VLSI TECHNOLOGY, INC.

ADVANCE INFORMATION
VM009

HIGH-SPEED DES DEVICE

FEATURES

- Supports three ciphering operations:
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
- Three data ports
  - Master Port
  - Slave Port
  - Auxiliary Port
- Class 3 ESD (Electro-Static Discharge) protection (greater than 4000V)
- Up to 33 MHz operation
- Validation by National Institute of Standards and Technology (NIST) Pending
- 40-lead plastic dual in-line or 44-lead plastic leaded chip carrier
- 1.0-micron CMOS technology; ensuring highly reliable operation

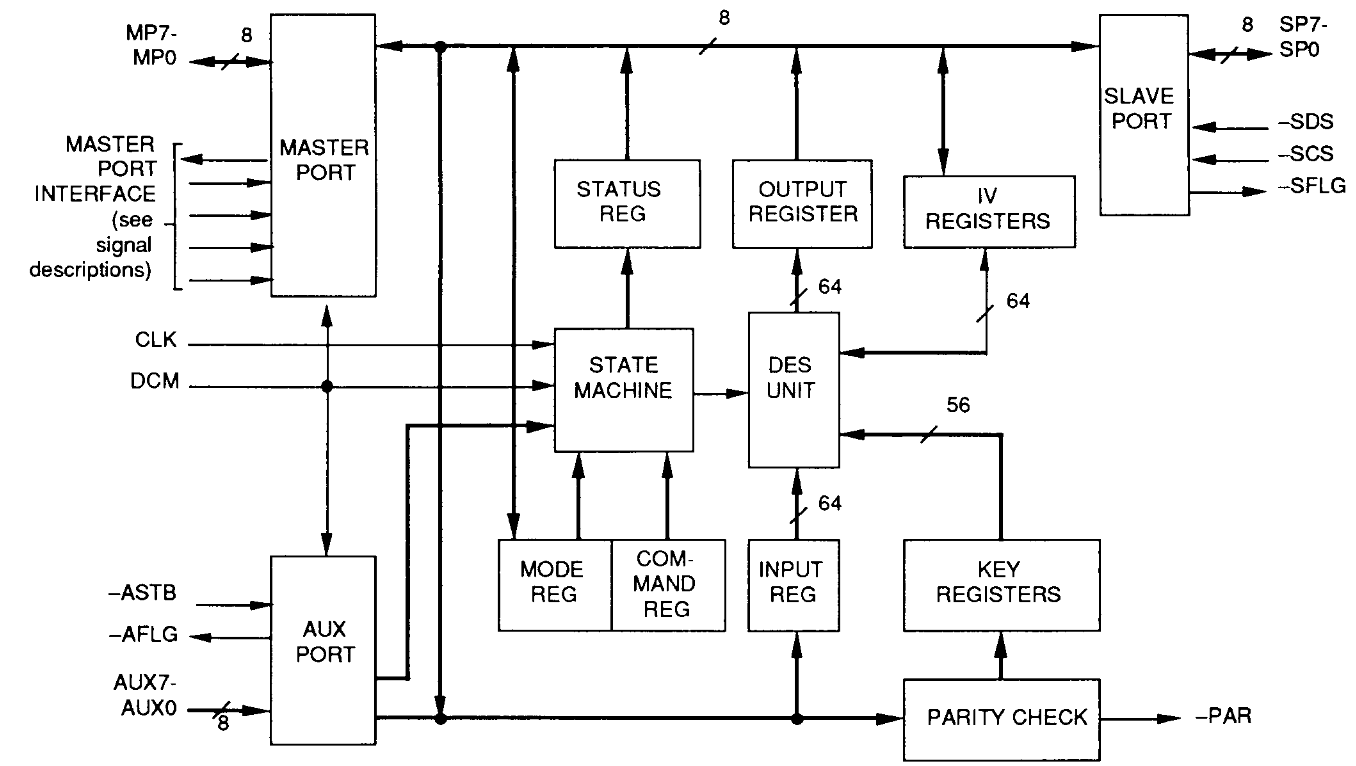
DESCRIPTION

The VM009 High-Speed DES Device supports the Data Encryption Standard (DES) algorithm as described in FIPS PUB 46-1 published by the National Bureau of Standards. A high throughput rate is achieved in either Electronic Codebook, Cipher Block Chaining, or Cipher Feedback modes of operation. Separate ports for plain-text, cipher-text, and key input enhance security and functionality.

The system communicates with the VM009 via port control lines and/or by commands entered through the Master Port. Once set up, data can flow through the VM009 at high speeds because input, output, and ciphering activities are all performed concurrently. External DMA control can easily be used to enhance throughput in some system configurations.

The VM009 is manufactured using VLSI's 1.0-micron CMOS technology and is available in either a 40-pin plastic dual in-line package or 44-pin plastic leaded chip carrier. All inputs and outputs are TTL compatible.

BLOCK DIAGRAM



ORDER INFORMATION

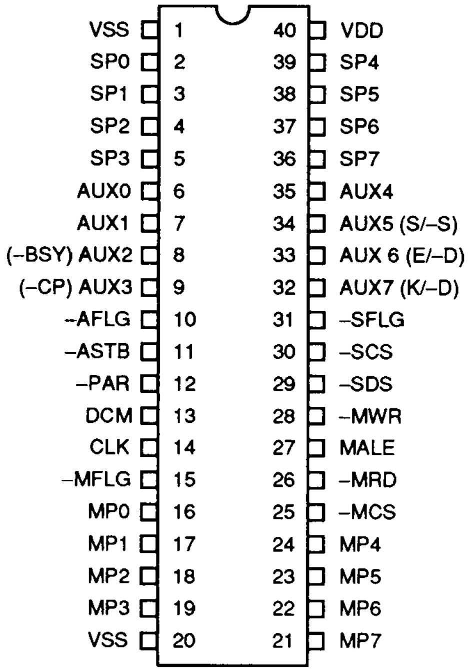
Part Number	Operating Temperature Range (TA)	Package	Bus Interface
VM009 -A-80	0°C to +85°C	40-pin Plastic Dual In-line Package	Strobed Address Enable
VM009 -A-86	0°C to +85°C	40-pin Plastic Dual In-line Package	Latched Address Enable
VM009 -B	0°C to +85°C	44-pin Plastic Leaded Chip Carrier	User Selectable Address Enable

March 1992

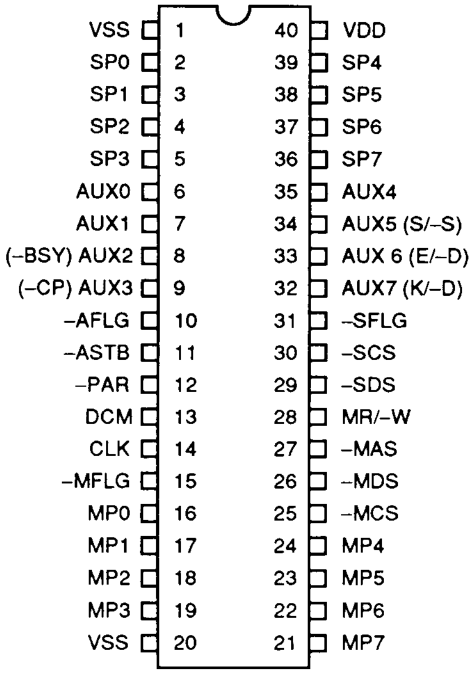
VLSI Technology, Inc. • 8375 South River Parkway • Tempe, AZ 85284 • 602-752-8574

PIN DIAGRAM:
(Plastic Dual-In Line)

VM009-A-86

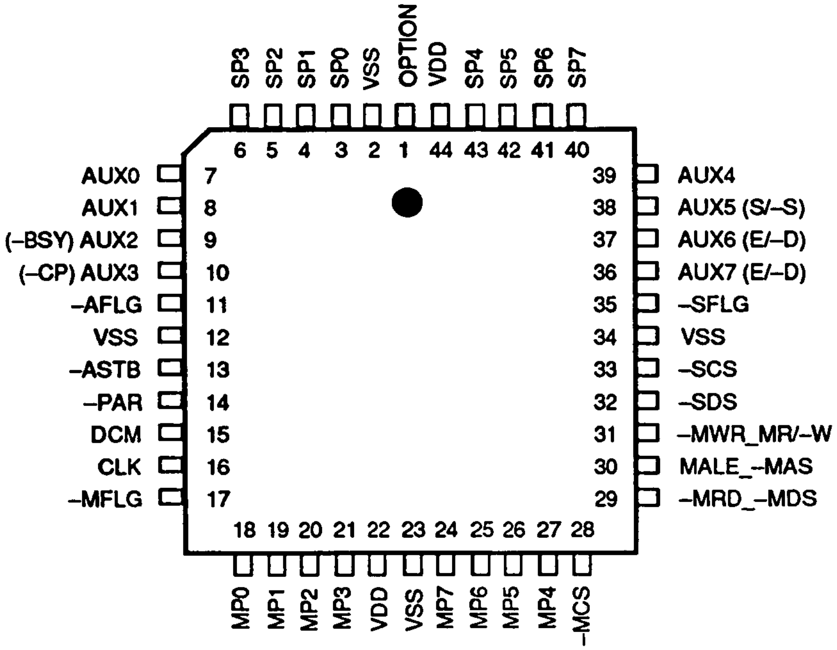


VM009-A-80



PIN DIAGRAM:
(Plastic Leaded Chip Carrier)

VM009-B



SIGNAL DESCRIPTIONS

Signal Name	40-Pin Number	44-Pin Number	Signal Type	Signal Description
SYSTEM INTERFACE				
CLK	14	16	I	Clock - An external timing source is input via the CLK pin. The Master and Slave Port Data Strobe signals must change synchronously with this clock input. In Direct Control Mode S/S must also be synchronous. In addition, the Auxiliary, Master and Slave Port Flag outputs) will change synchronously with the clock.
DCM	13	15	I	Direct Control Mode - Controls the operation of the VM009. The VM009 is placed into Multiplexed Control Mode when a low input is placed on DCM, enabling programmed access to internal registers through the Master Port and enabling input of keys through the Auxiliary Port. A high input on DCM specifies operation in Direct Control Mode. In Direct Control Mode, several of the Auxiliary Port pins become direct control/status signals which can be driven/sensed by high-speed controller logic, and access to internal registers through the Master Port is limited to the input or output register.
OPTION	N/A	1	I	OPTION (available only in the VM009-B version) - allows the user to modify the behavior of the Master Port Control interface. This modification optimizes the device for use with either the Strobed Address Enable or the Latched Address Enable types of microprocessors. When the OPTION pin is connected to VDD, the interface is optimized for the Strobed Address family. Tying the OPTION pin to VSS provides a Latched Address master port interface. The option pin must be tied to either VDD or VSS. If allowed to float, erratic operation of the VM009 will occur. The 40-lead DIP version of the VM009 is also available with either interface, but the configuration is fixed when the part is manufactured, and therefore cannot be changed.
MASTER PORT				
MP7-MP0	19-16, 21-24	21-18 24-27	I/O	Master Port Bus bits 7 through 0 - These bidirectional signals are used to input and output data, as well as to specify internal register addresses in the Multiplexed Control Mode. The Master Port provides software access to the Input, Output, Status, Command, and Mode Registers. For the VM009-A-86 interface, the three-state Master Port outputs are enabled only when the Master Port is selected by –MCS and when –MRD is strobed low. For the VM009-A-80 interface, the Master Port outputs are enabled only when selected by –MCS, and when MR/–W and –MDS are both low. Data and key information are entered into the Master Port, most significant byte first.
–MCS	25	28	I	Master Port Chip Select - This signal is used to select the Master Port. The level on –MCS is latched internally on the falling edge of MALE in the Multiplexed Control Mode. This latched level is sustained as long as MALE is low. The latch becomes transparent and the internal signal will follow the –MCS input, when MALE is high. No latching of –MCS occurs in Direct Control Mode. The level on –MCS is passed directly to the internal select circuitry regardless of the state of MALE.
MALE	27	30	I	(For VM009-A-86) Master Port Address Latch Enable - In Multiplexed Control Mode, an active high signal on this pin indicates the presence of valid address and chip select information at the Master Port. The information will be latched internally on the falling edge of MALE. In Direct Control Mode, MALE may be high or low without affecting the VM009's operation.
–MAS	27	30	I	(For VM009-A-80) Master Port Address Strobe - In Multiplexed Control Mode, an active LOW signal on this pin indicates the presence of valid address and chip select information at the Master Port. This information will be latched internally on the rising edge of –MAS. In Direct Control Mode, –MAS may be HIGH or LOW without affecting VM009 operation.

SIGNAL DESCRIPTIONS (Cont.)

Signal Name	40-Pin Number	44-Pin Number	Signal Type	Signal Description
				However, if both –MAS and –MDS are LOW simultaneously, the VM009 will be reset to ECB mode and all flags go inactive.
–MRD	26	29	I	(For VM009-A-86) Master Port Read (active low) - An input used in conjunction with a valid –MCS to indicate that data is to be placed on MP7-MP0 for an output operation. –MRD and –MWR are mutually exclusive; if both go low simultaneously, the VM009 is reset to ECB Mode and all flags go inactive.
–MDS	26	29	I	(For VM009-A-80) Master Port Data Strobe - This active LOW input is used in coincidence with a valid Master Port Chip Select (–MCS) to indicate that valid data is present on MP0-MP7 for an input operation or that data is to be placed on MP0-MP7 during output. –MDS and –MAS are mutually exclusive; if both go LOW simultaneously, the VM009 is reset to ECB mode and all flags go inactive.
–MWR	28	31	I	(For VM009-A-86) Master Port Write - This input signal indicates to the VM009 that valid data is present on MP7-MP0 for an input operation. The trailing edge of –MWR latches the data into the selected internal register. The VM009 is reset if –MWR and –MRD both go low simultaneously.
MR/–W	28	31	I	(For VM009-A-80) Master Port Read/Write - This input signal indicates to the VM009 whether the current Master Port operation is a read (HIGH) or a write (LOW), thereby indicating that data is to be transferred from or to an internal register, respectively. MR/–W is not latched internally and must be held stable while –MDS is LOW.
–MFLG	15	17	O	Master Port Flag - This flag indicates the need for a data transfer at the Master Port during a normal ciphering operation. The Master Port will be associated with either the Input Register or the Output Register, depending upon the control bits written to the Mode Register. If data is to be transferred through the Master Port to the Input Register, the –MFLG reflects the contents of the Input Register. After any START command is entered, –MFLG will go low whenever the Input Register is not full. –MFLG is forced high by any command other than a Start. If the Master Port is associated with the Output Register, –MFLG reflects the contents of the Output Register (except in Single Port configuration - see Detailed Description). –MFLG will go low whenever the Output Register is not empty. In Single Port Configuration, the Slave Port Flag (–SFLG, see below) is associated with the Output Register, while the Master Port Flag reflects the contents of the Input Register.
SLAVE PORT				
SP7-SP0	36-39 5-2	40-43 6-3	I/O	Slave Port Bus bits 7 through 0 - This bidirectional data bus provides a second input/output interface to the VM009. This allows overlapped input, output and ciphering operations. The three-state Slave Port outputs will be driven only when –SCS and –SDS are both low and –SFLG = 0, and the internal Port Control Configuration allows output to the Slave Port. Data entered or retrieved through this port is the most significant byte in/out first.
–SCS	30	33	I	Slave Port Chip Select - This input is logically combined with –SDS to ease Slave Port data transfers in a bus environment. –SCS is not latched internally, and may be tied permanently low without impairing Slave Port operation.
–SDS	29	32	I	Slave Port Data Strobe - In conjunction with –SCS low, indicates to the VM009 that data is to be driven onto SP7-SP0 for output, or that valid data is on SP7-SP0 for an input operation. The control bits in the Mode Register determine the direction of Data flow.

SIGNAL DESCRIPTIONS (Cont.)

Signal Name	40-Pin Number	44-Pin Number	Signal Type	Signal Description
–SFLG	31	35	O	Slave Port Flag) - This output indicates the state of either the Output Register or the Input Register, depending on control bits set in the Mode Register. In Dual Port Configuration, –SFLG will reflect the content of whichever register is associated with the Slave Port. In Single Port Configuration, –SFLG will go LOW whenever the Output Register is not empty during normal processing. If the Input Register is assigned to the Slave Port, –SFLG will go LOW whenever the Input Register is not full, once any of the Start commands has been entered. –SFLG will be forced inactive if any other command is entered. If the Slave Port is assigned to the Output Register, –SFLG will go LOW whenever the Output Register is not empty.
AUXILIARY PORT				
AUX7-AUX0	6-9, 32-35	7-10, 36-39	I/O	Auxiliary Port Bus bits 7 through 0 - When the VM009 is operated in Multiplexed Control Mode (DCM low), these eight bidirectional lines form a key-byte input port which may be used to enter the Master and Session Keys. This port is the only path available for entering the Master Key (session keys may alternatively be entered via the Master Port.) AUX0 is the least significant bit and is considered to be the parity bit in key bytes. The most significant byte is entered first. When the VM009 is operated in Direct Control Mode, the Auxiliary Port's key-entry function is disabled and five of the eight lines become direct control/status lines for interfacing to high-speed controllers. In this case, AUX0, AUX1, and AUX4 have no function (they may be tied high).
AUX7(K/–D)	32	36	I	Auxiliary Port Bus bit 7; Key/Data - In Direct Control Mode, when this signal goes high, the VM009 begins a key-data input sequence as if a Load Clear Key Through Master Port command had been entered. The level on E/–D will determine whether the subsequently entered clear-key bytes are written into the D Key Register (E/–D low) or the E Key Register (E/–D high). K/–D and S/–S are mutually exclusive control lines. When one goes high, the other must be low until the first returns to low. Also, both lines must be low whenever a transition occurs on DCM (entering or exiting Direct Control Mode).
AUX6(E/–D)	33	37	I	Auxiliary Port Bus bit 6; Encrypt/Decrypt - In Direct Control Mode, when S/–S goes high, producing a normal data ciphering operation, this input specifies whether the ciphering algorithm is to encrypt (E/–D high) or decrypt (E/–D low). When K/–D goes high, initiating entry of key bytes, the level on E/–D stipulates whether the bytes are to be written into the D Key Register (E/–D low) or the E Key Register (E/–D high). The E/–D input is not latched internally, and must be held constant whenever one or more of S/–S, K/–D, –BSY, or –CP are active. Scrambled data in the internal registers will result after failure to maintain the proper level on E/–D during loading or ciphering operations.
AUX5(S/–S)	34	38	I	Auxiliary Port Bus bit 5; Start/Stop - In Direct Control Mode, when this pin goes low (–Stop), the VM009 will follow the sequence that would normally occur when a Stop command is entered. However, when this pin goes high, a sequence equal to a Start Encryption or Start Decryption command will be followed. At the time S/–S goes high, the level on E/–D selects either the Start Encryption or Start Decryption process.
AUX2(–BSY)	8	9	O	Auxiliary Port Bus bit 2; Busy - In Direct Control Mode, this status output gives a hardware indication that the ciphering algorithm is in operation. –BSY is driven by the BSY bit in the Status Register. When the BSY bit is "1", –BSY is low.

SIGNAL DESCRIPTIONS (Cont.)

Signal Name	40-Pin Number	44-Pin Number	Signal Type	Signal Description
AUX3(–CP)	9	10	O	Auxiliary Port Bus bit 3; Command Pending - In Direct Control Mode, this active low status output gives a hardware indication that the VM009 is ready to accept input of key bytes following a low-to-high transition on K/–D. –CP is driven by the CP bit in the Status Register, such that when the CP bit is "1", –CP is low.
–ASTB	11	13	I	Auxiliary Port Strobe - The rising edge of –ASTB strobes the key data on pins AUX7-AUX0 into the suitable internal key register in Multiplexed Control Mode. This input is ignored unless –AFLG and DCM are both low. One byte of key data is entered on each –ASTB; most significant byte first.
–AFLG	10	11	O	Auxiliary Port Flag - This output signal indicates that the VM009 is expecting key data to be entered on pins AUX7-AUX0. This can occur only when DCM is low and a Load Key Through AUX Port command has been entered. During input of all eight bytes, –AFLG will remain low and will go high with the leading edge of the eighth –ASTB.
–PAR	12	14	O	Parity - The VM009 checks all the key bytes for odd parity as they enter through either the Master Port (Multiplexed or Direct Control Mode) or the Auxiliary Port (Multiplexed Control Mode only). If any key byte contains even parity, the PAR bit in the Status Register is set to "1" and –PAR goes low. (See Parity Checking of Keys). The least significant bit of key data is the parity.
POWER & GROUND PINS				
VDD	40	22, 44	PWR	Power Connection - +5 volts
VSS	1, 20	2, 12, 23, 34	GND	Ground Connection - 0 volts

SIGNAL LEGEND

Signal Code	Signal Type
I	Input
O	Output
I/O	Input/Output (bidirectional)
GND	Ground
PWR	Power

FUNCTIONAL DESCRIPTION

The design of the VM009 is optimized for high data throughput. Cryptographic key bytes can be written through both the Master and Auxiliary Ports. Data bytes can be transferred through both the Master and Slave Ports. Three 56-bit, write-only key registers are provided for the Master (M) Key, the Encryption (E) Key and the Decryption (D) Key. Parity checking is provided on incoming keys. Two 64-bit registers are provided for the Initial Vectors (IVE and IVD) required during feedback ciphering modes. Three 8-bit registers (Mode, Command and Status), are available through the Master Port for interfacing to a host microprocessor.

ALGORITHM PROCESSING

The VM009's Algorithm Processing Unit is designed to encrypt and decrypt data according to the National Bureau of Standards Date Encryption Standard (DES), as specified in Federal Information Processing Standards Publication (FIPS-PUB) 46-1.

The DES algorithm specifies a method for encrypting 64-bit blocks of plain-text into corresponding 64-bit blocks of cipher-text. The VM009 offers three ciphering methods which are selected by the Cipher Type field of the Mode Register: Electronic Code Book (ECB), Cipher Block Chain (CBC) and Cipher Feedback (CFB). These methods are implemented in accordance with FIPS-PUB 81. Electronic Code Book (ECB) is a straightforward implementation of the DES: 64 bits of plain-text in, 64 bits of cipher-text out, with no cryptographic reliance between blocks. Cipher Block Chain (CBC) also operates on blocks of 64 bits, but includes a feedback step which chains consecutive blocks so that duplicate data in the plain text (such as ASCII blanks) does not yield duplicate cipher text. CBC also provides an error extension characteristic valuable in protecting against false data insertions and deletions. Cipher Feedback (CFB) is an additive stream cipher method in which the DES generates a pseudorandom binary stream which is then exclusive-OR'd with the plain-text to form the cipher-text. The cipher text is then fed back to form a portion of the next DES input block. The VM009 implements 8-bit cipher feedback with one byte wide data input, output, and feedback paths. This method is useful for low speed, character-at-a-time serial communications.

MULTIPLE KEY REGISTERS

The VM009 provides the registers necessary to implement a multiple-key system. In such an arrangement, a single Master Key, stored in the VM009 M Key Register, is only used to encrypt session keys for transmission to remote DES equipment, and to decrypt session keys received from such equipment. The M Key Register may only be loaded through the Auxiliary Port.

In addition to the M Key Register, the VM009 contains two session key registers: the E Key Register, used to encrypt plain-text and the D Key Register, used to decrypt cipher-text.

All three registers are loaded by writing commands through the Master Port into the Command Register, and then writing the eight bytes of key data to the port when the Command Pending bit = "1" in the Status Register.

MULTIPLEXED VS. DIRECT CONTROL

The VM009 can be operated in either of two basic interfacing modes determined by the logic level on the DCM input pin. In Multiplexed Control Mode (DCM LOW), the VM009 is configured internally to allow a host CPU to directly address five of the internal Control/ Status/Data Registers thus controlling the device via mode and command values written to these registers. Also, in Multiplexed Control Mode, the Auxiliary Port is enabled for key input.

If the logic level on DCM is brought HIGH, the VM009 enters Direct Control Mode, and the Auxiliary Port pins are transformed into direct hardware status or control signals which can instruct the VM009 to perform a functional subset of its cipher processing at very high throughputs. This operating mode is especially suited for interfacing to high-speed peripheral devices.

INITIALIZATION

The VM009 can be reset in several ways:

1. By the "Software Reset" command
2. By a hardware reset, via appropriate assertion of the Master Port Control signals
3. By writing to the Mode Register
4. By aborting any command

All these sequences are the same internally, except that loading the Mode Register does not subsequently reset the Mode Register.

Once the reset process starts, the VM009 will not respond to further commands for approximately five clock cycles.

If a power-up hardware reset is used, the leading edge of the reset signal should not occur until approximately 1 ms after VCC has reached normal operating voltage. This delay time is necessary for internal signals to stabilize.

MASTER PORT READ/WRITE TIMING

The VM009's Master Port is designed to operate with multiplexed address-data buses. The Master Port can be optimized to interface with either an Strobed or Latched Address Enable microprocessor. For the 44-lead PLCC, the user may select the preferred interface by connecting the OPTION pin to either VDD or VSS. For the 40-lead DIP, the interface type must be chosen when the device is ordered.

The VM009-A-86 interface operates as follows.

The level on Master Port Chip Select (–MCS) is latched internally on the falling edge of MALE. This relieves the external address decode circuitry of the responsibility for latching chip select at address time.

The levels on MP1, MP2 are also latched internally on the falling edge of MALE and are then decoded to enable reading and writing of the VM009's internal registers (Mode, Command, Status, Input and Output). Again, eliminating the need for external address latching and decoding.

Data transfers through the Master Port are controlled by –MRD and –MWR. The transfers do not interfere with either the chip-select or address latches. Once the VM009 and a particular register have been selected, any number of reads or writes of that register can be accomplished without intervening address cycles. This feature speeds up loading keys and data, given the necessary transfer control external to the VM009.

The VM009-A-80 interface operates in a similar fashion except for the following:

- The level on –MCS is latched internally on the rising edge of –MAS.
- The leveles on MP1 and MP2 are also latched on the rising edge of –MAS and are subsequently decoded to enable reading and writing of the internal registers. (Mode, Command, Status, Input, and Output)
- Data transfers through the Master Port are controlled by –MDS and MR/–W. Data transfers do not disturb either the chip select or address latches. This allows any number of transfers to occur without intervening address cycles once the VM009 and a particular register have been selected.

LOADING KEY AND INITIAL VECTOR (IV) REGISTERS

Because the key and initial vector registers are not directly addressable through any of the VM009's ports, keys and initial vectors must be loaded via command sequences.

In Direct Control Mode, only the E Key and D Key registers can be loaded. The M Key and IV Registers are inaccessible in Direct Control Mode. Loading the E and D Key registers is done by asserting the proper state on the E/–D input (HIGH for E Key, LOW for D Key) and then raising the K/–D input. This indicates that key loading is required. The command processor will attach the proper Key Register to the Master Port and assert the –CP signal. The eight key bytes may then be written to the Master Port. All key and vector registers can be written in Multiplexed Control mode, and all but the Master (M) Key Register may be loaded with encrypted or clear data. If the operation is a Load Encrypted command, the subsequent data written to the Master or Auxiliary Port is routed first to the Input Register and decrypted before being written into the specified Key or Vector Register.

PARITY CHECKING OF KEYS

Key bytes are considered to contain seven bits of key information and one parity bit. By DES designation, the low-order bit is the parity bit. The parity checking circuit is enabled whenever a byte is written to one of three Key Registers. The output of the parity detection circuit is connected to pin –PAR, and the state of this pin is reflected in Status Register bit Par. Whenever a byte with even parity is detected, Status Register bit PAR goes to "1". In addition to the PAR bit, the Status Register has a Latched Parity Bit which is set to "1" whenever the Status Register PAR bit goes to "1". Once it is set, the LPAR bit is not cleared until a reset occurs or a new Load Key command is issued.

When an encrypted key is entered, the parity detect logic operates only after the decrypted key is available. The encrypted data is not checked for parity. The –PAR signal will reflect the state of the decrypted bytes on a byte-to-byte basis, as they are clocked through the parity check logic on their way to the Key Register. So, the time –PAR indicates the status of a byte of decrypted key data may be as short as four clock cycles. The LPAR bit in the Status Register will indicate if any erroneous bytes of data were entered.

DATA FLOW

Bits M2 and M3 of the Mode Register control the flow of data into and out of the VM009 through the Master and Slave Ports. Three basic configurations are provided: one Single Port and two Dual Port configurations.

SINGLE PORT CONFIGURATION

Only when the Mode Register configuration bits are set to Master Port does the simplest configuration occur where the Encrypt/Decrypt bit controls the processing of data. Data to be encrypted or decrypted is written to the Master Port Input Register address. To facilitate monitoring of the Input Register status, the –MFLG signal goes LOW when the Input Register is not full. Data is read by the host CPU through the Master Port Output Register address. –SFLG goes LOW when the Output Register is not empty. Thus, –MFLG is redefined as a Master Input Flag and –SFLG is redefined as a Master Output Flag.

DUAL PORT, MASTER PORT CLEAR CONFIGURATION

Both the Master and Slave Ports are used for data entry and exit in the Dual Port configurations. Plain-text for encryption can only be entered through the Master Port in the Master Port Clear configuration. Plain-text resulting from decryption can only be read out through the Master Port and cipher-text can only be handled through the Slave Port. The direction of data flow is controlled by either the Encrypt/Decrypt bit in the Mode Register or by the Start Encryption or Start Decryption commands. If encryption is specified, plain-text will flow through the Master Port to the Input Register, and cipher-text will be available at the Slave Port when the Output Register is ready. For decryption, the process is reversed: cipher-text being written to the Input Register through the Slave Port and plain-text being read from the Output Register through the Master Port.

DUAL PORT, SLAVE PORT CLEAR CONFIGURATION

This configuration is exactly like the Dual Port, Master Port Clear configuration, except that the direction of ciphering is reversed. That is, all data flowing in or out of the Master Port is cipher-text, and all data at the Slave Port is plain-text.

REGISTER DESCRIPTION

Figure 1 shows the registers in the VM009 which can be directly addressed through the Master Port. Following is a brief description of these registers and others not directly accessible.

INPUT REGISTER

The 64-bit, write-only Input Register is setup to appear to the user as eight bytes of push down storage. The number of bytes that have been stored is monitored. The register is considered empty when the data stored in it has been or is being processed, and is considered full when one byte of data has been entered for Cipher Feedback Mode or when eight bytes of data have been entered for the Electronic Code Book or Cipher Block Chain Mode. If attempts are made to write data into the Input Register when it is full, the Input Register will disregard the attempt but no data in the register will be destroyed.

OUTPUT REGISTER

The 64-bit, read-only Output Register is organized to appear as eight bytes of pop-up storage. The register is considered empty when all the data stored in it has been read out by the host CPU, and is considered full if it still contains one or more bytes of output data. If attempts are made to read data from the Output Register when it is empty, the buffers driving the output bus will remain in a three-state condition.

M, E, D, KEY REGISTERS

There are three 64-bit write-only key registers in the VM009: the Master Key Register, the Encrypt Key Register, and the Decrypt (D) Key Register. The Master Key can only be loaded through the Auxiliary Port. The Encrypt and Decrypt Keys can be loaded, as plain-text or cipher-text, through the Auxiliary Port or Master Port. Cipher-text is first routed to the Input Register where it is decrypted using the M Key and then written to the target key register from the Output Register.

INITIAL VECTOR REGISTERS

To store feedback values for Cipher Feedback and Block Chained ciphering modes, two 64-bit registers are provided. One Initial Vector (IVE) Register is used during encryption; the other (IVD), during decryption. Both registers can be loaded with either plain or cipher-text through the Master Port and both may be read out as either plain or cipher through the Master Port.

FIGURE 1. MASTER PORT REGISTER ADDRESSES

VM009-A-86:

DCM	MP2	MP1	–MRD	–MWR	–MCS	Register Addressed
0	x	0	1	0	0	Input Register
0	x	0	0	1	0	Output Register
0	0	1	1	0	0	Command Register
0	0	1	0	1	0	Status Register
0	1	1	x	x	0	Mode Register
x	x	x	x	x	1	No Register Accessed
1	x	x	1	0	0	Input Register
1	x	x	0	1	0	Output Register

VM009-A-80:

DCM	MP2	MP1	MR/–W	–MCS	Register Addressed
0	x	0	0	0	Input Register
0	x	0	1	0	Output Register
0	0	1	0	0	Command Register
0	0	1	1	0	Status Register
0	1	1	x	0	Mode Register
x	x	x	x	1	No Register Accessed
1	x	x	0	0	Input Register
1	x	x	1	0	Output Register

STATUS REGISTER

Figure 2 shows the bit assignments in the read-only Status Register. In each case, the output signal will be active LOW when the corresponding status bit is a "1". The Parity bit indicates the parity of the most recently entered key byte. On the other hand, the LPAR bit indicates whether any key byte with even parity has been encountered since the last Reset or Load Key command.

The "Busy" bit will be a "1" whenever the ciphering algorithm unit is actively encrypting or decrypting data. The "Busy" bit will remain a "1" even after ciphering is complete if the ciphered data cannot be transferred to the Output Register because that register still holds output from a previous ciphering cycle. "Busy" will be "0" at all other times, including times when no ciphering is possible because no data has been written to the Input Register.

The "Command Pending" bit will be Set to "1" by any command whose execution requires the transfer of data to or from a non-addressable internal register, such as when writing key bytes to the E Key Register or reading bytes from the IVE Register. "Command Pending" will be set following all commands except the three Start commands, the Stop command and the Software Reset command. "Command Pending" will return to "0" after all eight bytes have been transferred following a Load Clear, Read Clear or Read Encrypted command, and after data has been transferred, decrypted and loaded into the desired register following Load Encrypted commands.

The "Start/Stop" bit is set to "1" when one of the Start commands is entered and is reset to "0" when a reset occurs or when a new command other than a Start is entered.

MODE REGISTER

Figure 3 shows the Bit assignments in this 5-bit read/write register. The "Cipher Type" bits (M1, M0) indicate which ciphering mode (as defined in FIPS PUB 81) is to be used. On reset, the Cipher Type defaults to Electronic Code Book.

Configuration bits (M3, M2) indicate which data ports are to be associated with the Input and Output Registers and flags. When these bits are set to the Single Port, Master Only configuration (M3, M2 = 10), the Slave Port is disabled, and no manipulation of Slave Port Chip Select (–SCS) or Data Strobe (–SDS) can cause data movement through the Slave Port. All data transfers are accomplished through the Master Port. Both –MFLG and –SFLG are used in this configuration. –MFLG gives the status of the Input Register and –SFLG the Output Register.

FIGURE 2. STATUS REGISTER BIT ASSIGNMENTS

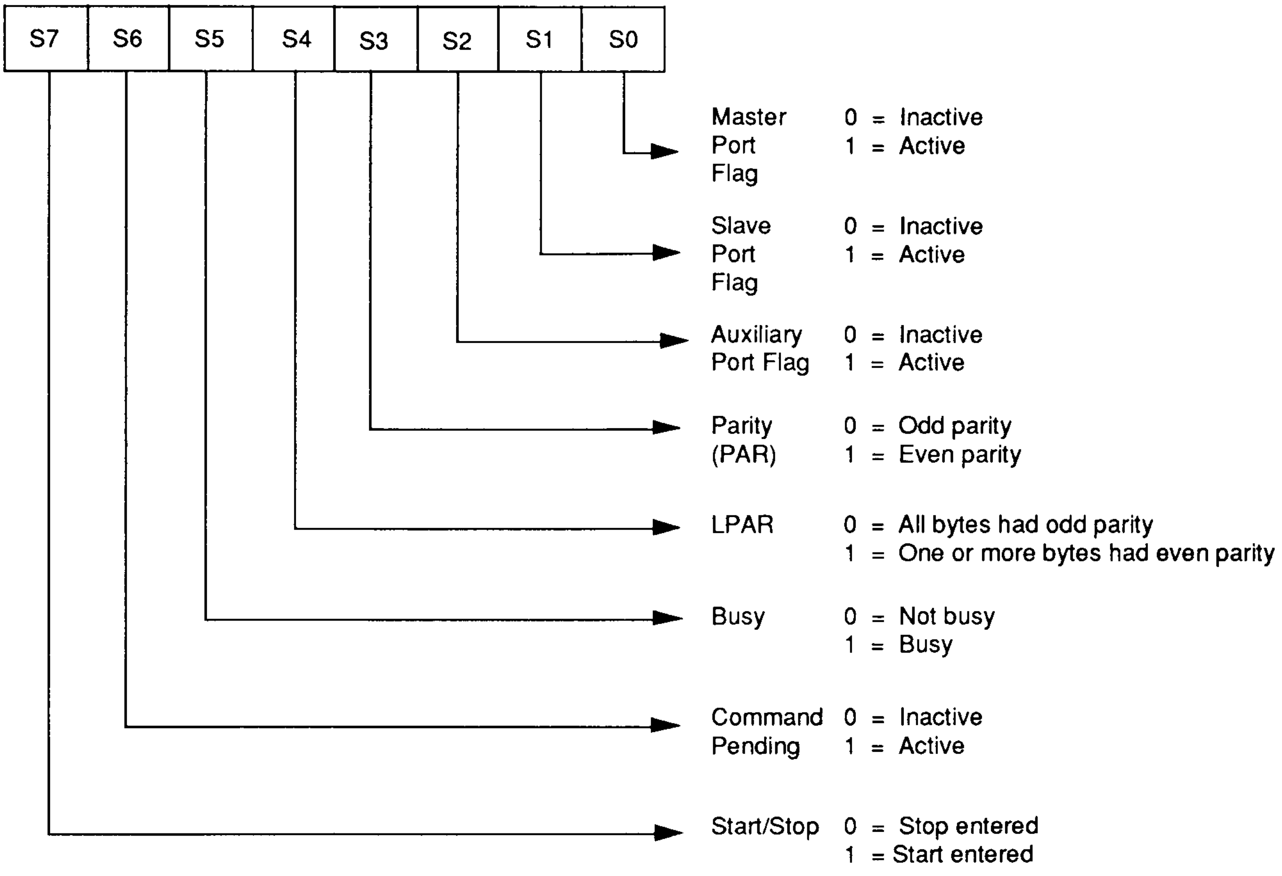
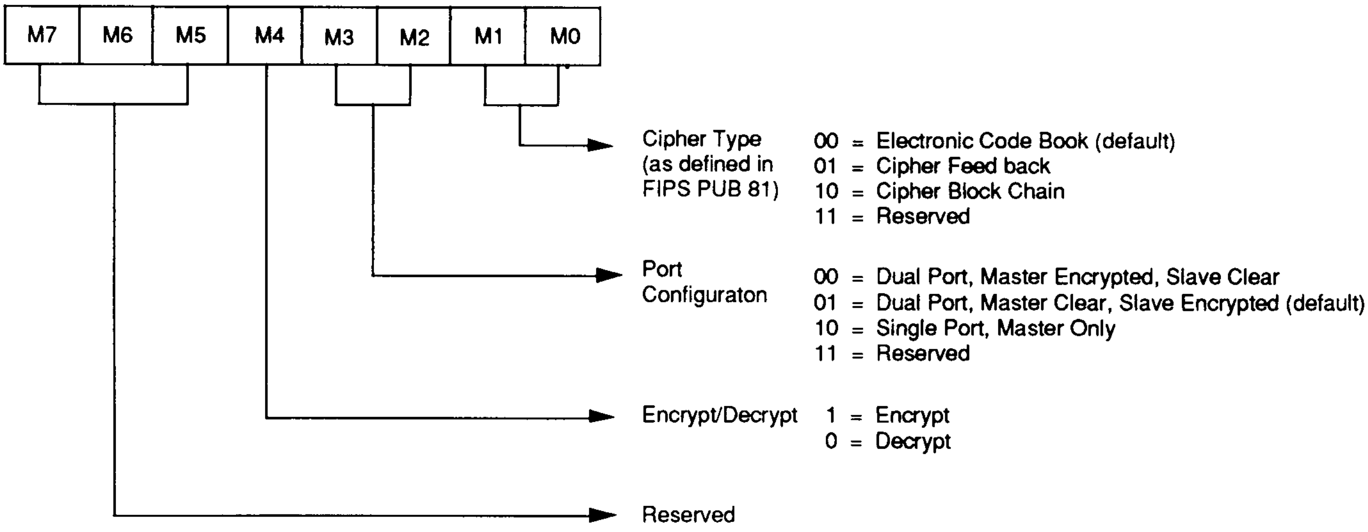


FIGURE 3. MODE REGISTER BIT ASSIGNMENTS


M7
M6
M5
M4
M3
M2
M1
M0
Cipher Type (as defined in FIPS PUB 81)
00 = Electronic Code Book (default)
01 = Cipher Feed back
10 = Cipher Block Chain
11 = Reserved
Port Configuraton
00 = Dual Port, Master Encrypted, Slave Clear
01 = Dual Port, Master Clear, Slave Encrypted (default)
10 = Single Port, Master Only
11 = Reserved
Encrypt/Decrypt
1 = Encrypt
0 = Decrypt
Reserved

When the Configuration Bits are set to one of the Dual Port configurations (M3, M2 = 00 or 01), both the Master and Slave Ports are available for input and output. When M3, M2 = 01 (the default configuration), the Master Port handles plain-text while the Slave Port handles cipher-text. Configuration M3, M2 = 00 reverses this assignment. Data direction at any particular moment is controlled by the Encrypt/Decrypt bit.

The Encrypt/Decrypt bit (M4) instructs the VM009 to encrypt or decrypt the data from the Input Register using the ciphering method specified by the Cipher Type bits. The Encrypt/Decrypt bit also controls data flow within the VM009.

COMMAND REGISTER

Data written to the 8-bit, write-only Command Register through the Master Port is interpreted as an instruction. A detailed description of each command is given under Commands. The commands and their binary representations are summarized in Figure 4.

FIGURE 4. IMPLICIT COMMAND SEQUENCES IN DIRECT CONTROL MODE

DCM	K/–D	E/–D	S/–S	Command Initiated
H	L	L	↑	Start Decryption
H	L	H	↑	Start Encryption
H	L	X	↓	Stop
H	↑	L	L	Load D Key Clear Through Master Port
H	↑	H	L	Load E Key Clear Through Master Port
H	↓	X	L	End Load Key Command
H	H	X	H	Not Allowed
L	Data	Data	Data	AUX Pins Become Key Inputs

COMMANDS

All operations of the VM009 result from command inputs. These command inputs are entered in Multiplexed Control Mode by writing a command byte to the Command Register. Command inputs are entered in Direct Control Mode by raising and lowering the logic levels on the K/–D, E/–D, and S/–S pins. Figure 4 shows the subset of commands executable in Direct Control Mode. All commands that may be given in Multiplexed Control Mode are shown in Figure 5.

Load Clear Key Through Auxiliary Port

These commands override the data flow specifications set in the Mode Register and cause the Master (M), Encrypt (E), or Decrypt (D) Key Register to be loaded with eight bytes written to the Auxiliary Port. When the Load command has been written to the Command Register, the Auxiliary Port Flag (–AFLG) will go LOW and the corresponding bit in the Status Register will go to "1", indicating that the device is able to accept key bytes at the Auxiliary Port pins. In addition, the Command Pending bit will go to "1" during the entire loading process.

Once data has been set up on the Auxiliary Port pins, each byte is written by placing a LOW signal on –ASTB. The actual write process occurs on the rising edge of –ASTB.

FIGURE 5. COMMAND CODES IN MULTIPLEXED CONTROL MODE

Hex Code	Register Addressed	Applicable Control Modes
90	Load Clear M Key Through Auxiliary Port	Direct & MUXed
91	Load Clear E Key Through Auxiliary Port	Direct & MUXed
92	Load Clear D Key Through Auxiliary Port	Direct & MUXed
11	Load Clear E Key Through Master Port	Direct & MUXed
12	Load Clear D Key Through Master Port	Direct & MUXed
B1	Load Encrypted E Key Through Auxiliary Port	MUXed Only
B2	Load Encrypted D Key Through Auxiliary Port	MUXed Only
31	Load Encrypted E Key Through Master Port	MUXed Only
32	Load Encrypted D Key Through Master Port	MUXed Only
85	Load Clear IVE Through Master Port	MUXed Only
84	Load Clear IVD Through Master Port	MUXed Only
A5	Load Encrypted IVE Through Master Port	Direct & MUXed
A4	Load Encrypted IVD Through Master Port	Direct & MUXed
8D	Read Clear IVE Through Master Port	MUXed Only
8C	Read Clear IVD Through Master Port	MUXed Only
A9	Read Encrypted IVE Through Master Port	MUXed Only
A8	Read Encrypted IVD Through Master Port	MUXed Only
39	Encrypt With Master Key	MUXed Only
41	Start Encryption	Direct & MUXed
40	Start Decryption	Direct & MUXed
C0	Start	Direct & MUXed
E0	Stop	Direct & MUXed
00	Software Reset	Direct & MUXed

–AFLG will go inactive right after the eighth strobe goes LOW. However, until the key loading process is completed, the Command Pending bit will remain "1". All key bytes are checked for odd parity as they are entered.

Load Clear Key Through Master Port

These commands override the data flow specifications set in the Mode Register and attach the Master port inputs to the Encrypt (E) or Decrypt (D) Key Register, as appropriate, until eight key bytes have been written. In Direct Control Mode, the command is initiated by raising the K/–D control input while the S/–S input is LOW. In this case, the level on E/–D determines which key register is written (HIGH = E Register). In Multiplexed Control Mode, the command is initiated by writing the Load command to the Command Register.

Once the command has been recognized, the Command Pending bit will go to "1", and in Direct Control Mode, –CP will go LOW, indicating that the user may begin key entry. The host system then writes eight bytes to the Master Port. When the key register has been loaded, the Command Pending bit will return to "0", and in Direct Control Mode, the –CP output will go to "1". The VM009 can now accept the next command.

Load Encrypted Key Through Auxiliary Port

Execution of these commands is similar to the Load Clear E (or D) Key Through Auxiliary Port, except that key bytes are first decrypted using Electronic Code Book mode and the Master (M) Key, and then loaded into the appropriate key register after having passed through the parity checking logic.

The Command Pending bit will be "1" during the entire decrypt-and-load operation, and the Busy bit) will be "1" during the actual decryption process.

Load Encrypted Key Through Master Port

These commands are similar in effect to Load Clear E (or D) Key Through Master Port, except that key bytes are initially decrypted using Electronic Code Book modes and the Master (M) Key, and then loaded byte-by-byte into the target key register after having passed through the parity checking logic.

Load Clear IV Register Through Master Port

These commands are virtually identical to Load Clear E (or D) Key Through Master Port except that no parity checking occurs and the data written to the Input Register address is routed to the IVE or IVD Register instead of a key register.

Load Encrypted IV Register Through Master Port

These commands are similar to the Load Encrypted E (or D) Key Through Master Port commands. The data flow specifications set in the Mode Register are overridden, and the eight vector bytes are decrypted using the Decryption (D) Key and the Electronic Code Cook mode. The resulting plain-text vector bytes are loaded into the target Initial Vector Register, and no parity checking occurs. The Command Pending will be "1" during the entire decryption-and-load operation but the Busy bit does not go to "1" during the decryption process.

Read Clear IV Register Through Master Port

These commands override the data flow specifications set in the Mode Register and connect the appropriate Initial Vector Register to the Master Port

FIGURE 6. ASSOCIATION OF MASTER PORT FLAG (–MFLG) AND SLAVE PORT

Encrypt/ Decrypt	Port Configuration		Input Register Flag	Output Register Flag
M4	M3	M2		
0	0	0	–MFLG	–SFLG
0	0	1	–SFLG	–MFLG
0	1	0	–MFLG	–SFLG
1	0	0	–SFLG	–MFLG
1	0	1	–MFLG	–SFLG
1	1	0	–MFLG	–SFLG

at the Output Register address. In this state, each IV Register appears as eight bytes of FIFO storage. The first byte of data will be available 6 clocks after the loading of the command register. The Command Pending bit will be set to "1" and will stay "1" until sometime after the eighth byte is read out. The host system is responsible for reading out exactly eight bytes.

Read Encrypted IV Register Through Master Port

These commands override the specifications set in the Mode Register and encrypt the contents of the Specified Initial Vector Register using Electronic Code Book Mode and the Encrypt (E) Key. The resulting cipher text is placed in the Output Register from which can then be read out as eight bytes through the Master Port. The Busy bit will be "1" during the actual encryption process. When Busy goes to "0", the encrypted vector bytes are ready to be read out. During the entire encryption-and-output process, the Command Pending bit will be "1", and will go to "0" when the eighth byte is read out. The host system is responsible for reading out exactly eight bytes.

Encrypt With Master Key

This command overrides the data flow specifications set in the Mode Register and causes the VM009 to accept eight bytes from the Master Port. These bytes are then written to the Input Register. When eight bytes have been received, the VM009 encrypts the input using the Master (M) Key. The ciphertext is loaded into the Output Register, where it may be read out through the Master Port. The Command Pending and Busy bits are used to sense the three phases of this operation. As soon as the Input Register can accept data, Command Pending goes to "1". When exactly eight bytes have been entered, the Busy bit will go to "1" until the Encryption process is complete.

When Busy goes to "0", the encrypted data is available to be read out. command Pending will return to "0" when the eighth byte has been read.

Start Encryption, Start Decryption, Start

These "Start" commands begin normal data ciphering by setting the Start/Stop bit in the Status Register to "1". The Start Encryption and Start Decryption commands clearly specify the ciphering direction by forcing the Encrypt/Decrypt bit in the Mode Register to "1" or "0", respectively. Whereas, Start uses the current state of the Encrypt/Decrypt bit, as specified in a previous Mode Register load.

When a Start command has been entered, the Port Status Flag (–MFLG or –SFLG) associated with the Input Register will go LOW, indicating that data may be written to the Input Register to begin ciphering.

In Direct Control Mode, the Start command is issued by raising the level on the S/–S input. The ciphering direction is specified by the level on E/–D. If E/–D is HIGH when S/–S goes HIGH, the command is Start Encryption, and if E/–D is LOW, it is Start Decryption.

Stop

In the Status Register, the Stop command clears the Start/Stop bit to "0" which causes the input flag (–MFLG or SFLG) to become inactive, thus inhibiting the loading of any further input into the DES Unit. If ciphering is in progress (Busy bit is "1" or –BSY is active), it will finish ciphering, and any data in the Output Register will remain accessible. In CFB Mode, the last byte of data must be read out before issuing the Stop command.

In Direct Control Mode, the Stop command is implied when the signal level on the S/–S input goes from HIGH to LOW).

Software Reset

This command acts like a hardware reset: it forces the VM009 back to its default configuration, and all processing flags go inactive. The default configuration includes setting the Mode Register to Electronic Code Book Mode and Dual Port Configuration with Master Port clear, slave port encrypted.

AC CHARACTERISTICS: TA = 0°C to +85°C, VDD = 5 V ±10%, VSS = 0 V

Symbol	Parameter	Min	Max	Unit	Conditions (See Note)
Clock					
tWH	Clock Width HIGH	15		ns	
tWL	Clock Width LOWS	15		ns	
tC	Clock HIGH to Next Clock HIGH	30		ns	
Reset					
tRESET	–MRD • –MWR LOW to –MRD • –MWR HIGH (Reset Pulse Width)	tC		ns	Note 12
Direct Control Mode					
tSS	S/–S LOW to DCM HIGH (Set-up)	3 tC		ns	Note 12
tUS	K/–D LOW to DCM' HIGH (Set-up)	3 tC		ns	Note 12
tCS	DCM HIGH to S/–S HIGH	6 tC		ns	Note 12
tCK	DCM HIGH to K/–D HIGH	6 tC		ns	Note 12
tEK	E/–D VALID to K/–D HIGH (Set-up)	3 tC		ns	Note 12
tKP	K/–D HIGH to –CP LOW		20	ns	
tKE	K/–D LOW to E/–D INVALID (Hold)	tC		ns	Note 12
tLS	Clock LOW to S/–S VALID	20	20	ns	
tES	E/–D VALID to S/–S HIGH (Set-up)	3 tC		ns	Note 12
tSFL	S/–S HIGH to –MFLG (–SFLG) LOW (Port Input Flag)		20	ns	Note 12
tCFI	Clock HIGH to –MFLG (–SFLG) LOW (Port Input Flag)		20	ns	Note 2
tCBL	Clock HIGH to –BSY LOW		20	ns	
tCBH	Clock LOW to –BSY HIGH		20	ns	
tCFO	Clock HIGH to –MFLG (–SFLG) LOW (Port Output Flag)		20	ns	
tSFH	S/–S LOW to –MFLG (–SFLG) HIGH (Port Input Flag)		20	ns	Note 3

Note: Direct control mode maximum values are estimated.

AC CHARACTERISTICS (Cont.): TA = 0°C to +85°C, VDD = 5 V ±10%, VSS = 0 V

Symbol	Parameter	Min	Max	Unit	Conditions
Multiplexed Control Mode - Master Port					
tMW	MALE Width (HIGH)	10		ns	
tMML	–MCS LOW to MALE LOW (Set-up)	5		ns	
tMMH	MALE LOW to –MCS HIGH (Hold)	5		ns	
tAS	Address INVALID to MALE LOW (Address Set-up Time)	5		ns	
tAH	MALE LOW to Address INVALID (Address Hold Time)	5		ns	
tRH	Read Data Hold Time		5	ns	
tRWH	Memory Read/Write Hold Time	5		ns	
tDSDA	Data Strobe LOW to Data Available		15	ns	
tDH	Data Hold Time		5	ns	
Master/Slave Port Read/Write					
tSELM	–MCS LOW to –MRD, –MWR LOW (Select Set-up)	5		ns	Note 4
tHM	–MRD, –MWR HIGH to –MCS HIGH (Select Hold)	5		ns	Note 4
tWID	–MRD, –MWR LOW to –MRD, –MWR HIGH Width - Write, Data Read Width - Status Register Read	 10 10		 ns ns	
	–SDS LOW to –SDS HIGH (Read, Write)	10		ns	
tCMH	–MRD, –MWR HIGH to Clock HIGH	3	tC - 1 ns	ns	Note 11
tCSH	–SDS HIGH to Clock HIGH	3	tC - 1 ns	ns	Note 11
tSRM	–MRD, –MWR HIGH to –MRD, –MWR LOW (Data Strobe Recovery Time)	0.5 tC		ns	
tSRS	–SDS HIGH to –SDS LOW (Data Strobe Recovery Time)	0.5 tC		ns	
tDS	Write Data VALID to –MWR (–SDS) HIGH Set-up Time - Key Load Set-up Time - Data Write Set-up Time - Command/Mode Register Write	 2 2 2		 ns	

AC CHARACTERISTICS (Cont.): TA = 0°C to +85°C, VDD = 5 V ±10%, VSS = 0 V

Symbol	Parameter	Min	Max	Unit	Conditions
Master/Slave Port Read/Write (Cont.)					
tHWM	–MWR HIGH to Write Data INVALID (Hold Time)	5		ns	
tHWS	–SDS HIGH to Write Data INVALID (Hold Time)	5		ns	
tRM	–MRD LOW to Read Data VALID Read Access Time - Data		14	ns	Assume 50 pf Load
tRS	–SDS LOW to Read Data VALID Read Access Time - Data	0	17	ns	Assume 50 pf Load
tRA	–MRD (–SDS) HIGH to Read Data INVALID (Hold Time)	0	5	ns	
tLSM	–MRD, –MWR LOW to –MFLG (–SFLG) HIGH (Last Strobe)		17	ns	Assume 50 pf Load
tLSS	–SDS LOW to –SFLG HIGH (Last Strobe)			ns	Not yet measured
tLSK	–MWR HIGH to –CP HIGH (Last Strobe - Key Load)			ns	Not yet measured
tMSL	–MRD, –MWR (–SDS) HIGH to S/–S LOW (Hold Time)	25	tLA + tWH +18 ns	ns	Assume 50 pf Load
tKW	–MWR HIGH to –PAR VALID (Key Write)		220	ns	
tRWL	MALE LOW to –MRD, –MWR HIGH	10		ns	
tMWR	–MRD, –MWR Pulse Width	0.5 tC		ns	

AC CHARACTERISTICS (Cont.): TA = 0°C to +85°C, VDD = 5 V ±10%, VSS = 0 V

Symbol	Parameter	Min	Max	Unit	Conditions
Auxiliary Port Key Entry					
tASW	–ASTB LOW to –ASTB HIGH (Width)	10		ns	
tLA	Clock LOW to –ASTB HIGH	3	tC - 1 ns	ns	
tRT	–ASTB HIGH to Next –ASTB HIGH	tLA + tWH		ns	
tADV	Write-Data VALID to –ASTB HIGH (Data Set-up Time)	2		ns	
tADH	–ASTB HIGH to Write-Data INVALID (Data Hold Time)	2		ns	
tAP	–ASTB HIGH to –PAR VALID		tLA + tWH + 18 ns	ns	Assume 50 pf Load
tAF	–ASTB LOW to –AFLG HIGH (Last Strobe)		12	ns	At 50 pf

Notes:
1. All input transition times assumed < 20 ns except clock which is < 10 ns.
2. Parameter 22 applies to all input blocks exept the first (when S/–S first goes HIGH).
3. When S/–S goes inactive (LOW) in Direct Control mode, the flag associated with the input port will turn off.
4. Direct Control Mode only.
5. In Cipher Feedback, the Port Flag (–MFLG or –SFLG) will go inactive following the leading edge of the first data strobe (–MRD, –MWR, or –SDS); in all other modes and operations, the flags go inactive on the eigth data strobe.
6. Do not remove K/–D until CP is inactive (HIGH).
7. Do not change E/–D until –MFLG (–SFLG) is inactive (HIGH).
8. In Cipher Feedback, –BSY must be inactive (HIGH) before S/–S goes inactive (LOW).
9. –AFLG must go active (LOW) before –ASTB goes inactive (LOW).
10. TWL is the clock width (LOW).
11. tC is the clock cycle time.

FIGURE 8. CLOCK AND RESET

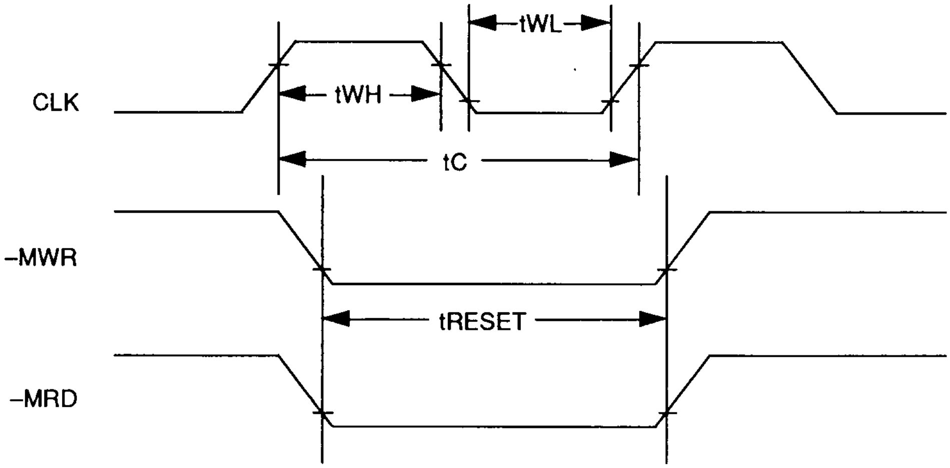


FIGURE 9. CONTROL AND STATUS SIGNALS (DIRECT CONTROL MODE)

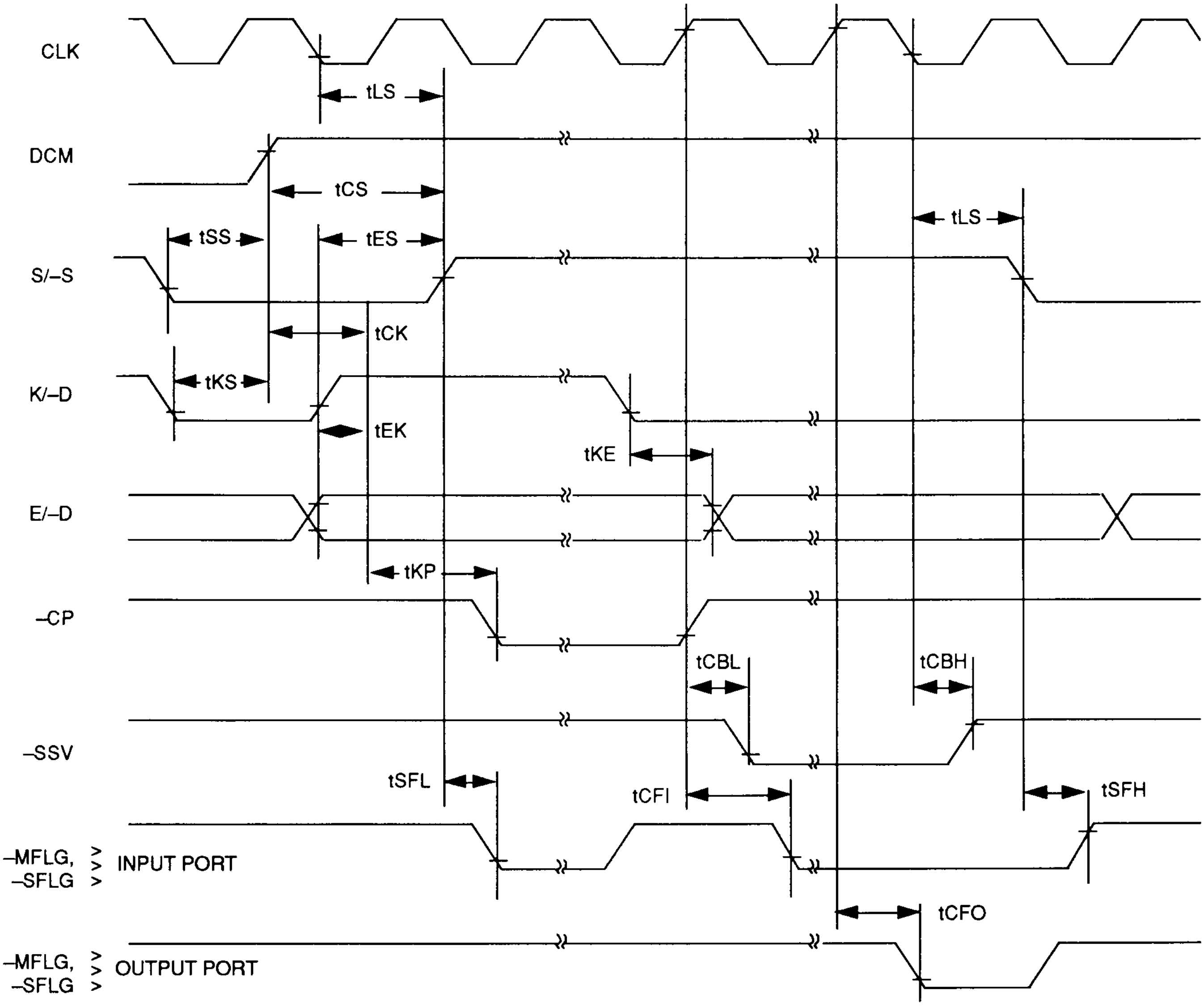


FIGURE 10. MASTER PORT, MULTIPLEXED CONTROL MODE READ/WRITE (VM009-A-86)

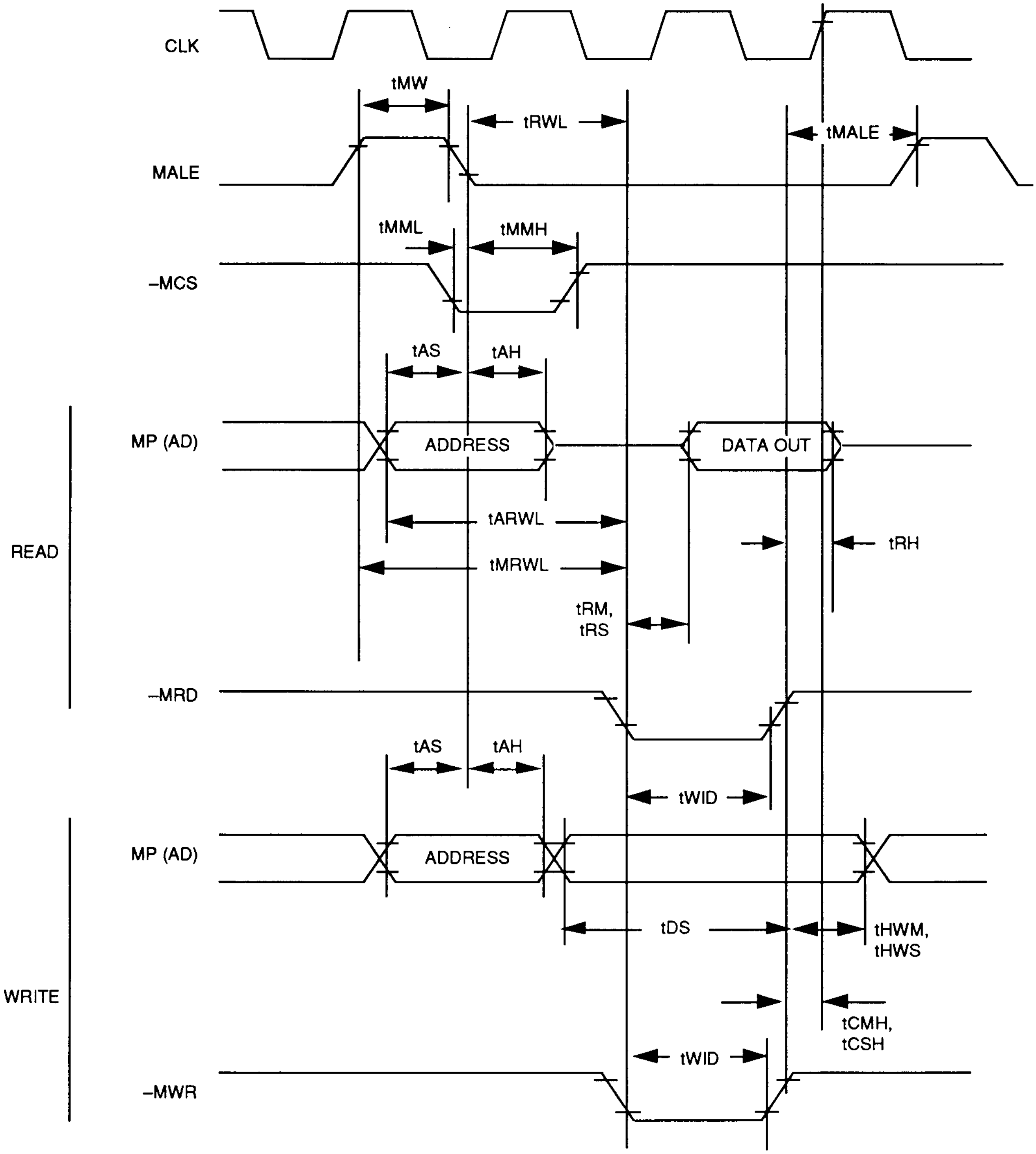


FIGURE 11. MASTER PORT, MULTIPLEXED CONTROL MODE READ/WRITE (VM009-A-80)

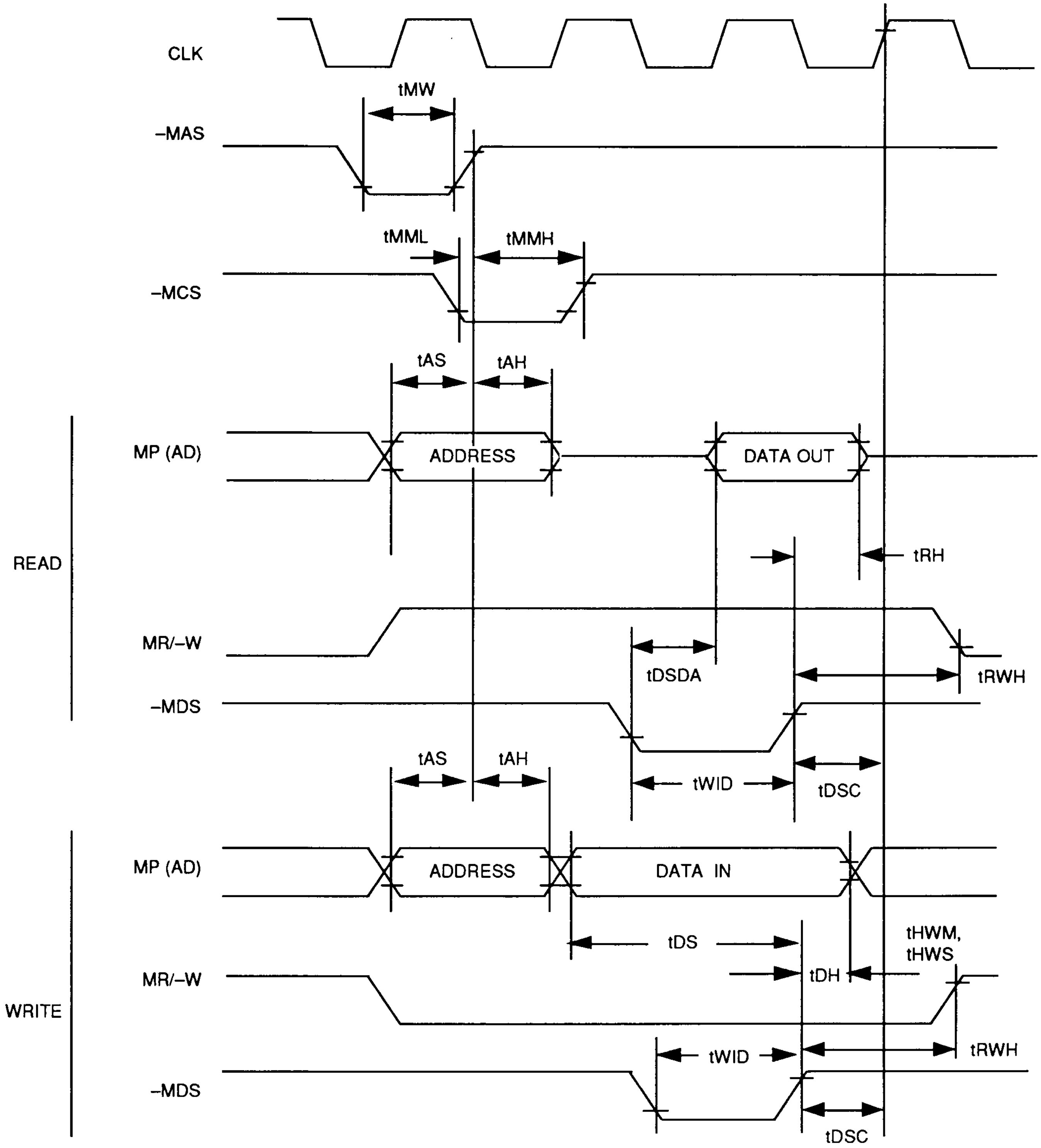


FIGURE 12. MASTER (SLAVE) PORT READ/WRITE (VM009-A-86)

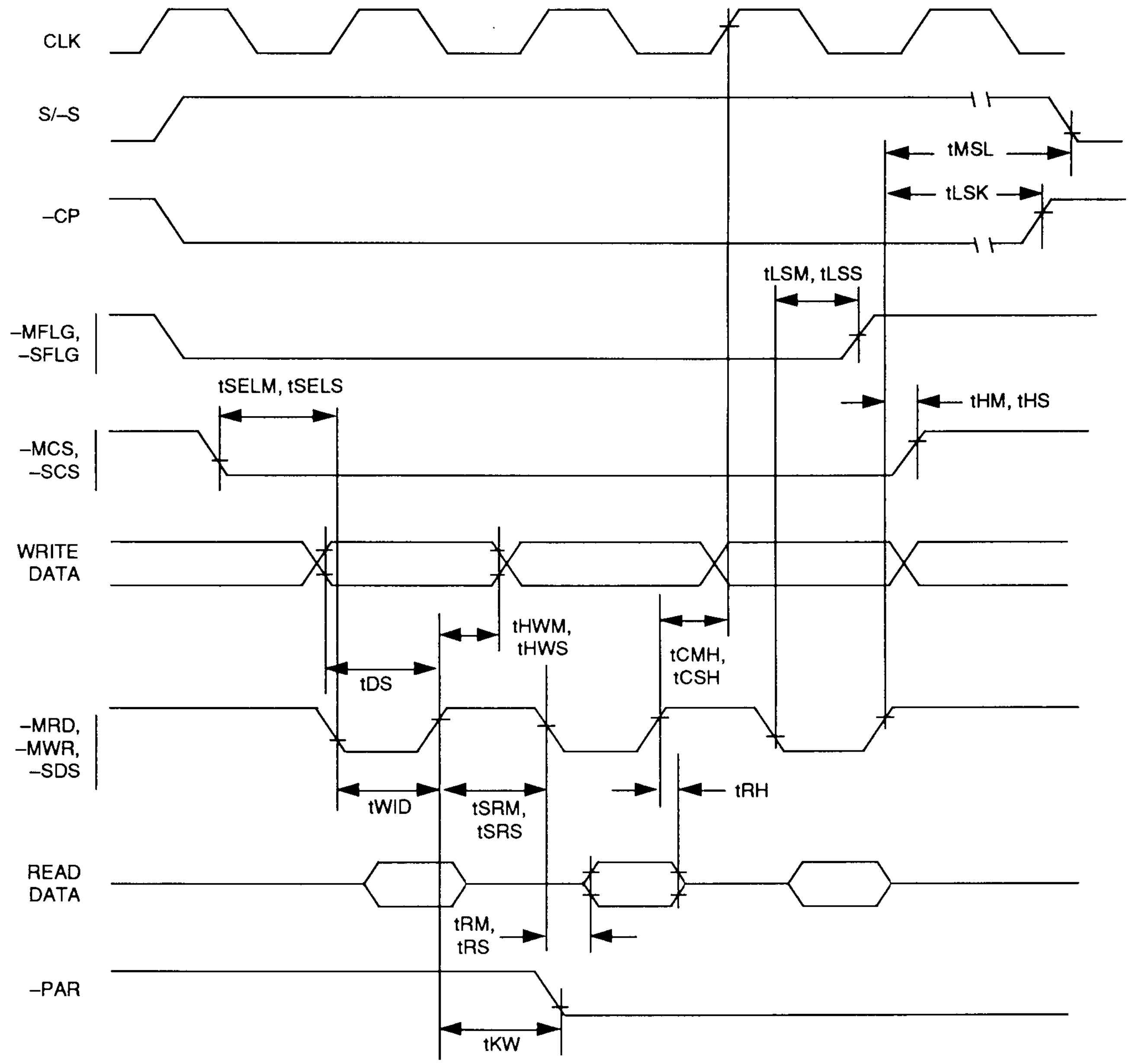


FIGURE 13. MASTER (SLAVE) PORT READ/WRITE (VM009-A-80)

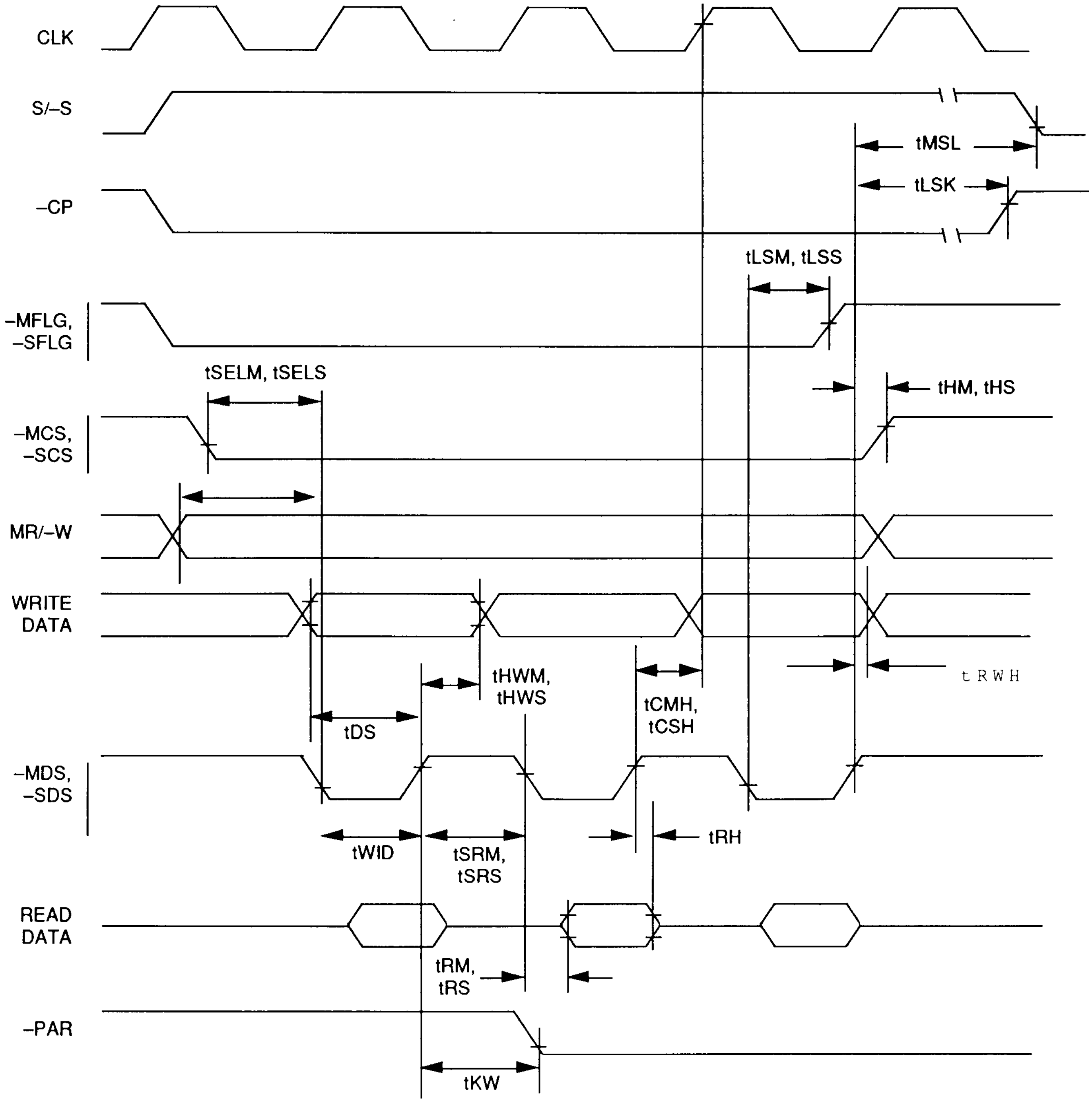
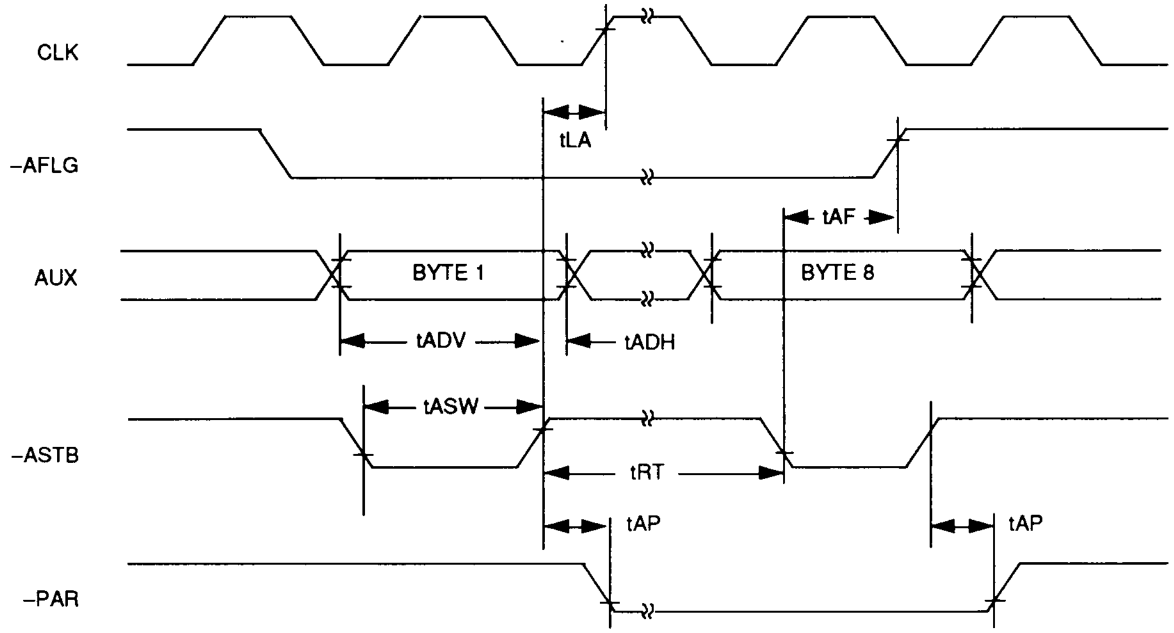


FIGURE 12. AUXILIARY-PORT KEY ENTRY



ABSOLUTE MAXIMUM RATINGS

Ambient Operating Temperature	0°C to +85°C
Storage Temperature without Bias	–65°C to +150°C
Supply Voltage to Ground	–0.5 V to 7.0 V
Applied Output Voltage	–0.5 V to VDD + 0.3 V
Applied Input Voltage	–0.5 V to VDD + 0.3 V

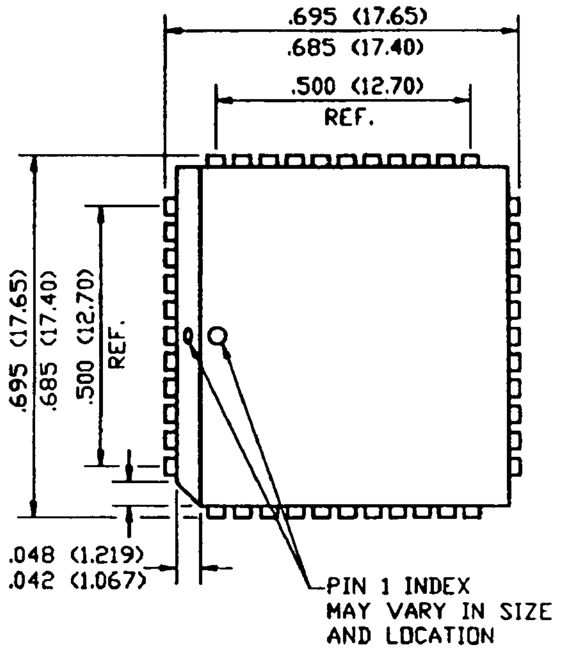
Stresses above those listed may cause permanent damage to the device. These are stress ratings only. Functional operation of this device at these or any other conditions above those indicated in this data sheet is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

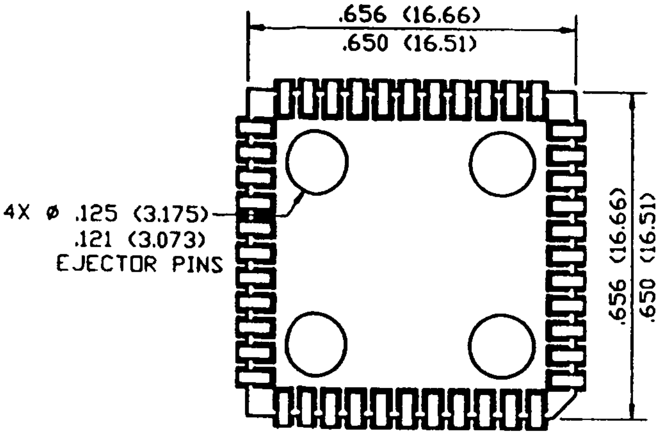
DC CHARACTERISTICS: TA = 0°C to +85°C, VDD = 5 V ±10%, VSS = 0 V

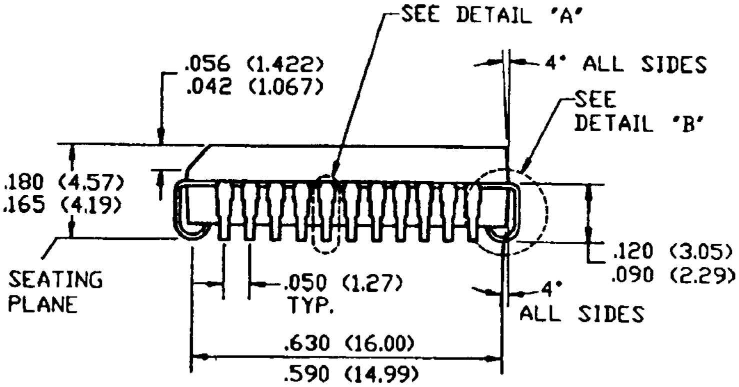
Symbol	Parameter	Min	Max	Unit	Conditions
VIL	Input Low Voltage	–0.5	0.8	V	
VIH	Input High Voltage	2.2	VCC	V	
VOL	Output Low Voltage		0.4	V	IOL = 3.2 mA
VOH	Output High Voltage	2.4		V	IOH = –400 µA
II	Input Leakage Current		±10	µA	VSS < VIN < VCC
IOZ	Output Leakage Current		±10	µA	VSS = +.40 < VIN < VCC
ICC	Supply Current (Average)		250	mA	

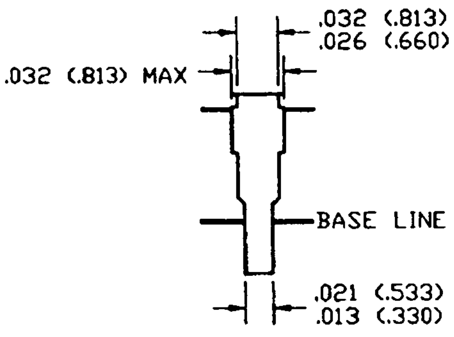
PACKAGE OUTLINE:

44-Lead Plastic Leaded Chip Carrier (PLCC)

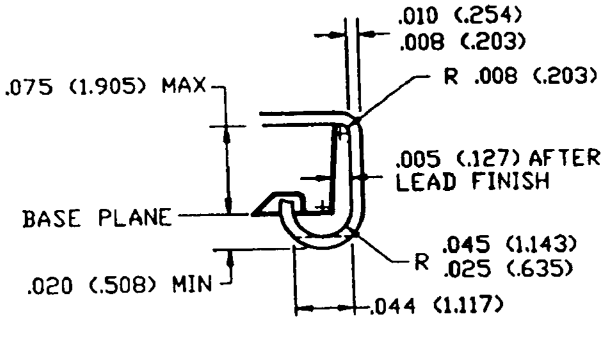








DETAIL 'A'



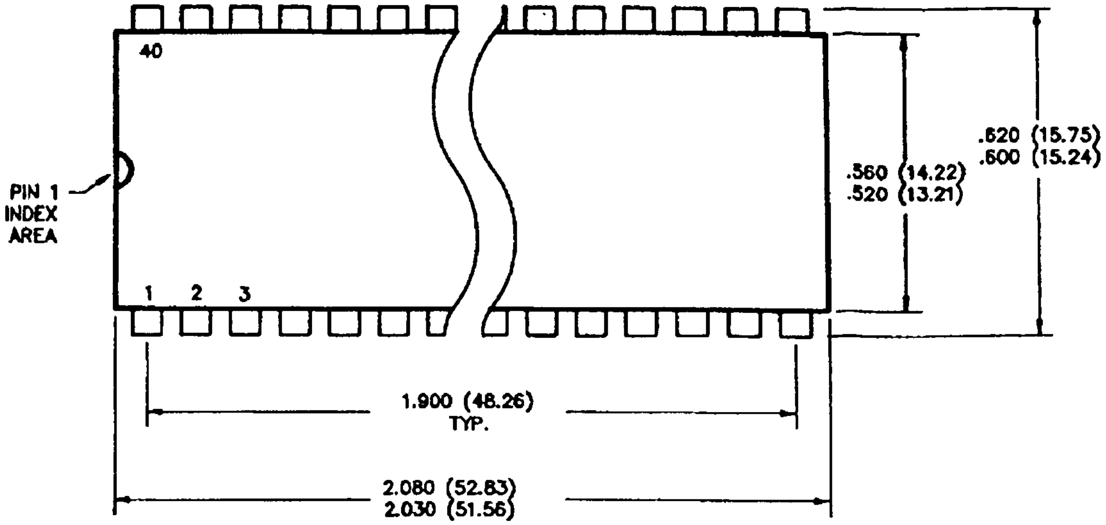
DETAIL 'B'

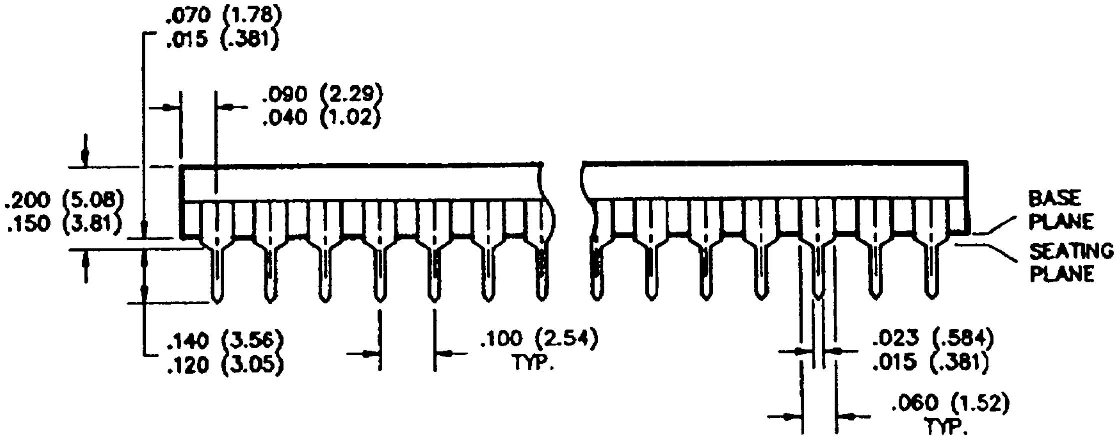
NOTES:

1. LEAD FINISH: MATTE TIN PLACE OR SOLDER PLATE.
2. LEADFRAME MATERIAL: COPPER.
3. TOLERANCE TO BE +/- .005 (0.127).
4. DIMENSIONS ARE IN INCHES (METRIC).
5. MOLDED PLASTIC DIMENSION DOES NOT INCLUDE END FLASH BURR WHICH IS .010 (0.254) MAX. ALL 4 SIDES.
6. SPACING TO BE MAINTAINED BETWEEN FORMED LEAD AND MOLDED PLASTIC ALONG FULL LENGTH OF LEAD.
7. CONTROLLING DIMENSION IS INCHES.

PACKAGE OUTLINE:

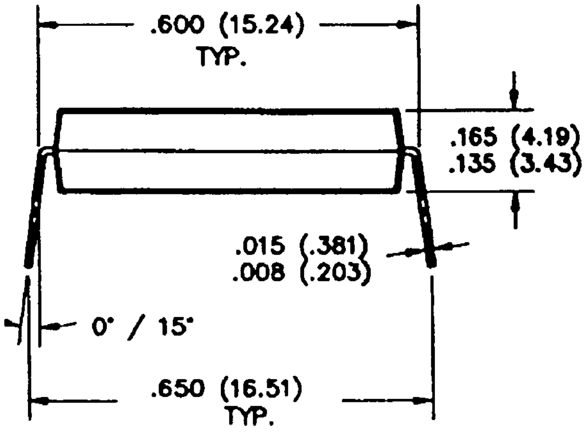
40-Lead Plastic Dual In-line (P-DIP)





NOTES:

1. LEAD FINISH: SOLDER PLATE
2. LEAD MATERIAL: COPPER.
3. PACKAGE LENGTH DOES NOT INCLUDE END FLASH BURR WHICH IS .010 (0.254) MAX. AT EACH END.
4. TOLERANCE TO BE +/- .005 (0.127) UNLESS OTHERWISE NOTED.
5. DIMENSIONS ARE IN INCHES AND (METRIC).
6. PIN 1 INDEX MAY VARY IN SIZE AND SHAPE.



VLSI TECHNOLOGY, INC.

ADVANCE INFORMATION
VM009

VLSI CORPORATE OFFICES

CORPORATE HEADQUARTERS • COMMUNICATIONS PRODUCTS DIVISION AND SPECIAL PRODUCTS DIVISION
VLSI Technology, Inc. • 1109 McKay Drive • San Jose, CA 95131 • 408-434-3100

PERSONAL COMPUTER PRODUCTS DIVISION AND GOVERNMENT PRODUCTS DIVISION
VLSI Technology, Inc. • 8375 South River Parkway • Tempe, AZ 85284 • 602-752-8574

VLSI SUBSIDIARY

COMPASS DESIGN AUTOMATION, INC.
1865 Lundy Avenue • San Jose, CA 95131 • 408-433-4880

VLSI SALES OFFICES AND TECH CENTERS

ARIZONA
8375 South River Parkway
Tempe, AZ 85284
602-752-6450
FAX 602-752-6001

CALIFORNIA
1110 Ringwood Court
San Jose, CA 95131
408-922-5200
FAX 408-922-5252
Mail:
1109 McKay Drive
San Jose, CA 95131

6345 Balboa Blvd.,
Building 1, Suite 100
Encino, CA 91316
818-609-9981
FAX 818-609-0535

30 Corporate Park,
Stes. 100-102
Irvine, CA 92714
714-250-4900
FAX 714-250-9041

FLORIDA
2200 Park Central N., Ste. 600
Pompano Beach, FL 33064
305-971-0404
FAX 305-971-2086

GEORGIA
3200 Peachtree Industrial Blvd.
Duluth, GA 30136
404-476-8574
FAX 404-476-3790

ILLINOIS
3100 Higgins Rd., Ste. 155
Hoffman Estates, IL 60195
708-884-0500
FAX 708-884-9394

MARYLAND
8424 Veterans Highway
Millersville, MD 21108
301-987-8777
FAX 301-987-4489

MASSACHUSETTS
261 Ballardvale St.
Wilmington, MA 01887
508-658-9501
FAX 508-657-6420

NEW JERSEY
311C Enterprise Dr.
Plainsboro, NJ 08536
609-799-5700
FAX 609-799-5720

NORTH CAROLINA
1000 Park Forty Plaza, Ste. 300
Durham, NC 27713
919-544-1891/92
FAX 919-544-6667

TEXAS
850 E. Arapaho Rd., Ste. 270
Richardson, TX 75081
214-231-6716
FAX 214-669-1413

WASHINGTON
405 114th Ave. SE, Ste. 300
Bellevue, WA 98004
206-453-5414
FAX 206-453-5229

FRANCE
2, Allee des Garays
F-91124 Palaiseau Cedex
France
1-69 93 26 00
FAX 1-64 47 04 80

GERMANY
Rosenkavalierplatz 10
D-8000 Muenchen 81
Germany
89-92795-0
FAX 89-92795-145

HONG KONG
Shui On Centre 1504-07
6-8 Harbour Road
Wanchai, Hong Kong
852-802-7755
FAX 852-802-7959

ITALY
Italia S.R.L.
Centro Direzionale Colleoni
Palazzo Cassiopeia, 3
I-20041 Argrate Brianza (MI)
39-6056791
FAX 39-6056808

JAPAN
Shuwa-Kioicho TBR Bldg., #101
Kojimachi 5-7, Chiyoda-Ku
Tokyo, Japan 102
03-3239-5211
FAX 03-3239-5215

Shinsaibashi MID Bldg., 7F
Minami Senba 3-2-29
Chuo-ku, Osaka, 542, Japan
06-243-6041
FAX 06-243-6960

TAIWAN
Unit 7, 7th Floor, Lotus Bldg.
136 Jen-Ai Rd., Section 3
Taipei, Taiwan, R.O.C.
886-2-325-4422
FAX 886-2-325-4411

UNITED KINGDOM
486-488 Midsummer Blvd.
Saxon Gate West, Central Milton
Keynes, MK9 2EQ
United Kingdom
09 08/66 75 95
FAX 09 08/67 00 27

VLSI SALES OFFICES

ALABAMA
2614 Artie St., Ste. 36
Huntsville, AL 35805
205-539-5513
FAX 205-536-8622

CONNECTICUT
850 North Main St., Bldg. 1, 2C
Wallingford, CT 06492
203-265-6698
FAX 203-265-3653

FLORIDA
Ste. 483, 4th Floor
18167 U. S. 19 North
Clearwater, FL 34624
818-538-0681

MINNESOTA
5831 Cedar Lake Rd.
St. Louis Park, MN 55416
612-545-1490
FAX 612-545-3489

NEW YORK
349 W. Commercial St.
Ste. 2272
E. Rochester, NY 14445
716-586-0670
FAX 716-586-0672

OHIO
4 Commerce Park Square
23200 Chagrin Blvd., Ste.600
Cleveland, OH 44122
216-292-8235
FAX 216-464-7609

OREGON
10300 S.W. Greenburg Rd.,
Ste. 478
Portland, OR 97223
503-244-9882
FAX 503-245-0375

TEXAS
9600 Great Hills Trail,
Ste. 150W
Austin, TX 78759
512-343-8191
FAX 512-343-2759

JAPAN
Shuwa-Kioicho Park Bldg., #503
Kioicho 3-6, Chiyoda-Ku
Tokyo, Japan 102
03-3262-0850
FAX 03-3262-0881

SINGAPORE
627 Aljunied Rd. #05-01
Pacific Building
Singapore 1438
65-742-2314
FAX 65-741-1979

VLSI AUTHORIZED DESIGN CENTERS

COLORADO
SIS MICROELECTRONICS, INC.
Longmont, 303-776-1667

ILLINOIS
ASIC DESIGNS
Naperville, 708-717-5841

MAINE
QUADIC SYSTEMS, INC.
South Portland, 207-871-8244

PENNSYLVANIA
INTEGRATED CIRCUIT
SYSTEMS, INC.
King of Prussia, 215-265-8690

EIRE AND U.K.
PA TECHNOLOGY
Herts, 76-261222

SYMBIONICS
Cambridge, 223-421025

FRANCE
CETIA
Toulon Cedex, 9-42-12005

SOREP
Chateaubourg, 99-623955

INDIA
ARCUS TECHNOLOGY LTD.
Bangalore, 91-812-217307

JAPAN
ADC CORPORATION
Tokyo, 03-3492-1251

LSI SYSTEMS, INC.
Kanagawa, 0462-29-3220

NIPPON STEEL CORPORATION
Tokyo, 03-5566-2141

KOREA
ANAM VLSI DESIGN CENTER
Seoul, 82-2-553-2106

NORWAY
NORKRETS AS
Oslo, 47-2360677/8

VLSI SALES REPRESENTATIVES

ARIZONA
LUSCOMBE ENGINEERING
Scottsdale, 602-949-9333

CALIFORNIA
EMERGING TECHNOLOGY
San Jose, 408-263-9366
Cameron Park, 916-676-4387

COLORADO
LUSCOMBE ENGINEERING
Longmont, 303-772-3342

IDAHO
EMERGING TECHNOLOGY
Boise, 208-378-4680

IOWA
SELTEC SALES
Cedar Rapids, 319-364-7660

KANSAS
ELECTRI-REP
Overland Park, 913-649-2168

MICHIGAN
APPLIED DATA MANAGEMENT
Ann Arbor, 313-741-8558
Ypsilanti, 313-485-2974

MISSOURI
ELECTRI-REP
St. Louis, 314-993-4421

NEW YORK
ADVANCED COMPONENTS
Syracuse, 315-437-6700

OHIO
APPLIED DATA MANAGEMENT
Cincinnati, 513-579-8108

OREGON
ELECTRA TECHNICAL SALES
Beaverton, 503-643-5074

UTAH
LUSCOMBE ENGINEERING
Salt Lake City, 801-565-9885

WASHINGTON
ELECTRA TECHNICAL SALES
Kirkland, 206-821-7442

AUSTRALIA
GEORGE BROWN GROUP
Adelaide, 61-8-352-2222
Brisbane, 61-7-252-3876
Melbourne, 61-3-878-8111
Newcastle, 61-49-69-6399
Perth, 61-9-362-1044
Sydney, 61-2-638-1888

AUSTRIA
THOMAS NEUROTH
Wien, 0043-222-82 56 45

CANADA
DAVETEK MARKETING, INC.
British Columbia, 604-430-3680

INTELATECH, INC.
Mississauga, 416-629-0082

HONG KONG
LESTINA INTERNATIONAL, LTD
Tsimshatsui, 852-7351736

ISRAEL
RDT ELECTRONICS ENG. LTD
Tel-Aviv, 23-4832119

SINGAPORE
DYNAMIC SYSTEMS PTE, LTD
Singapore, 65-742-1986

TAIWAN
PRINCETON TECH CORP.
Taipei, 886-2-917-8856

WEIKENG INDUSTRIAL CO.
Taipei, 886-2-776-3998

THAILAND
TRON ELECTRONICS CO. LTD
Bangkok, 66 2 260-3913

VLSI DISTRIBUTORS

United States represented by
ARROW/SCHWEBER
except where noted

ALABAMA
Huntsville, 205-837-6955

ARIZONA
Phoenix, 602-431-0030

CALIFORNIA
Arrow Pacific, 408-432-7171
Los Angeles, 818-880-9686
Orange County, 714-838-5422
San Diego, 619-565-4800
San Francisco, 408-441-9700

COLORADO
Denver, 303-799-0258

CONNECTICUT
Wallingford, 203-265-7741

FLORIDA
North Florida, 407-333-9300
South Florida, 305-429-8200

GEORGIA
Atlanta, 404-497-1300

ILLINOIS
Chicago, 708-250-0500

INDIANA
Indianapolis, 317-299-2071

IOWA
Cedar Rapids, 319-395-7230

KANSAS
Kansas City, 913-541-9542

MARYLAND
Baltimore, 301-596-7800

MASSACHUSETTS
Boston, 508-658-0900

MICHIGAN
Detroit, 313-462-2290

MINNESOTA
Minnesota, 612-941-5280

MISSOURI
St. Louis, 314-567-6888

NEW JERSEY
Philadelphia, 609-596-8000
North Jersey, 201-227-7880

NEW YORK
Rochester, 716-427-0300
Metro, 516-231-1000

NORTH CAROLINA
Raleigh, 919-876-3132

OHIO
Dayton, 513-435-5563
Cleveland, 216-248-3990

OKLAHOMA
Tulsa, 918-252-7537

OREGON
ALMAC/ARROW
Portland, 503-629-8090

PENNSYLVANIA
Pittsburgh, 412-963-6807

TEXAS
Austin, 512-835-4180
Dallas, 214-380-6464
Houston, 713-530-4700

UTAH
Salt Lake City, 801-973-6913

WASHINGTON
ALMAC/ARROW
Seattle, 206-643-9992
Spokane, 509-924-9500

WISCONSIN
Milwaukee, 414-792-0150

BELGIUM/LUXEMBURG
MICROTRON
Mechelen, 215-212223

CANADA
ARROW/SCHWEBER
Montreal, 514-421-7411
Ottawa, 613-226-6903
Toronto, 416-670-7769
Vancouver, 604-421-2333

SEMAD
Calgary, 403-252-5664
Markham, 416-475-8500
Montreal, 514-694-0860
Ottawa, 613-727-8325
British Columbia, 604-420-9889

DENMARK
DELCO
Lynge, 45 42-189533

ENGLAND
HAWKE COMPONENTS
Bramley, NR Basingstoke
256-880800

KUDOS-THAME LTD
Berks, 734-351010

FINLAND
COMDAX
Helsinki, 80-670277

FRANCE
ASAP s.a.
Montigny-le-Bretonneux,
1-30438233

GERMANY
DATA MODUL GmbH
Muenchen, 089-560170

ELECTRONIC 2000 AG
Muenchen, 089-420010

EAST GERMANY
ZENTRUM MIKROELEKTRONIK
Dresden, 0037-51-588464

ITALY
INTER-REP S.P.A.
Torino, 11-2165901

JAPAN
ASAHI GLASS CO. LTD
Tokyo, 03-3218-5854

TOKYO ELECTRON, LTD
Tokyo, 03-3340-8111

TOMEN ELECTRONICS
Tokyo, 03-3506-3650

NETHERLANDS
TME
Aa Heeswijk-Dinther,
4139-8895

PUERTO RICO
ISLA CARIBE ELECTRO SALES
Guaynabo, 809-720-4430

SWEDEN
TRACO AB
Farsta, 8-930000

SPAIN AND PORTUGAL
SEMICONDUCTORES s.a.
Barcelona, 3-21723 40

SWITZERLAND
DECTRO SWISS ELECTRONIC
DESIGN AG
Zuerich, 0041-1-3868-600

3/92

The information contained in this document has been carefully checked and is believed to be reliable. However, VLSI Technology, Inc. (VLSI) makes no guarantee or warranty concerning the accuracy of said information and shall not be responsible for any loss or damage of whatever nature resulting from the use of, or reliance upon it. VLSI does not guarantee that the use of any information contained herein will not infringe upon the patent, trademark, copyright, mask work right or other rights of third parties, and no patent or other license is implied hereby. This document does not in any way extend VLSI's warranty on any product beyond that set forth in its standard terms and conditions of sale. VLSI Technology, Inc. reserves the right to make changes in the products or specifications, or both, presented in this publication at any time and without notice.

LIFE SUPPORT APPLICATIONS: VLSI's products are not intended for use as critical components in life support appliances, devices, or systems in which the failure of a VLSI product to perform could be expected to result in personal injury.

190009-001 2M 4/92