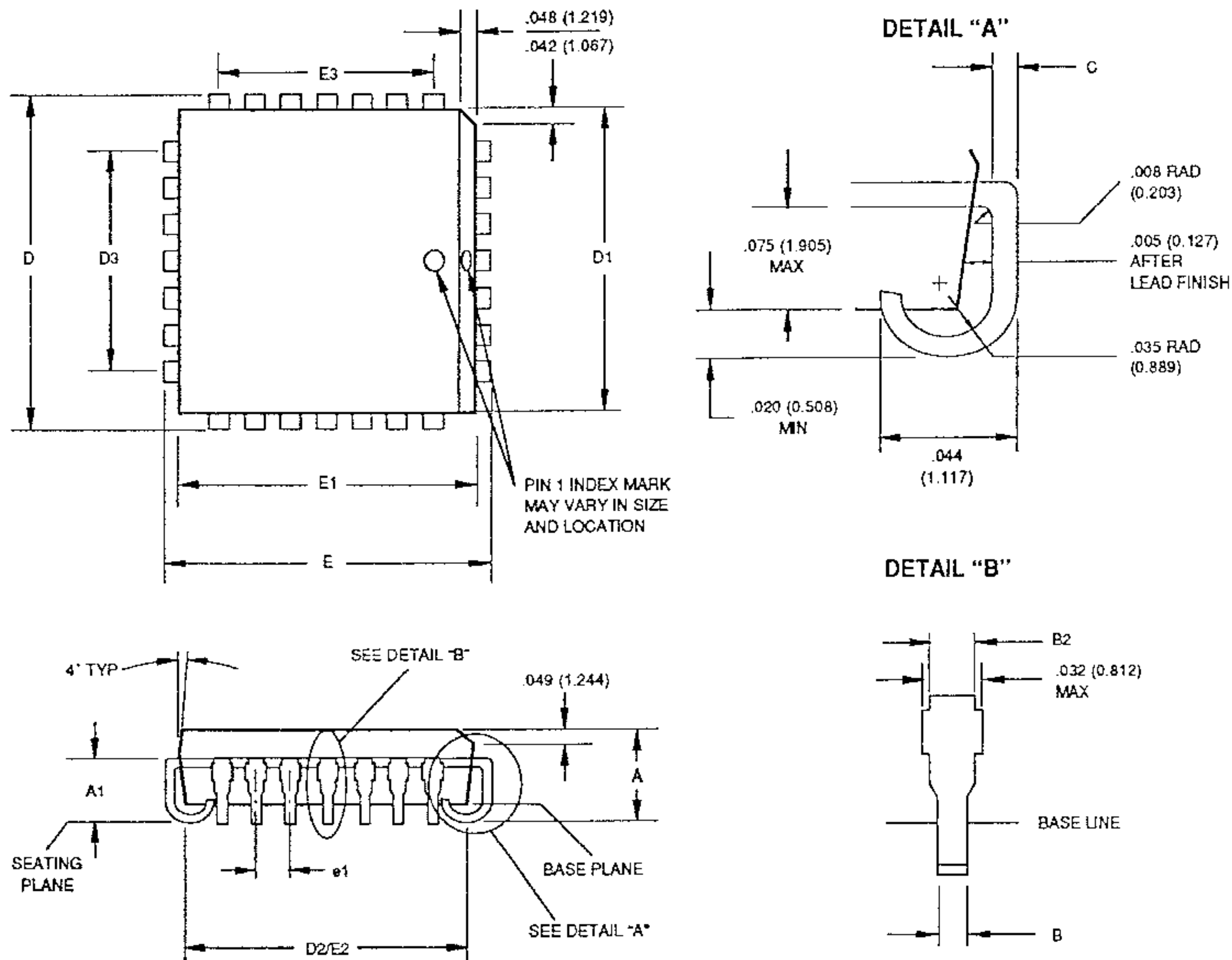
DC Supply Voltage		+4V to +6V
Operating Temperature Range	Commercial	0 to $70\text{ }^{\circ}\text{C}$
	Industrial	-40 to $+85\text{ }^{\circ}\text{C}$

ABSOLUTE MAXIMUM RATINGS

Power Supply Voltage (V_{DD})	-0.5 to +7.0V
Power Dissipation ($P_{D_{MAX}}$)	1 Watt
Operating Temperature (T_{OPT})	See operating temperature ranges
Storage Temperature	-65 to $+150\text{ }^{\circ}\text{C}$

Stress beyond those listed above may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to maximum rating conditions for extended periods may affect device reliability.

PLASTIC LEADED CHIP CARRIER (PLCC)



Theta JA (5) (°C/Watt)	45
VLSI Doc. No.	25-60001

Symbol		A	A1	B	B2	C	D	D1	D2	D3
Dimension in (mm)	MIN	.165 (4.19)	.090 (2.29)	.013 (.330)	.026 (.660)	.008 (.203)	.485 (12.32)	.450 (11.43)	.390 (9.91)	.300 (7.62) Ref
	MAX	.180 (4.57)	.120 (3.05)	.021 (.553)	.032 (.813)	.010 (.254)	.495 (12.57)	.495 (11.58)	.430 (10.92)	
Symbol		E	E1	E2	E3	e1	N	ND	NE	
Dimension in (mm)	MIN	.485 (12.32)	.450 (11.43)	.390 (9.91)	.300 (7.62) Ref	.050 (1.27) Typ	28	7	7	
	MAX	.495 (12.57)	.456 (11.58)	.430 (10.92)						