WD2001/2002/20C03A
Data Encryption Devices

FEATURES

- Certified by the National Bureau of Standards
- Transfer rate

WD2001/2002-20	161 Kbytes per second with 2MHz clock
WD2001/2002-30	242 Kbytes per second with 3MHz clock
WD20C03A-05	403 Kbytes per second with 5MHz clock
WD20C03A-08	645 Kbytes per second with 8MHz clock
WD20C03A-10	807 Kbytes per second with 10MHz clock

- Encrypts/decrypts 64-bit data words using 56-bit key word
- Single-port 28-pin package WD2001/20C03A or dual-port 40-pin package WD2002
- Command bit programming using the DAL bus or input pins
- Parity check on key word loading
- Standard 8-bit microprocessor interface
- TTL compatible inputs and outputs
- Key stored in device is not externally accesssible
- Electronic Code Book (ECB) and Cipher Block Chaining (CBC) in WD20C03A
- Battery Back-up capability of internal key register in WD20C03A CMOS device*
- Separate clear and cipher bus structure on WD2002

APPLICATIONS

- Secure brokerage transactions
- Electronic fund transfers
- Secure banking/business accounting
- Mainframe communications
- Remote and host computer communications
- Secure disk or mag tape data storage
- Secure packet-switching transmission

*Available 3rd Quarter 1988.

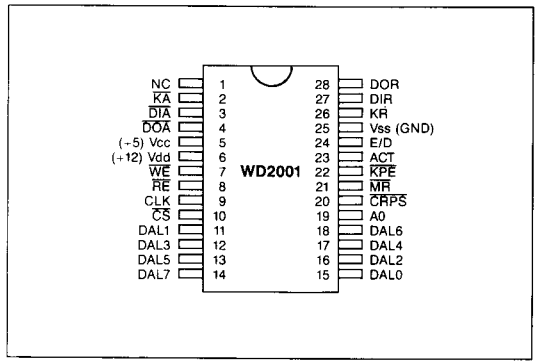


FIGURE 1. WD2001

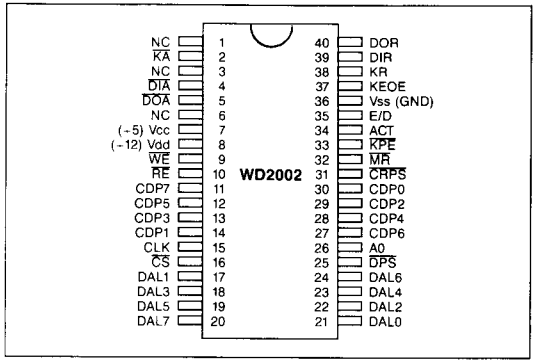


FIGURE 2. WD2002

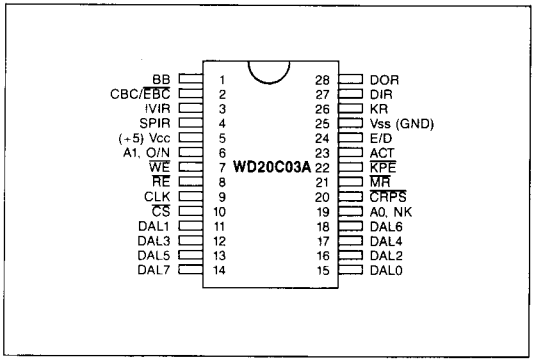
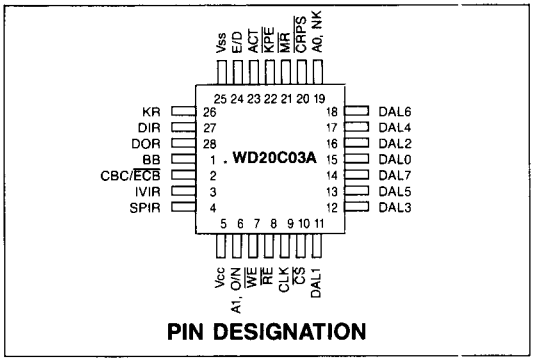
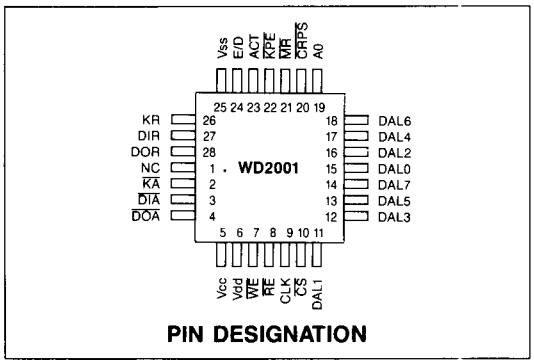


FIGURE 3. WD20C03A



PIN DESIGNATION



PIN DESIGNATION

INTRODUCTION

The Western Digital WD2001/2002/20C03A Data Encryption/Decryption devices are designed to encrypt and decrypt 64-bit blocks of data using the algorithm specified in the Federal Information Processing Data Encryption Standard (#46). These devices encrypt a 64-bit clear text word using a 56-bit, user-specified key to produce a 64-bit cipher text word. When reversed, the cipher text word is decrypted to produce the original clear text word.

The WD2001 and the WD2002 are fabricated in silicon gate NMOS and the WD20C03A is silicon gate CMOS technology. All devices are TTL compatible on inputs and outputs.

All charts and diagrams shown in this data sheet describe all three devices except where indicated. There are separate sections to describe the device organization and operation for the WD2001/2002 and for the WD20C03A.

NOTE: These devices cannot be shipped outside of the United States of America without authorization from the State Department and the Department of Defense.

TABLE 1. PIN DESCRIPTION

2001	2002	20C03A	SIGNAL NAME	MNEMONIC	FUNCTION
N/C	N/C	1	BATTERY BACK-UP KEY	BB	When $\overline{CRPS}$ is logic 1 or open, this pin is an output reflecting the status of the BATTERY BACK-UP KEY bit (bit 5) of the COMMAND REGISTER. When $\overline{CRPS}$ is a logic 0 or low, this pin is an input that overrides the BATTERY BACK-UP KEY bit.
11-18	17-24	11-18	DATA LINES	DAL 0 > DAL 7	Eight active true, three-state, bi-directional I/O lines used for information transfer to and from the DES device. During single port operation, all COMMAND/STATUS, KEY WORD and DATA WORD transfers are via this bus. During dual port operation in the WD2002 all COMMAND/STATUS, KEY WORD and clear DATA WORD transfers are via the CIPHER DATA PORT (CDP) bus.***
N/A*	11-14 27-30	N/A*	CIPHER DATA PORT	CDP 0 > CDP 7	These pins are available on the WD2002 and are active true, three-state, bi-directional I/O lines used only in dual port operation. Cipher DATA WORD transfers are via this bus.
6	8	N/A	POWER SUPPLY	V_{DD}	+12V

TABLE 1. PIN DESCRIPTION (continued)

2001	2002	20C03A	SIGNAL NAME	MNEMONIC	FUNCTION
N/A	N/A	6	ADDRESS 1, OLD/NEW	A1, O/N	When $\overline{CRPS}$ is a logic 1 or open, and this input is a logic 1, the STATUS REGISTER is addressed ($\overline{CS}$ = 0, A0 = 1). When this input is a logic 0, the COMMAND REGISTER is addressed ($\overline{CS}$ = 0, A0 = 1). This input is ignored when A0 = 0. When $\overline{CRPS}$ is a logic 0 or low and this input is a logic 0, the device is in the WD20C03A mode. When this input is a logic 1, the device is in the WD2001 mode. The only way to return to the WD20C03A mode after setting the device in the WD2001 is by resetting the device.
5	7	5	POWER SUPPLY	V_{CC}	+5 V
25	36	25	GROUND	V_{SS}	GROUND
9	15	9	CLOCK	CLK	System clock input.
21	32	21	$\overline{MASTER\ RESET}$	$\overline{MR}$	$\overline{MR}$ active low resets the COMMAND/STATUS REGISTER and resets internal circuitry. (Requires active clock for reset operation.)
10	16	10	$\overline{CHIP\ SELECT}$	$\overline{CS}$	$\overline{CS}$ is made low to access registers within the device.
8	10	8	$\overline{READ\ ENABLE}$	$\overline{RE}$	The contents of the selected register are placed on the DAL (or CDP) bus lines when $\overline{CS}$ and $\overline{RE}$ are made low.
7	9	7	$\overline{WRITE\ ENABLE}$	$\overline{WE}$	Information on the DAL (or CDP) bus lines is written into the selected register when $\overline{CS}$ and $\overline{WE}$ are made low.
19	26	N/A	ADDRESS 0	A0	When this input is active high (during $\overline{CS}$ enable), the COMMAND/STATUS REGISTER is addressed. (A0 active high will override internally generated addressing of the KEY and DATA REGISTERS as described on page 7). This input is ignored when $\overline{CRPS}$ is low.
N/A	N/A	19	ADDRESS 0, NEW KEY	A0, NK	When $\overline{CRPS}$ is a logic 1 or open, this input pin has the same functions as A0 on the WD2001/2002. When $\overline{CRPS}$ and A1, O/N are a logic 0, a logic 1 on this input pin will request that a new key be loaded in the KEY REGISTER. The device will respond by activating the KR pin.
26	38	26	KEY REQUEST	KR	This output is active high when the DES device is requesting that a byte of the KEY WORD be written into the KEY REGISTER. (The KEY REGISTER is automatically addressed when KR is active, unless overridden by A0.)
2	2	N/A	$\overline{KEY\ ACKNOWLEDGE}$	$\overline{KA}$	This output is active low when $\overline{WE}$ is made low while the KEY REGISTER is addressed. (Can be used for a handshake.)

TABLE 1. PIN DESCRIPTION (continued)

2001	2002	20C03A	SIGNAL NAME	MNEMONIC	FUNCTION
N/A	N/A	2	CIPHER BLOCK CHAINING/ ELECTRONIC CODE BOOK	CBC/$\overline{\text{ECB}}$	When $\overline{\text{CRPS}}$ is a logic 1 or open, this pin is an output pin reflecting the status of CBC/$\overline{\text{ECB}}$ bit (bit 7) of the COMMAND REGISTER. When $\overline{\text{CRPS}}$ is a logic 0, this pin is an input pin and overrides the CBC/$\overline{\text{ECB}}$ bit of the COMMAND REGISTER.
27	39	27	DATA-IN REQUEST	DIR	This output is active high when the DES device is requesting that a byte of the DATA WORD be written into the DATA REGISTER. (The DATA REGISTER is automatically addressed when DIR is active, unless overridden by A0.)
3	4	N/A	$\overline{\text{DATA-IN ACKNOWLEDGE}}$	$\overline{\text{DIA}}$	This output is active low when $\overline{\text{WE}}$ is made low while the DATA REGISTER is addressed. (Can be used for a handshake.)
N/A	N/A	3	INITIAL VECTOR-IN REQUEST	IVIR	This output is active high when the device is requesting that a byte of the IV WORD be written into the IV REGISTER. (The IV REGISTER is automatically addressed when IVIR is active, unless overridden by A0.)
28	40	28	DATA-OUT REQUEST	DOR	This output is active high when the DES device is requesting that a byte of the DATA WORD be read from the DATA REGISTER. (The DATA REGISTER is automatically addressed when the DOR is active, unless overridden by A0.)
4	5	N/A	$\overline{\text{DATA-OUT ACKNOWLEDGE}}$	$\overline{\text{DOA}}$	This output is active low when $\overline{\text{RE}}$ is made low while the DATA REGISTER is addressed. (Can be used for handshake.)
N/A	N/A	4	SPECIAL PATTERN-IN	SPIR	This output is active high during battery back-up mode, when the device is requesting that a byte of the SPECIAL PATTERN WORD be written into the DATA REGISTER. (The DATA REGISTER is automatically addressed when SPIR is active, unless overridden by A0.)
22	33	22	$\overline{\text{KEY PARITY ERROR}}$	$\overline{\text{KPE}}$	This output is active low when enabled via the COMMAND/STATUS REGISTER bit 2 (KEOE) and a parity error has been detected during loading of the KEY REGISTER.
20**	31**	20**	$\overline{\text{COMMAND REGISTER PIN SELECT}}$	$\overline{\text{CRPS}}$	This input selects DAL bus or input pin programming of the COMMAND/STATUS REGISTER. $\overline{\text{CRPS}}$ high or open selects DAL bus programming. $\overline{\text{CRPS}}$ low selects input pin programming.
23	34	23	ACTIVATE	ACT	When $\overline{\text{CRPS}}$ is a logic 1 or open, this pin is an output reflecting the status of the ACTIVATE bit (C/S R1) of the COMMAND/ STATUS REGISTER. When $\overline{\text{CRPS}}$ is a logic 0, this pin is an input that overrides the ACTIVATE bit of the COMMAND/STATUS REGISTER.

TABLE 1. PIN DESCRIPTION (continued)

2001	2002	20C03A	SIGNAL NAME	MNEMONIC	FUNCTION
N/A*	37	N/A*	KEY ERROR OUTPUT ENABLE	KEOE	This output indicates the status of the KEY ERROR OUTPUT ENABLE bit (C/S R2) of the COMMAND/STATUS REGISTER. This output is active when input pin programming is selected ($\overline{CRPS}$ low). This pin is available on the WD2002 40-pin package version only.
24	35	24	$\overline{ENCRYPT}$/ DECRYPT	$\overline{E}$/D	When $\overline{CRPS}$ is high or open, this pin is an output reflecting the status of the $\overline{ENCRYPT}$/ DECRYPT bit (C/S R3) of the COMMAND/ STATUS REGISTER. When $\overline{CRPS}$ is low, this pin is an input pin that overrides the $\overline{ENCRYPT}$/DECRYPT bit of the COMMAND/ STATUS REGISTER.
N/A*	25**	N/A	$\overline{DUAL\ PORT\ SELECT}$	$\overline{DPS}$	When this input is high or open, single port operation is selected and all DES chip transfers are via the DAL bus. When $\overline{DPS}$ is low, dual port operation is selected and both the DAL bus and the CDP bus are used creating separate buses for clear data (DAL bus) and for cipher data (CDP bus). This pin is available on the WD2002 40-pin package version only.

*The WD2001/WD20C03A 28-pin package versions do not have the 8 CDP pins, the KEOE pin, or the $\overline{DPS}$ pin.
**These inputs have internal pull-up resistors.
*** L.S.B. (DATA BIT 0) at DAL 7 and CDP 7. M.S.B. (DATA BIT 7) at DAL 0 and CDP 0.

WD2001/2002 ORGANIZATION

The WD2001 and WD2002 Data Encryption Standard (DES) devices consist of a 56-bit KEY REGISTER, a 64-bit DATA REGISTER, an 8-bit COMMAND/STATUS REGISTER, plus the necessary logic to check KEY parity and implement the National Bureau of Standards (NBS) algorithm. Although the DES device interfaces to a wide variety of processors including mini-computers, the interface is tailored to the 8080A class microprocessor. The block diagram is shown in Figure 4.

TYPICAL APPLICATION

Figure 5 shows a block diagram for a floppy disk based, DES secure smart terminal. The Direct Memory Access (DMA) controller optimizes data transfer operations not only for the floppy disk but also for file encryption and decryption operations.

Secure features for the terminal include: secure file storage on floppy disks, clear/secure transmission using the communications I/O, and battery back-up of the terminal ID key.

Tampering with the terminal by unauthorized persons either through the keyboard, power supply, interrupt interlock, or attempting to open the service panel results in memory scrambling and terminal ID key destruction. A hardware option was also included to allow the use of the UC1671 or the WD1935A for bit-oriented SDLC, HDLC, or ADCCP protocols.

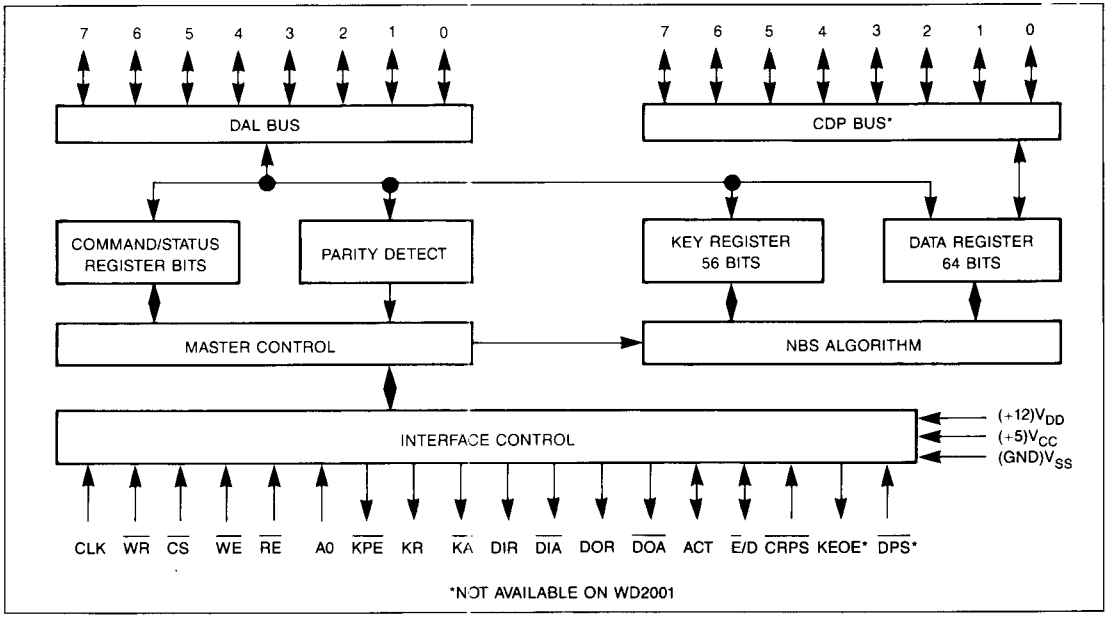


FIGURE 4. WD2001/2002 BLOCK DIAGRAM

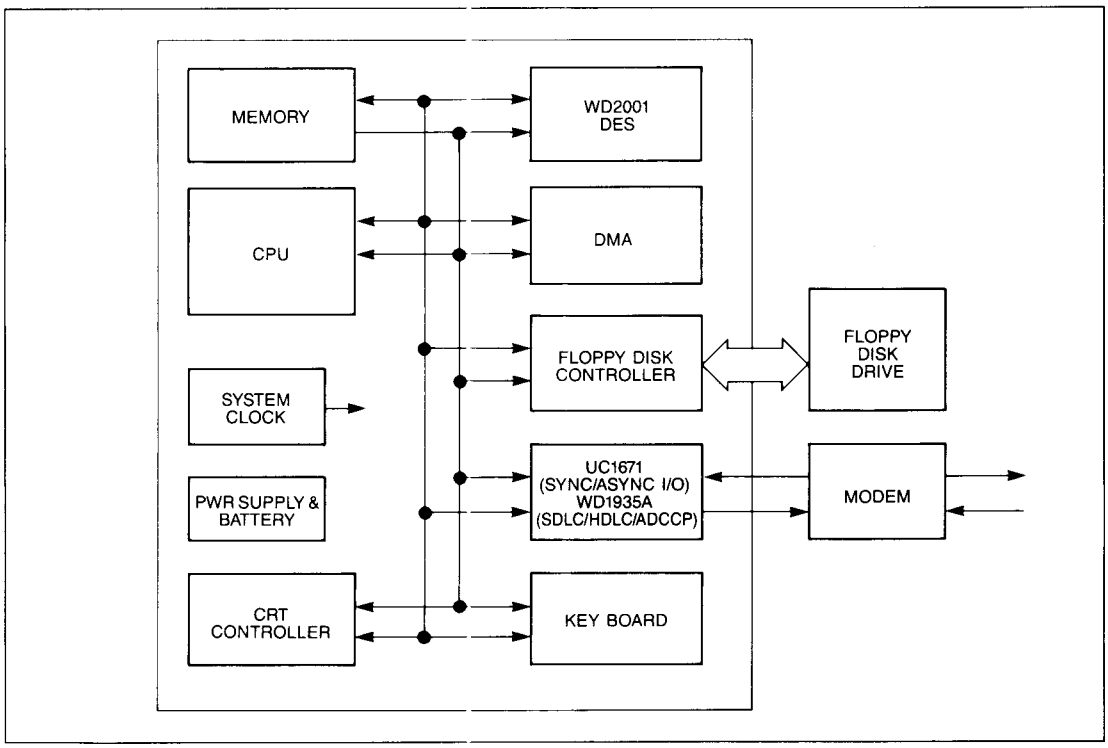


FIGURE 5. BLOCK DIAGRAM: SECURE SMART TERMINAL

OPERATIONAL OVERVIEW

This section gives an overview of how the WD2001/2002 devices function. More specific detail is discussed in the section called Operation.

These devices can be programmed for encryption or decryption, and single port (WD2001) or dual port (WD2002) operation. Data is encrypted or decrypted with a 64-bit, user-defined KEY WORD. Data encrypted with a given KEY WORD can be decrypted only by using the same KEY WORD.

The KEY REGISTER is loaded by the system with eight successive bytes (8-bit). Parity is checked on each byte of the KEY WORD as it is loaded into the KEY REGISTER. The seventh bit (DAL 0) of each 8-bit byte is reserved for odd parity for that byte and is not used in the algorithm calculation. Similarly, the DATA REGISTER is loaded with eight successive bytes (8-bit) and is read by reading eight successive bytes (8-bit).

When the WD2001/2002 is programmed for encryption, the DATA REGISTER is loaded with eight bytes of plain or clear text. The device encrypts the data and the encrypted data may be read from the DATA REGISTER (64-bits of encrypted text).

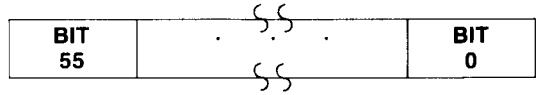
When the device is programmed for decryption, the DATA REGISTER is loaded with eight bytes of encrypted or cipher text. The device decrypts the data and the plain text may be read from the DATA REGISTER (64-bits of plain text). Note that all transfers to and from the KEY REGISTER and/or DATA REGISTER must occur in eight successive bytes (8-bit).

REGISTER DESCRIPTION

The following sections describe the KEY, DATA, and COMMAND/STATUS REGISTERS of the WD2001/2002.

Key Register

This 56-bit register contains the KEY which is used to encrypt or decrypt the data with the DES algorithm. Eight successive bytes are needed to load the KEY REGISTER. The KEY REGISTER can be loaded only when there is a KEY REQUEST, that is, bit four in the COMMAND/STATUS REGISTER is set to one and/or the KR output pin is high. This is a LOAD-ONLY REGISTER.

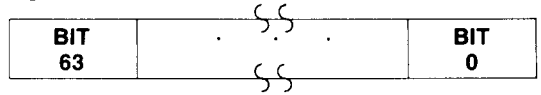


KEY REGISTER (LOAD ONLY)

Data Register

This 64-bit register contains the plain or cipher text either to be read out or that has been loaded in. During encryption, the DATA REGISTER is loaded with plain text and contains cipher text to be read out. During decryption, the DATA REGISTER is loaded with cipher text and contains plain text to be read out. The DATA REGISTER is always read or loaded with eight successive bytes (8-bit).

The DATA REGISTER can only be loaded when there is a DATA-IN REQUEST, that is bit six in the COMMAND/STATUS REGISTER is set to one and/or the DIR output pin is high. Similarly, the DATA REGISTER can be read only when there is a DATA-OUT REQUEST, that is bit seven in the COMMAND REGISTER is set to one and/or the DOR output is high.



DATA REGISTER

Command/Status Register

This 8-bit register controls the operation of the WD2001/2002 and monitors its status. Bits 4, 5, 6, and 7 status-only bits (read only). Bits 1, 2, and 3 are COMMAND/STATUS bits (read/write) and are normally loaded only once for an entire encryption or decryption process. Bit 0 is not used.

7	6	5	4	3	2	1	0
DOR	DIR	$\overline{\text{KPE}}$	KR	$\overline{\text{E}}$/D	KEOE	ACT	N/U
STATUS BITS (READ-ONLY)				COMMAND/STATUS BITS (READ/WRITE)			

COMMAND/STATUS REGISTER

TABLE 2. COMMAND/STATUS REGISTER

BIT	NAME	FUNCTION
0	NOT USED	
1	ACTIVATE	This bit must be set from a logic 0 to a logic 1 to initiate loading the KEY REGISTER. This bit must be a logic 1 for encrypt/decrypt operation. This is a read/write bit.
2	KEY ERROR OUTPUT ENABLE (KEOE)	When a logic 0, the KEY PARITY ERROR output pin (KPE) remains inactive regardless of the status of the KEY PARITY ERROR bit (bit 5). When a logic 1, the KEY PARITY ERROR output pin is active when the KPE bit (bit 5) is a logic 1. This bit is set to a logic 1 upon a MASTER RESET. This is a read/write bit.
3	$\overline{\text{ENCRYPT}}$/DECRYPT ($\overline{\text{E}}$/D)	When a logic 0, data is to be encrypted. When a logic 1, data is to be decrypted. This is a read/write bit.
4	KEY REQUEST (KR)	This bit is set one clock period after the ACTIVATE bit is set (from a logic 0 to a logic 1). It is reset upon loading of the last (8th) byte of the KEY REGISTER. This is a read-only bit.
5	$\overline{\text{KEY PARITY ERROR}}$ ($\overline{\text{KPE}}$)	This bit is set internally upon detection of a parity error during loading of the KEY REGISTER. It is reset when the ACTIVATE bit is programmed from a logic 1 to a logic 0 (i.e., chip is deactivated). This is a read-only bit.
6	DATA-IN REQUEST (DIR)	This bit is set either upon: (a) Completion of KEY REGISTER loading – or – (b) Completion of DATA REGISTER reading (i.e., the last DATA-OUT REQUEST has been serviced by an 8-byte read and the DATA REGISTER is now empty and ready to be loaded with the next DATA WORD). It is reset upon loading of the last (8th) byte of the DATA REGISTER. This is a read-only bit.
7	DATA-OUT REQUEST (DOR)	This bit is set upon completion of the internal encrypt/decrypt calculation of a DATA WORD. It is reset upon the reading of the last (8th) byte of the DATA REGISTER. This is a read-only bit.

NOTE: All bits of the COMMAND/STATUS REGISTER are reset to a logic 0 upon $\overline{\text{MASTER RESET}}$, except KEOE (bit two) which is set to a logic 1 and bit zero which is read as a logic 1 by default during a COMMAND/STATUS REGISTER read.

OPERATION

This section explains how the WD2001/2002 devices function.

The WD2001/2002 is initiated by programming Bit 1 (ACT, ACTIVATE) to a logic 1 in the COMMAND/STATUS REGISTER. The device will respond by activating Bit 4 (KR, KEY REQUEST) in the COMMAND/STATUS REGISTER and the KEY REQUEST (KR) output.

A0 must be deactivated to allow the WD2001/2002 to address the KEY REGISTER internally and load the KEY REGISTER with the 64-bit KEY WORD. The KEY REGISTER is loaded with eight successive bytes (8-bit) by activating $\overline{\text{WRITE ENABLE}}$ ($\overline{\text{WE}}$) eight times (with $\overline{\text{CS}}$ active).

When $\overline{\text{WE}}$ is activated, the WD2001/2002 deactivates the KEY REQUEST (KR) output. When $\overline{\text{WE}}$ is deactivated, the WD2001/2002 activates the KR output. The WD2001/2002 will activate eight KEY REQUESTS to fill up the KEY REGISTER.

When $\overline{\text{WE}}$ is activated, the WD2001/2002 will also respond by activating the $\overline{\text{KEY ACKNOWLEDGE}}$ ($\overline{\text{KA}}$) output. Thus, $\overline{\text{KA}}$ will be activated eight times during the loading of the KEY REGISTER.

The KR and $\overline{\text{KA}}$ outputs can either be used for asynchronous handshaking (as in DMA control) or, after the first activated KR, further activations can be ignored and the KEY REGISTER can be loaded synchronously (as in programmed I/O) by eight successive activations of $\overline{\text{WE}}$.

Each byte of the KEY WORD is checked for odd parity when it is loaded into the KEY REGISTER (see Figure 6). If a parity error is detected, the WD2001/2002 will set Bit 5 ($\overline{\text{KPE}}$, $\overline{\text{KEY PARITY ERROR}}$) in the

COMMAND/STATUS REGISTER to a logic 1. If Bit 2 (KEOE, KEY ERROR OUTPUT ENABLE) in the COMMAND/STATUS REGISTER has been set, the device will also activate the KPE output. Bit 5 ($\overline{KPE}$) in the COMMAND/STATUS REGISTER will be reset to a logic 0 when Bit 1 (ACT, ACTIVATE) in the COMMAND/STATUS REGISTER is reset to a logic 0.

After loading the eighth (last) byte of the KEY WORD into the KEY REGISTER, the WD2001/2002 will set Bit 6 (DIR, DATA-IN REQUEST) in the COMMAND/STATUS REGISTER and activate the DATA-IN REQUEST (DIR) output (see Figure 7). The 64-bit DATA WORD must then be loaded into the DATA REGISTER which will be loaded in the same manner as the KEY REGISTER by eight successive activations of DATA-IN REQUEST (DIR) output, $\overline{WRITE\ ENABLE}$ ($\overline{WE}$) input, and $\overline{DATA\text{-}IN\ ACKNOWLEDGE}$ ($\overline{DIA}$) output.

After the eighth (last) byte of the DATA WORD has been loaded, the WD2001/2002 starts its operation internally by encrypting or decrypting the data to the DES algorithm. Upon completion of this operation, the encrypted or decrypted data is internally loaded into the DATA REGISTER, and the WD2001/2002 will set Bit 7 (DOR, DATA-OUT REQUEST) in the COMMAND/STATUS REGISTER and activate the DATA-OUT REQUEST (DOR) output (see Figure 8).

The DATA WORD must then be read from the DATA REGISTER in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST (DOR) output, $\overline{READ\ ENABLE}$ ($\overline{RE}$) input, and $\overline{DATA\text{-}OUT\ ACKNOWLEDGE}$ ($\overline{DOA}$) output.

For both DATA-IN and DATA-OUT, after the first request further activations of the DIR, DOR, $\overline{DIA}$, and $\overline{DOA}$ outputs can be ignored and the DATA REGISTER can be loaded or read by eight successive activations of $\overline{WE}$ or $\overline{RE}$.

After the eighth (last) byte of the DATA REGISTER has been read, the WD2001/2002 will reactivate the DATA-IN REQUEST. The cycle of loading the DATA REGISTER, encrypting or decrypting of the data to the DES algorithm, and reading the new data from the DATA REGISTER is repeated until all the required data (text) has been encrypted or decrypted with the current KEY WORD.

When this is completed, Bit 1 (ACT, ACTIVATE) in the COMMAND/STATUS REGISTER should be reset to a logic 0 to lock the last KEY WORD loaded into the WD2001/2002 and prevent the access and use of it by an unauthorized user. To resume operation, the ACTIVATE bit must be reset to a logic 1, which activates KEY REQUEST, and a new KEY must be loaded before access to the DATA REGISTER is possible.

To encrypt plain data, it is loaded into the DATA REGISTER, and then encrypted data is read from the DATA REGISTER after Bit 3 ($\overline{ENCRYPT}$/DECRYPT) in the COMMAND/STATUS REGISTER has been set to a logic 0.

To decrypt encrypted data, it is loaded into the DATA REGISTER, and then plain data is read from the DATA REGISTER after Bit 3 ($\overline{ENCRYPT}$/DECRYPT) in the COMMAND/STATUS REGISTER has been set to a logic 1.

NOTE: To accomplish switching from encryption to decryption (or vice versa) with the same KEY WORD before a DATA WORD transfer is initiated, A0 must be set to a logic 1. The WD2001/2002 will then override the internal addressing of the DATA REGISTER and address the COMMAND/STATUS REGISTER, which can now be reprogrammed. When A0 is reset to a logic 0, the device will then internally address the DATA REGISTER, while awaiting the loading of the next DATA WORD.

DUAL PORT OPTION (WD2002 ONLY)

When $\overline{DUAL\ PORT\ SELECT}$ ($\overline{DPS}$, pin 25) input is set to a logic 1 or left open (that is, single port operation is selected), all transfers to and from the WD2002 use the DAL bus. The CDP bus is not used and remains three-stated.

When $\overline{DPS}$ is set to a logic 0 (that is, dual port operation is selected), all transfers to and from the COMMAND/STATUS REGISTER, transfers to the KEY REGISTER, and transfers of clear DATA WORDS still use the DAL bus. However, encrypted (cipher) DATA WORDS are now transferred using the CDP bus. This provides separate buses for clear and encrypted (cipher) text.

Encryption during dual port operation requires loading clear data using the DAL bus and reading encrypted (cipher) data using the CDP bus.

Decryption during dual port operation requires loading encrypted (cipher) data using the CDP bus and reading clear data using the DAL bus.

COMMAND SELECT OPTION

When the $\overline{COMMAND\ REGISTER\ PIN\ SELECT}$ ($\overline{CRPS}$) input is set to a logic 0, the ACT and $\overline{E}$/D pins are enabled as inputs and they will override bits 1 and 3 (respectively) in the COMMAND/STATUS REGISTER. This override allows input pins to control the device. Bit 2 (KEOE) in the COMMAND/STATUS REGISTER will remain a logic 1.

The A0 bit will be disregarded in this option and the COMMAND/STATUS REGISTER cannot be accessed using the DAL bus lines.

Note that the ACT pin must be toggled from a logic 1 to a logic 0 to clear a parity error detection when operating in this mode.

All other operations remain the same as described previously.

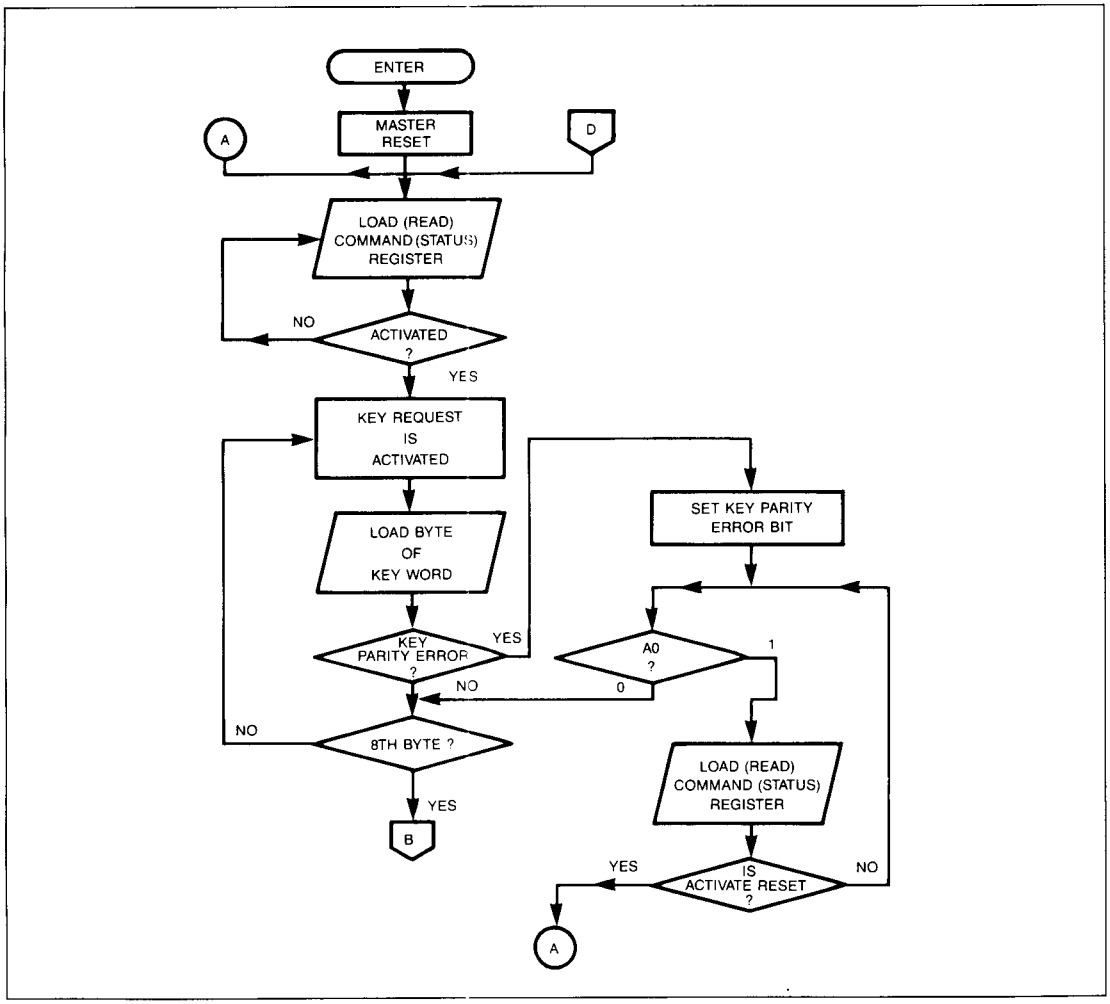


FIGURE 6. LOADING THE KEY WORD

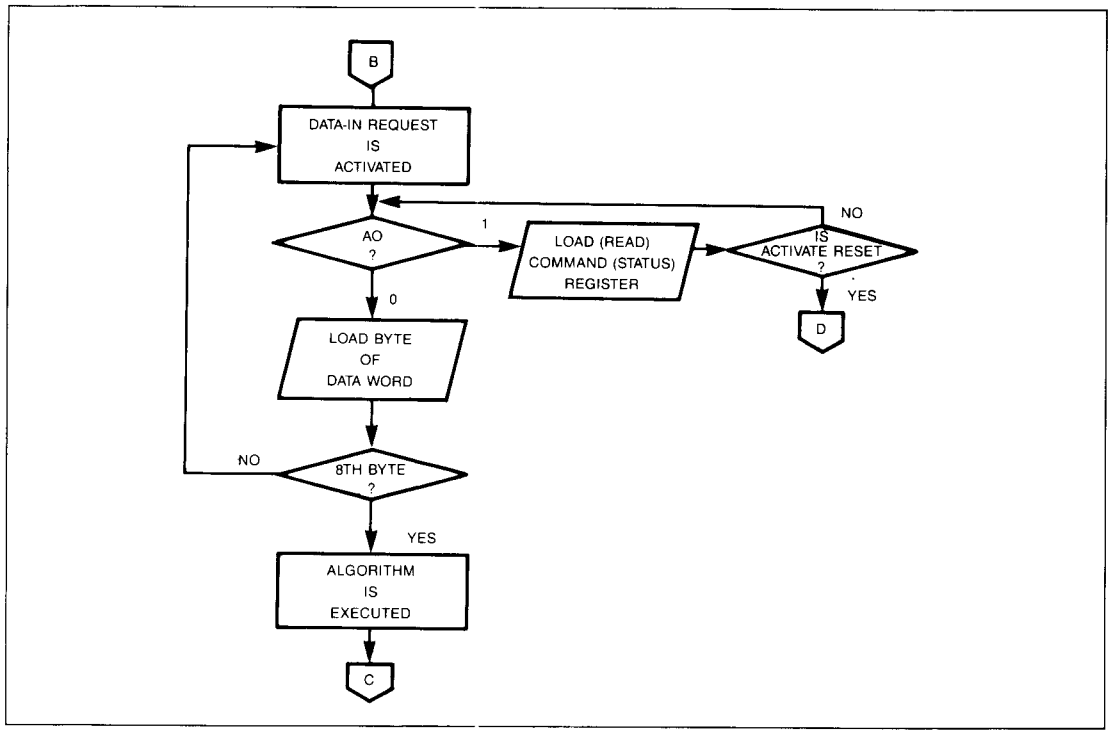


FIGURE 7. ACTIVATING DIR OUTPUT

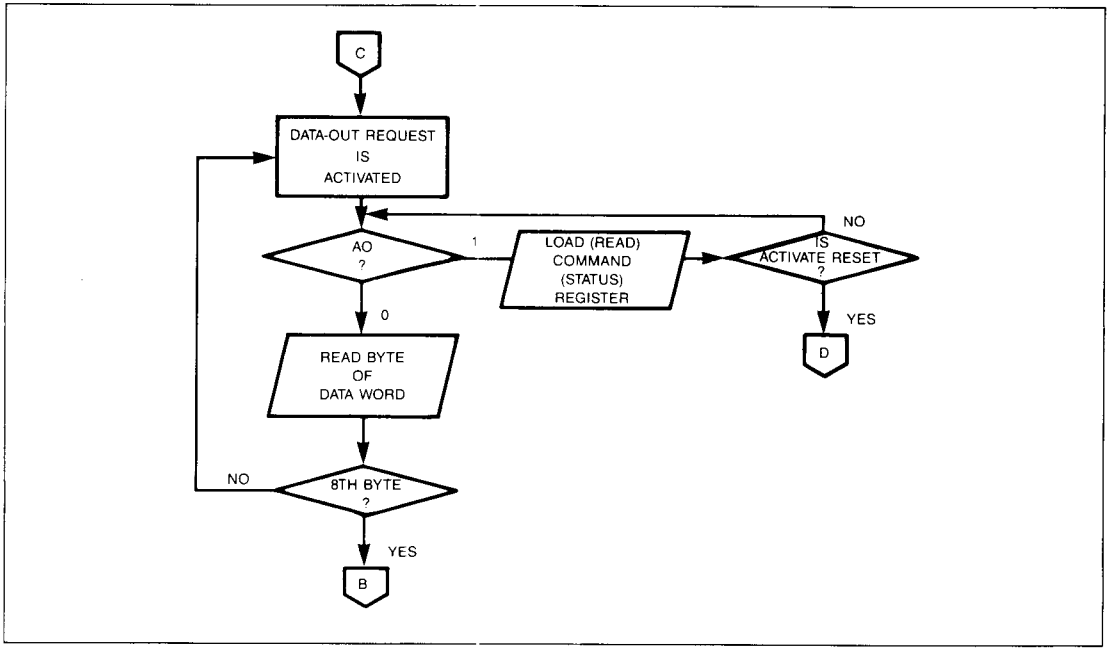


FIGURE 8. ACTIVATING DOR OUTPUT

WD20C03A ORGANIZATION

The WD20C03A Data Encryption Standard (DES) device consists of eight registers plus the necessary logic to implement Battery Back-up Key, two ciphering options, the DES algorithm, and key parity checking.

The eight registers include a 56-bit KEY REGISTER, a 64-bit DATA REGISTER, a 64-bit INITIAL VECTOR REGISTER, a 64-bit TEMP REGISTER, two 8-bit registers for both COMMAND and STATUS, a 56-bit STATIC KEY REGISTER, and a 64-bit STATIC DATA REGISTER.

A block diagram of the WD20C03A is shown in Figure 9.

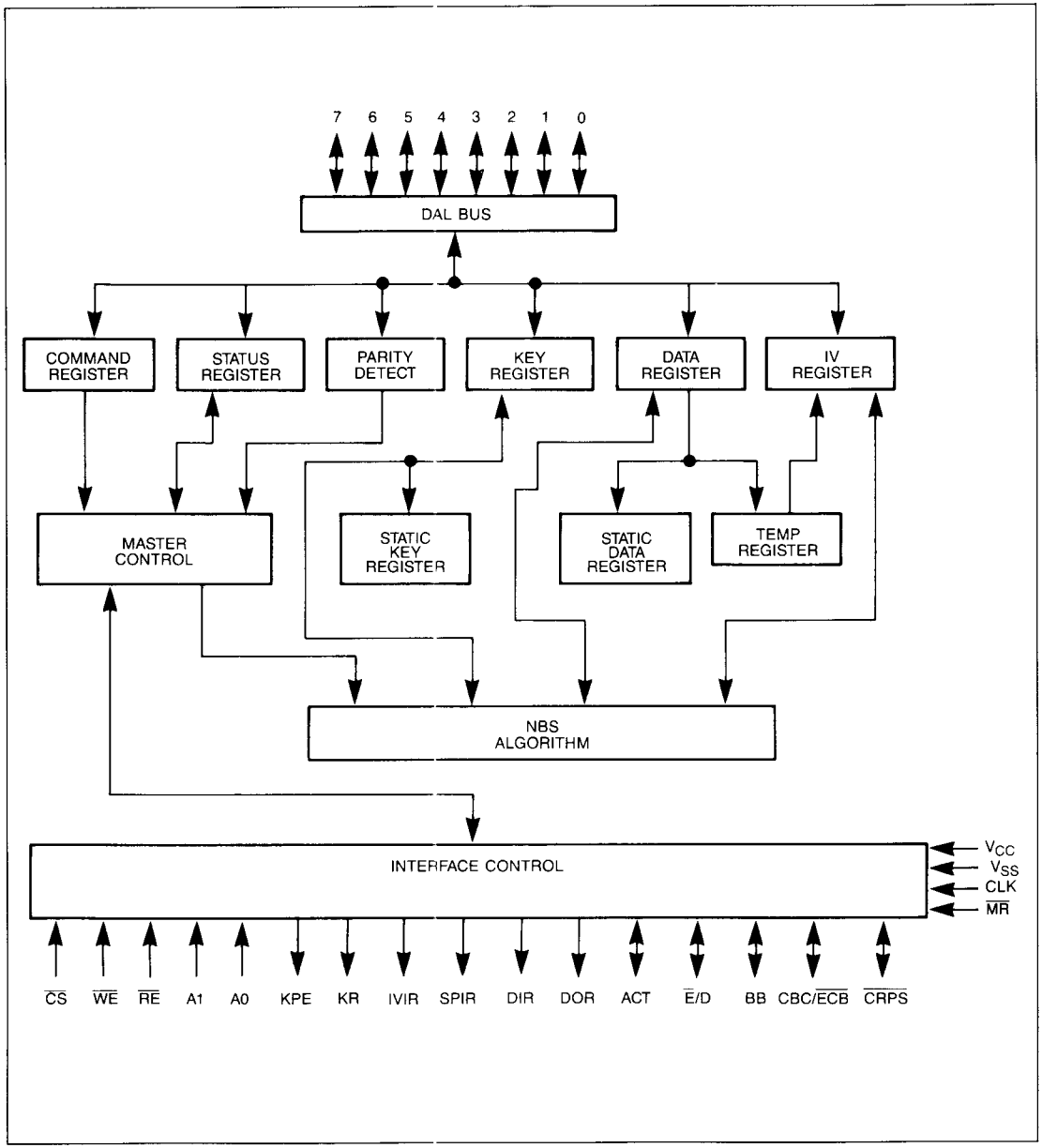


FIGURE 9. WD20C03A BLOCK DIAGRAM

OPERATIONAL OVERVIEW

This section gives an overview of how the WD20C03A functions. More specific detail is described in the section called Operation.

The WD20C03A can be programmed for encryption or decryption using either the Electronic Code Book ($\overline{ECB}$) or Cipher Block Chaining (CBC) modes with or without a Battery Back-up Key. Data is encrypted or decrypted with a 64-bit, user-defined KEY WORD. Data encrypted with a given KEY WORD can be decrypted only using the same KEY WORD.

The KEY REGISTER is loaded by the system with eight successive bytes (8-bit). Parity is checked on each byte of the KEY WORD as it is loaded into the KEY REGISTER. The seventh bit (DAL 0) of each 8-bit byte is reserved for odd parity for that byte and is not used in the algorithm calculation.

In a mode without a Battery Back-up Key, the KEY WORD is requested after each activation and should be loaded into the KEY REGISTER. The STATIC KEY REGISTER and STATIC DATA REGISTER are not used in this mode.

In a mode with a Battery Back-up Key, the KEY WORD is requested only when the user requests a new key by programming the COMMAND REGISTER, or when the KEY WORD stored in the STATIC KEY REGISTER is found no longer valid after power-up key verification. In this mode, the KEY WORD is loaded into the STATIC KEY REGISTER, and a special 64-bit pattern is requested and encrypted by the WD20C03A The encrypted pattern is loaded in the STATIC DATA REGISTER.

During power-down or power failure, the contents of these two STATIC REGISTERS are retained by the battery back-up power. As soon as the power is up again, the contents in the STATIC DATA REGISTER are used to verify and validate the contents in the STATIC KEY REGISTER during the key verification process.

When the WD20C03A is programmed for the Cipher Block Chaining (CBC) mode, the INITIAL VECTOR (IV) is requested by the device after the KEY WORD is loaded into the KEY REGISTER and is ready to be used for encryption or decryption. The INITIAL VECTOR REGISTER is loaded with eight successive bytes (8-bit) of INITIAL VECTOR data at the start of each encryption or decryption process.

To encrypt plain data, the DATA REGISTER is loaded with eight successive bytes (8-bit) of the first plain text block. The contents of the DATA REGISTER are then added (modulo 2) to the contents of the INITIAL VECTOR REGISTER one bit at a time. The modified text is then encrypted to the DES algorithm and the resulting encrypted (cipher) text is loaded into the INITIAL VECTOR REGISTER for the next block of plain text to be modified, ready to be read out. This cycle is repeated until all required data is encrypted.

To decrypt encrypted data, the DATA REGISTER is loaded with eight successive bytes (8-bit) of the first cipher text block. The contents of the DATA REGISTER are loaded into the TEMP REGISTER and at the same time, they are decrypted to the DES algorithm. The resulting text in the DATA REGISTER is added (modulo 2) with the contents of the initial VECTOR REGISTER. The contents of the INITIAL VECTOR REGISTER becomes plain text and are loaded into the DATA REGISTER, ready to be read out. The contents of the TEMP REGISTER are then loaded into the INITIAL VECTOR REGISTER to allow for the next block of cipher text. This cycle is repeated until all required data is decrypted.

When the WD20C03A is programmed for the Electronic Code Book ($\overline{ECB}$) mode, neither the INITIAL VECTOR REGISTER nor the TEMP REGISTER are used. The DATA WORD is requested by the device after the KEY WORD is loaded in the KEY REGISTER and ready to be used for encryption or decryption. In both encryption and decryption, the DATA REGISTER is loaded with eight successive bytes (8-bit) of text, then the contents of the DATA REGISTER go through the DES algorithm calculation. The resulting text in the DATA REGISTER is ready to be read out. It is read by reading eight successive bytes (8-bit).

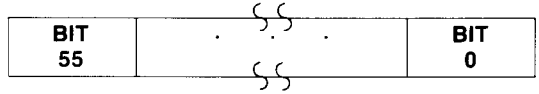
The data transfer into or out of the device's registers (KEY REGISTER, DATA REGISTER, IV REGISTER) through the DAL bus is accomplished by loading or reading out eight successive bytes (8-bit). The data transfer between registers (KEY REGISTER, STATIC KEY REGISTER, DATA REGISTER, STATIC DATA REGISTER, IV REGISTER, TEMP REGISTER) is performed internally and automatically by this device.

REGISTER DESCRIPTION

The following sections describe the registers of the device, which include the KEY, STATIC KEY, DATA, STATIC DATA, IV, TEMP COMMAND, and STATUS REGISTERS.

Key Register

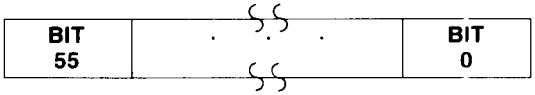
This 56-bit register contains the KEY which is used to encrypt or decrypt the data with the DES algorithm. The KEY REGISTER can be loaded with eight successive bytes only when there is a KEY REQUEST (Status bit and Output). The KEY REGISTER can also be parallel loaded from STATIC KEY REGISTER in Battery Back-up Key mode. This is a WRITE-ONLY REGISTER.



KEY REGISTER
(LOAD ONLY)

Static Key Register

This 56-bit register contains the current KEY for data encryption and decryption using the DES algorithm. The STATIC KEY REGISTER is updated when a new KEY is loaded into the KEY REGISTER and when the device is programmed for Battery Back-up mode. The contents of this register are retained by battery power during power-down or power failure. If the device is programmed for a mode without a Battery Back-up Key, this register is not used. The register is not accessible to the user.

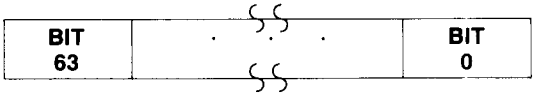


STATIC KEY REGISTER

Data Register

This 64-bit register contains the plain or cipher text either to be read out or that has been loaded in. During encryption, the DATA REGISTER is loaded with plain text and contains cipher text to be read out. During decryption, the DATA REGISTER is loaded with cipher text and contains plain text to be read out. The DATA REGISTER is always read or loaded with eight successive bytes (8-bit).

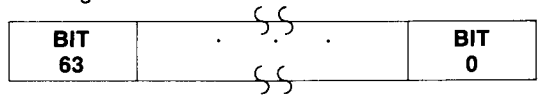
The DATA REGISTER can only be loaded when there is a DATA-IN REQUEST or SPECIAL PATTERN-IN REQUEST (Status bit and Output). Similarly, the DATA REGISTER can only be read when there is a DATA-OUT REQUEST (Status bit and Output). However, when the device is programmed for a mode with Battery Back-up, the contents of this register can be parallel loaded into the STATIC DATA REGISTER when the special pattern for key verification is encrypted.



DATA REGISTER

Static Data Register

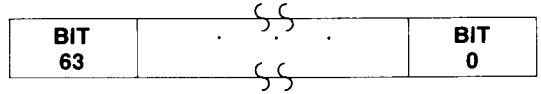
This 64-bit register contains the encrypted special pattern for key verification. When the device is programmed for a mode with a Battery Back-up, the STATIC DATA REGISTER is updated whenever a new key is loaded in. The special pattern is loaded in the DATA REGISTER and encrypted by the new key, then the new encrypted special pattern is loaded into the STATIC DATA REGISTER. The contents of this register are retained by battery power during power-down or power failure. If the device is programmed for a mode without a Battery Back-up Key, the register is not used. This register is not accessible to the user.



STATIC DATA REGISTER

IV Register

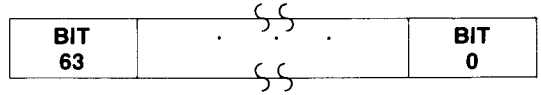
This 64-bit register contains the initial vector or cipher text for the Cipher Block Chaining mode. This register is first loaded with the eight successive bytes (8-bit) of the INITIAL VECTOR REGISTER for the first block of plain or cipher text. After the current text in the DATA REGISTER (plain or cipher) has been processed (encrypted or decrypted), this register will be loaded with the current cipher text from the DATA REGISTER (encrypt) or the next block of text from the TEMP REGISTER (decrypt). This register is not used in the Electronic Code Book mode.



IV REGISTER

Temp Register

This 64-bit register is a temporary storage place used in the Cipher Block Chaining mode. This register temporarily stores the current cipher text, before this text is loaded into the IV REGISTER during the decryption process. This register is loaded with the eight bytes of cipher text from the DATA REGISTER. This register is not used in the Electronic Code Book mode and is not accessible to the user.



TEMP REGISTER

Command Register

This 8-bit register controls the operation of the WD20C03A and can be read or loaded by the user. It is normally loaded only once for an entire encryption or decryption process.

0	1	2	3	4	5	6	7
N/O	ACT	KEOE	$\overline{E}$/D	N/U	BB	NK	CBC/$\overline{ECB}$

TABLE 3. COMMAND REGISTER

BIT	NAME	FUNCTION
0	NEW/OLD (N/O)	When a logic 0, the DES chip is backward compatible with the WD2001 chip in both hardware and software. When a logic 1, the DES chip is in the WD20C03A mode.
1	ACTIVATE (ACT)	This bit must be a logic 1 for encrypt/decrypt operation. When this bit is set from a logic 0 to a logic 1, one of the following events will happen: (1) Initiates loading the KEY REGISTER in non-battery back-up key mode. (2) Initiates loading the KEY REGISTER in Battery Back-up Key mode while NK (command bit) is a logic 1. (3) Initiates SPECIAL PATTERN-IN REQUEST in Battery Back-up Key mode while NK = 0 and KV (status bit) is a logic 1. (4) Initiates a DATA-IN REQUEST in Battery Back-up Key mode while NK = 0, KV = 0, and CBC/$\overline{\text{ECB}}$ (command bit) is a logic 0. (5) Initiates an INITIAL VECTOR-IN REQUEST in Battery Back-up Key mode while NK = 0, KV = 0 and CBC/$\overline{\text{ECB}}$ = 1.
2	KEY ERROR OUTPUT ENABLE (KEOE)	When a logic 0, the $\overline{\text{KEY PARITY ERROR}}$ output pin ($\overline{\text{KPE}}$) remains inactive regardless of the status of the $\overline{\text{KEY PARITY ERROR}}$ bit (status bit 2). When a logic 1, the $\overline{\text{KEY PARITY ERROR}}$ output pin is active when the KPE bit (status bit 2) is a logic 1. This bit is set to a logic 1 upon a $\overline{\text{MASTER RESET}}$.
3	$\overline{\text{ENCRYPT}}$/DECRYPT ($\overline{\text{E}}$/D)	When a logic 0, data is to be encrypted. When a logic 1, data is to be decrypted.
4	NOT USED	
5	BATTERY BACK-UP KEY (BB)	When a logic 0, the DES chip is in non-battery back-up key mode. When a logic 1, the DES chip is in Battery Back-up Key mode.
6	NEW KEY REQUEST (NK)	This bit is ignored in non-battery back-up key mode. While in Battery Back-up Key mode, a KEY REQUEST is initiated when NK = 1, or the chip will skip the key loading process and do either the Cipher Block Chaining process or the electronic code process when NK = 0.
7	$\overline{\text{CIPHER BLOCK CHAINING}}$/$\overline{\text{ELECTRONIC CODE BOOK}}$ (CBC/$\overline{\text{ECB}}$)	When a logic 0, the DES chip will encrypt/decrypt data using the electronic code book method. When a logic 1, the DES chip will encrypt/decrypt data using the Cipher Block Chaining method.

NOTE: All bits of the COMMAND REGISTER are reset to a logic 0 upon $\overline{\text{MASTER RESET}}$, except bit 4 (N/U), bit 3 ($\overline{\text{KEOE}}$) and bit 0 (N/O) which will be set to 1. When $\overline{\text{CRPS}}$ = 0 this register is disregarded after $\overline{\text{MASTER RESET}}$.

Status Register

This 8-bit register monitors the status of the device. THIS IS A READ-ONLY REGISTER.

0	1	2	3	4	5	6	7
KV	RLK	SPIR	IVIR	KR	KPE	DIR	DOR

STATUS REGISTER (READ-ONLY)

TABLE 4. STATUS REGISTER

BIT	NAME	FUNCTION
0	KEY VERIFICATION REQUEST (KV)	If the $\overline{CRPS}$ pin is a logic 1, this bit is set each time the N/O bit of the COMMAND REGISTER is set from a logic 0 to a logic 1. If the $\overline{CRPS}$ pin is a logic 0 and N/O is a logic 0, this bit is set upon each $\overline{MASTER\ RESET}$. It is reset at the end of the KEY VERIFICATION process while the KEY is found valid or at the end of the KEY RE-LOADING process.
1	RELOAD KEY REQUEST (RLK)	This bit is set when the user requests a new KEY (NK = 1) in Battery Back-up Key mode (BB = 1) or at the end of the KEY VERIFICATION process when the KEY is found not valid. When this bit is set, the KEY RE-LOADING process will start. This bit is reset at the end of the KEY RE-LOADING process. The reset occurs when the encrypted SPECIAL PATTERN (encrypted by the new loaded KEY) is loaded into the STATIC DATA REGISTER from the DATA REGISTER.
2	SPECIAL PATTERN-IN REQUEST (SPIR)	This bit is set to a logic 1 when the ACT bit is programmed from a logic 0 to a logic 1, BB = 1, NK = 0, and KV = 1, or, when KR is reset from a logic 1 to a logic 0 and RLK = 1. It is reset upon the loading of the last (8th) byte of the SPECIAL PATTERN into the DATA REGISTER.
3	INITIAL VECTOR-IN REQUEST (IVIR)	This bit is set to a logic 1 upon one of the following conditions: (1) Completion of KEY REGISTER loading while BB = 0 and CBC/$\overline{ECB}$ = 1. (2) Completion of KEY RE-LOADING process while BB = 1 and CBC/$\overline{ECB}$ = 1. (3) Completion of KEY VERIFICATION process and the KEY being found valid while BB = 1 and CBC/$\overline{ECB}$ = 1. (4) The ACT bit is programmed a logic 0 to a logic 1 while BB = 1, NK = 0, KV = 0 and CBC/$\overline{ECB}$ = 1. This bit is reset upon loading of the last (8th) byte of the INITIAL VECTOR.
4	KEY REQUEST (KR)	This bit is set to a logic 1 when ACT is programmed from a logic 0 to a logic 1 and BB = 0 or, when RLK is set internally from a logic 0 to a logic 1. It is reset upon loading of the last (8th) byte of the KEY REGISTER.
5	KEY PARITY ERROR (KPE)	This bit is set internally upon detection of a parity error during loading of the KEY REGISTER. It is reset when ACT is programmed from a logic 1 to a logic 0 (i.e., the chip is deactivated).
6	DATA-IN REQUEST (DIR)	Ths bit is set to a logic 1 upon one of the following conditions: (1) Completion of KEY REGISTER loading while BB = 0 and CBC/$\overline{ECB}$ = 0. (2) Completion of the KEY RE-LOADING process while BB = 1 and CBC/$\overline{ECB}$ = 0. (3) Completion of the KEY VERIFICATION process and the KEY being found valid while BB = 1 and CBC/$\overline{ECB}$ = 0. (4) The ACT bit is programmed from a logic 0 to a logic 1 while BB = 1, NK = 0, KV = 0 and CBC/$\overline{ECB}$ = 0. (5) Completion of IV REGISTER loading while BB = 1 and CBC/$\overline{ECB}$ = 1.

TABLE 4. STATUS REGISTER (continued)

BIT	NAME	FUNCTION
6 (cont.)	DATA-IN REQUEST (DIR) (cont.)	(6) Completion of DATA REGISTER reading (i.e., the last DATA-OUT REQUEST has been serviced by an 8-byte read and the DATA REGISTER is now empty and ready to be loaded with the next DATA WORD). This bit is reset upon loading of the last (8th) byte of the DATA REGISTER.
7	DATA-OUT REQUEST (DOR)	This bit is set upon completion of the internal encrypt/decrypt calculation of a DATA WORD. It is reset upon reading the last (8th) byte of the DATA REGISTER.

NOTE: Upon $\overline{\text{MASTER RESET}}$, all bits of the STATUS REGISTER are reset to a logic 0 when $\overline{\text{CRPS}}$ is a logic 1. When $\overline{\text{CRPS}}$ = 0 and N/O = 0, all bits are reset to 0 except KV (bit 0) which is set to a logic 1.

OPERATION

This section explains how the WD20C03A operates.

For backward compatibility with the functions of the WD2001 (ECB only), Bit 0 (N/O) in the COMMAND REGISTER is used to control whether the WD20C03A is in the WD2001 mode ($\overline{\text{ECB}}$) or in the WD20C03A mode (ECB or CBC).

When the N/O bit is programmed to a logic 0, the device is in the WD2001 mode (ECB) and only the COMMAND/STATUS, DATA, and KEY REGISTERS are then available. The pinouts and the operation of the device and the functions of the three registers in this mode are exactly the same as in the WD2001. V_{DD} (12V) can still be connected to pin six when the WD20C03A is in the WD2001 mode.

When the N/O bit is programmed to a logic 1, the device is in the WD20C03A mode ($\overline{\text{ECB}}$ or CBC), that is, the WD20C03A can be selected to operate in one of the following four modes:

(a) Electronic Code Book mode without a Battery Back-up Key
(b) Cipher Block Chaining mode without a Battery Back-up Key
(c) Electronic Code Book mode with a Battery Back-up Key
(d) Cipher Block Chaining mode with a Battery Back-up Key

Each mode operates as follows:

(a) Electronic Code Book mode without a Battery Back-up Key

The WD20C03A will operate in this mode when Bit 5 (BB), and Bit 7 (CBC/$\overline{\text{ECB}}$) in the COMMAND REGISTER are set to a logic 0. After the device is selected to be in this mode, it will be initiated by setting Bit 1 (ACT) in the COMMAND REGISTER to a logic 1. The WD20C03A will respond by activating the KEY REQUEST (KR, pin 26) output.

A0 must be deactivated (to allow the WD20C03A to internally address the KEY REGISTER) before loading the 64-bit KEY WORD into the KEY REGISTER. The KEY REGISTER is loaded with eight successive bytes (8-bit) by activating $\overline{\text{WE}}$ eight times (with $\overline{\text{CS}}$ active).

When $\overline{\text{WE}}$ is activated, the WD20C03A deactivates the KEY REQUEST (KR) output. When $\overline{\text{WE}}$ is deactivated, the WD20C03A activates the KR output. The WD20C03A will activate eight KEY REQUESTS to fill up the KEY REGISTER.

$\overline{\text{CS}}$	A0	A1	$\overline{\text{CRPS}}$	REGISTER
0	1	1	1	Status
0	1	0	1	Command
0	0	X	1	Key

X = Don't care

FIGURE 10. WD20C03A REGISTER SELECT

The KR output can either be used for asynchronous handshaking (as in DMA control) or, after the first activated KR, further activations can be ignored and the KEY REGISTER can be loaded synchronously (as in programmed I/O) by eight successive activations of $\overline{\text{WE}}$.

Each byte of the KEY WORD is checked for odd parity when it is loaded into the KEY REGISTER. If a parity error is detected, the WD20C03A will set Bit 5 ($\overline{\text{KPE}}$, $\overline{\text{KEY PARITY ERROR}}$) in the STATUS REGISTER to a logic 1. If Bit 2 (KEOE, KEY ERROR OUTPUT ENABLE) in the COMMAND REGISTER has been set, the device will also activate the $\overline{\text{KPE}}$ (pin 22) output. Bit 5 ($\overline{\text{KPE}}$, $\overline{\text{KEY PARITY ERROR}}$) in the STATUS REGISTER will be reset to a logic 0 when Bit 1 (ACT, ACTIVATE) in the COMMAND REGISTER is reset to a logic 0.

After loading the eighth (last) byte of the KEY WORD into the KEY REGISTER, the WD20C03A will set Bit 6 (DIR, DATA-IN REQUEST) in the STATUS REGISTER and activate the DATA-IN REQUEST (DIR, pin 27) output. The 64-bit DATA WORD should then be loaded into the DATA REGISTER, which will be loaded in the same manner as the KEY REGISTER by eight successive activations of DATA-IN REQUEST (DIR, pin 27) output and $\overline{WE}$ input.

After the eighth (last) byte of the DATA WORD has been loaded, the WD20C03A starts its operation internally by encrypting or decrypting the data to the DES algorithm. Upon completion of this operation, the encrypted or decrypted data is internally loaded into the DATA REGISTER, the WD20C03A will set Bit 7 (DOR, DATA-OUT REQUEST) in the STATUS REGISTER and will activate the DATA-OUT REQUEST (DOR, pin 28) output.

The DATA WORD must then be read from the DATA REGISTER in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST (DOR, pin 28) output and $\overline{RE}$ input.

As previously explained, after the first request, further activations of the DIR and DOR outputs can be ignored and the DATA REGISTER can be loaded or read by eight successive activations of $\overline{WE}$ or $\overline{RE}$.

After the eighth (last) byte of the DATA REGISTER has been read, the WD20C03A will reactivate the DATA-IN REQUEST. The cycle of loading the DATA REGISTER, encrypting or decrypting of the data to the DES algorithm, and reading the new data from the DATA REGISTER is repeated until all the required data has been encrypted or decrypted with the current KEY WORD.

When this is completed, Bit 1 (ACT, ACTIVATE) in the COMMAND/STATUS REGISTER should be reset to a logic 0 to lock the last KEY WORD loaded into the WD20C03A. This prevents the access and use of it by an unauthorized user. To resume operation, the ACTIVATE bit must be reset to a logic 1. This activates the KEY REQUEST and a new KEY must be loaded before access to the DATA REGISTER is possible.

To encrypt plain data, it is loaded into the DATA REGISTER, and then encrypted data is read from the DATA REGISTER after Bit 3 ($\overline{ENCRYPT}$/DECRYPT) in the COMMAND REGISTER has been set to a logic 0.

To decrypt encrypted data, it is loaded into the DATA REGISTER, and then plain data is read from the DATA REGISTER after Bit 3 ($\overline{ENCRYPT}$/DECRYPT) in the COMMAND REGISTER has been set to a logic 1.

NOTE: To accomplish switching from encryption to decryption (or vice versa) with the same KEY WORD before a DATA WORD transfer is initiated, A0 must be set to 1 and A1 to 0. The WD20C03A will then override the internal addressing of the DATA REGISTER and address the COMMAND REGISTER, which now can be reprogrammed. When A0 is deactivated, the device will then internally address the DATA REGISTER, while awaiting the loading of the next DATA WORD.

(b) Cipher Block Chaining mode without a Battery Back-up Key

The WD20C03A will operate in this mode when Bit 5 (BB) and Bit 7 (CBC/EBC) in the COMMAND REGISTER are set respectively to a logic 0 and a logic 1. Once the device is programmed in this mode, it can be initiated by setting Bit 1 (ACT) in the COMMAND REGISTER to a logic 1. The WD20C03A DES will now respond by activating the KEY REQUEST (KR) output. Refer to Figure 10 for register selection.

A0 must be deactivated (to address the KEY REGISTER internally), and the KEY REGISTER must be loaded with the 64-bit KEY WORD in the same manner as performed in the Electronic Code Book mode without a Battery Back-up Key.

When the eighth (last) byte of the KEY WORD is loaded in the KEY REGISTER, the WD20C03A will set Bit 3 (IV-IN REQUEST) in the STATUS REGISTER and will activate the IV-IN REQUEST (IVIR) output. The 64-bit INITIAL VECTOR WORD must then be loaded into the IV REGISTER in the same manner as the KEY REGISTER was loaded, that is, by eight successive activations of IV-IN REQUEST output and $\overline{WE}$ input.

After the eighth (last) byte of the INITIAL VECTOR WORD has been loaded, the WD20C03A will set Bit 6 (DATA-IN REQUEST) in the STATUS REGISTER and will activate the DATA-IN REQUEST (DIR) output. The 64-bit DATA WORD must then be loaded into the DATA REGISTER in the same manner as the KEY REGISTER was loaded, that is, by eight successive activations of DATA-IN REQUEST output and WE input.

The plain text is loaded into the DATA REGISTER when the $\overline{ENCRYPT}$/DECRYPT bit has been set to a logic 0. When this is completed, that is, after the eighth (last) byte of the plain DATA WORD has been loaded into the device, the contents of the IV REGISTER will be added to the plain text consecutively bit by bit with modulo 2 arithmetic and the WD20C03A will begin the internal calculation of the DES algorithm for the cipher text.

When completed, this data is not only loaded into the DATA REGISTER but also into the IV REGISTER to override the original INITIAL VECTOR WORD. After (parallel) loading the new data in these two REGISTERS, the WD20C03A will set Bit 7 (DATA-OUT REQUEST) in the STATUS REGISTER and will activate the DATA-OUT REQUEST (DOR) output.

The new cipher DATA WORD must then be read from the DATA REGISTER in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST output and $\overline{RE}$ input.

After the eighth (last) byte of the DATA REGISTER contents have been read, the WD20C03A will reactivate the DATA-IN REQUEST and the next cycle can begin. This will continue until all required (plain) data has been encrypted with the current KEY WORD in the manner previously described, that is, by:

(1) loading the DATA REGISTER with plain text
(2) adding the (previous) cipher text contents of the IV REGISTER to the contents of the DATA REGISTER
(3) calculating the DES algorithm for cipher text
(4) loading it into the IV REGISTER for operation (addition) to the 64-bit (plain) DATA WORD
(5) reading it (cipher text) from the DATA REGISTER.

When decrypting, Bits 1 (ACT) and Bit 3 ($\overline{\text{ENCRYPT}}$/DECRYPT) in the COMMAND REGISTER are set to 1 respectively. This will activate the KEY REQUEST output indicating that the original key must now be loaded into the KEY REGISTER. After the key is loaded, the WD20C03A will request that the initial vector be loaded into the IV REGISTER. When this is completed, the data request input pin will be activated and the first eight bytes of cipher data need to be loaded into the DATA REGISTER. When this is completed, that is, after the eight bytes of the cipher DATA WORD have been loaded into the device, the contents of the DATA REGISTER will be transferred into the TEMP REGISTER and the WD20C03A will begin the internal calculation of the DES algorithm for the clear data.

When completed, this data is added consecutively bit by bit to the contents of the IV REGISTER using modulo 2 arithmetic. The modified plain text data is then loaded into the DATA REGISTER while the contents of the TEMP REGISTER are loaded into the IV REGISTER, overriding the existing INITIAL VECTOR.

After completion of these operations, Bit 7 (DATA-OUT REQUEST) in the STATUS REGISTER will be set and the DATA-OUT REQUEST (DOR) output will be activated. The plain DATA WORD must then be read from the DATA REGISTER in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST output and $\overline{\text{RE}}$ input.

After the eighth (last) byte of the DATA REGISTER contents have been read, the WD20C03A will reactivate the DATA-IN REQUEST and the next cycle can begin. This will continue until all required (cipher) data has been decrypted with the current KEY WORD in the manner previously described, that is, by:

(1) loading the DATA REGISTER with cipher text
(2) loading the contents of the DATA REGISTER into the TEMP REGISTER
(3) calculating the DES algorithm for clear text
(4) adding the clear text contents in the TEMP REGISTER to the (previous) cipher text contents in the IV REGISTER
(5) loading plain text into the DATA REGISTER
(6) transferring the contents of the TEMP REGISTER to the IV REGISTER for the next 64-bit cipher DATA WORD
(7) reading it (plain text) from the DATA REGISTER.

As previously explained, for DATA-IN, IV-IN, and DATA-OUT, after the first request, further activations of the DIR, IVIR, and DOR outputs are not necessary. Loading the IV REGISTER and the DATA REGISTER is performed by eight successive activations of $\overline{\text{WE}}$ and reading the DATA REGISTER is performed by eight successive activations of $\overline{\text{RE}}$.

When all required data has been encrypted or decrypted with the current KEY WORD, Bit 1 (ACTIVATE) in the COMMAND REGISTER should be programmed to logic 0 to lock the last KEY loaded into the WD20C03A. This prevents the access and use of it by an unauthorized user. To resume operation, the ACTIVATE bit must be programmed to logic 1. This activates the KEY REQUEST and a new KEY must be loaded before access to the DATA REGISTER is possible.

NOTE: At the end of each encrypted or decrypted file (or message), the WD20C03A is waiting for the DATA WORD, not for the reloading of the INITIAL VECTOR: that is, DIR output is active. In order to activate the IVIR output and re-load the INITIAL VECTOR, the device has to be re-started. This can be accomplished by deactivating the WD20C03A and then reactivating it once more. This forces the re-loading of the KEY WORD. This procedure should be followed even when it is desired to use the same KEY WORD for the encryption or decryption of the next file (or message).

(c) Electronic Code Book mode with a Battery Back-up Key

The WD20C03A will operate in this mode when Bit 5 (BB) and Bit 7 (CBC/ECB) in the COMMAND REGISTER are set respectively to logic 1 and logic 0. After the device is programmed to be in this mode, it will be initiated by setting Bit 1 (ACT) in the COMMAND REGISTER to a logic 1. The WD20C03A will respond in one of the following ways:

(1) When Bit 6 (NK, NEW KEY) in the COMMAND REGISTER is set to a logic 1, the WD20C03A will respond by setting Bit 1 (RLK, RE-LOAD KEY) and Bit 4 (KR, KEY REQUEST) in the STATUS REGISTER. The device will also reactivate the KEY REQUEST (pin 26) output and it will now be in the KEY RE-LOADING state.

A0 needs to be deactivated to allow the WD20C03A to select the KEY REGISTER internally and to load it with the 64-bit KEY WORD in same manner as in the Electronic Code Book mode without a Battery Back-up Key. Refer to Figure 10 for register selection.

When the eighth (last) byte of the KEY WORD has been loaded into the KEY REGISTER, its contents will then be transferred to the STATIC KEY REGISTER and Bit 2 (SPECIAL PATTERN-IN REQUEST) in the STATUS REGISTER is set and the SPECIAL PATTERN-IN REQUEST (SPIR, pin 4) output is activated.

The 64-bit SPECIAL PATTERN must now be loaded into the DATA REGISTER in the same manner as the KEY REGISTER, that is, by eight successive activations of SPECIAL PATTERN-IN REQUEST input and $\overline{WE}$ input.

When the eighth (last) byte of the SPECIAL PATTERN has been loaded into the DATA REGISTER, the device will start to encrypt the SPECIAL PATTERN WORD in Electronic Code Book mode. Upon completion of the DES algorithm calculation, the cipher data will then be loaded into the STATIC DATA REGISTER, and the WD20C03A will reset Bit 1 (RE-LOAD KEY) and Bit 0 (KEY VERIFICATION) in the STATUS REGISTER. The device will now be out of the KEY RE-LOADING state and will continue in Electronic Code Book mode by setting Bit 6 (DATA-IN REQUEST) in the STATUS REGISTER and activating the DATA-IN REQUEST (DIR, pin 27) output.

(2) When Bit 6 (NEW KEY) in the COMMAND REGISTER is set to logic 0 and Bit 0 (KEY VERIFICATION) in the STATUS REGISTER is set to logic 1, the WD20C03A will respond by setting Bit 2 (SPECIAL PATTERN-IN) in the STATUS REGISTER. The device will also activate the SPECIAL PATTERN-IN (SPIR) output, load the contents of the STATIC KEY REGISTER into the KEY REGISTER in order to encrypt the SPECIAL PATTERN, and will now be in the KEY VERIFICATION state.

A0 must be deactivated (to allow the WD20C03A to address the DATA REGISTER internally) and the DATA REGISTER must be loaded with the 64-bit SPECIAL PATTERN WORD in the same manner as the KEY REGISTER was loaded, that is, by eight successive activations of SPECIAL PATTERN-IN REQUEST output and $\overline{WE}$ input.

When the eighth (last) byte of the SPECIAL PATTERN has been loaded into the DATA REGISTER, the WD20C03A will start to encrypt and the SPECIAL PATTERN WORD in the Electronic Code Book mode. Upon the completion of the DES algorithm calculation, the cipher data will be compared with the contents of the STATIC DATA REGISTER.

If they are not the same, the WD20C03A will set Bit 1 (RE-LOAD KEY) and Bit 4 (KEY REQUEST) in the STATUS REGISTER and will activate the KEY REQUEST (pin 26) output to start the KEY RE-LOADING process as was previously described (see C-1). Upon the completion of the KEY RE-LOADING operation, the device will set Bit 6 (DATA-IN REQUEST) in the STATUS REGISTER and activate the DATA-IN REQUEST (DIR, pin 27) output to start the Electronic Code Book mode.

If the new cipher data and the contents of the STATIC DATA REGISTER are the same, the WD20C03A will reset Bit 0 (KEY VERIFICATION), set Bit 6 (DATA-IN REQUEST) in the STATUS REGISTER, and activate the DATA-IN REQUEST (DIR, pin 27) output to start the Electronic Code Book mode.

(3) When Bit 6 (NEW KEY) in the COMMAND REGISTER is set to a logic 0 and Bit 0 (KEY VERIFICATION) in the STATUS REGISTER is set to a logic 0, the WD20C03A will load the contents of the STATIC KEY REGISTER into the KEY REGISTER, set Bit 6 (DATA-IN REQUEST) in the STATUS REGISTER, and activate the DATA-IN REQUEST (DIR, pin 27) output to start the Electronic Code Book mode. The operation is the same as previously described in the Electronic Code Book mode without a Battery Back-up Key.

NOTE: To accomplish switching from encryption to decryption (or vice versa) without deactivating the WD20C03A, and before a DATA WORD transfer is initiated, A0 must be set to 1 and A1 to 0 to address COMMAND REGISTER and override the addressing of the DATA REGISTER internally. The COMMAND REGISTER can now be re-programmed. When A0 is reset to a logic 0, the WD20C03A will now address the DATA REGISTER internally while awaiting the loading of the next DATA WORD.

(d) Cipher Block Chaining mode with a Battery Back-up Key

The WD20C03A will operate in this mode when Bit 5 (BB) and Bit 7 (CBC/$\overline{ECB}$) in the COMMAND REGISTER are set to a logic 1. After the device is selected to be in this mode, it will be initiated by setting Bit 1 (ACT) in the COMMAND REGISTER to a logic 1.

The WD20C03A will respond in one of the three ways previously described in Section C (Electronic Code Book with a Battery Back-up Key mode). However, after completion of the KEY RE-LOAD or KEY VERIFICATION operations, the device will start operating in the Cipher Block Chaining mode instead of the Electronic Code Book mode. It will set Bit 3 (INITIAL VECTOR-IN REQUEST) in the STATUS REGISTER and will activate the INITIAL VECTOR-IN REQUEST (IVIR, pin 3) output.

When the WD20C03A is in the Cipher Block Chaining mode, its operation is the same as previously described in the Cipher Block Chaining mode without a Battery Back-up Key.

NOTE: At the end of each encrypted or decrypted file (or message), the WD20C03A is waiting for the DATA WORD, not for the reloading of the INITIAL VECTOR; that is, DIR output is active. In order to activate the IVIR output and re-load the INITIAL VECTOR, the device has to be re-started. This can be accomplished by deactivating the WD20C03A and then reactivating it once more. This forces the re-loading of the KEY WORD. This procedure should be

followed even when it is desired to use the same KEY WORD for the encryption or decryption of the next file (or message.)

COMMAND SELECT OPTION

The WD20C03A can be programmed through the DAL bus lines or through the input pins. When the COMMAND REGISTER PIN SELECT ($\overline{CRPS}$, pin 20) input is set to a logic 0, the O/N, ACT, $\overline{E}$/D, NK, BB, and CBC/$\overline{ECB}$ pins are enabled as inputs and they will override bits 0, 1, 3, 5, 6, and 7 in the COMMAND REGISTER. This override allows input pins to control the WD20C03A. Bit 2 (KEOE) in the COMMAND REGISTER will remain a logic 1.

The A1 and A0 bits will be disregarded in this option, and the COMMAND and STATUS REGISTERS cannot be accessed using the DAL bus lines.

Note that the ACT pin must be toggled from a logic 1 to a logic 0 to clear a parity error detection when operating in this mode.

All other operations remain the same as described previously.

NOTE: Upon $\overline{MASTER\ RESET}$, while $\overline{CRPS}$ and N/O pins are a logic 0, the WD20C03A will not return to the 2001 mode, but will stay in the WD20C03 mode and Bit 0 (KV) in the STATUS REGISTER will be set.

TABLE 5. MAXIMUM RATINGS FOR WD2001/2002/20C03A

V_{DD} with respect to V_{SS} (Ground) ..... +15 to −0.3V
Maximum voltage to any input pin with respect to V_{SS} ..... +15 to −0.3V
Operating Temperature ..... 0°C (32°F) to 70°C (158°F)
Power Dissipation ..... 1 Watt

STORAGE TEMPERATURE

Plastic ..... −55°C (−67°F) to 125°C (257°F)
Ceramic ..... −65°C (−85°F) to 150°C (302°F)

NOTE

Maximum limits indicate where permanent device damage occurs. Continuous operation at these limits is not intended and should be limited to those conditions specified in the DC Electrical Characteristics.

TABLE 6. DC OPERATING CHARACTERISTICS

T_A = 0°C (32°F) to 70°C (158°F), V_{DD} = 12V ±.6V, V_{CC} = +5V ± .25V, V_{SS} = 0V

SYMBOL	CHARACTERISTIC	MIN	MAX	UNIT	CONDITION
*I_{LI}	Input Leakage		10	μA	V_{IN} = V_{DD}
**I_{LL}	Input Low Current		1.6	mA	V_{IN} = V_{SS}
I_{OL}	Data Bus Leakage		±10	μA	V_{OUT} = V_{CC} or V_{SS}
IC_{CAVE}	V_{CC} Supply Current		100 15	mA mA	WD2001/2002 WD20C03A
ID_{DAVE}	V_{DD} Supply Current		25	μA	
V_{IH}	Voltage Input High	2.4		V	
V_{IL}	Voltage Input Low (all inputs)		0.8	V	
V_{OH}	Voltage Output High	2.8		V	I_{OH} = −100μA
V_{OL}	Voltage Output Low		0.4	V	I_{OL} = 1.6mA

*I_{LI} applies only to inputs without pull-up resistors.
**I_{IL} applies only to inputs with pull-up resistors.

TABLE 7. AC OPERATING CHARACTERISTICS WD2001/2002-05 500KHz CLOCK

T_A = 0°C (32°F) to 70°C (158°F), V_{DD} = +12V ±.6V, V_{CC} = +5V ±.25V, V_{SS} = 0V

SYMBOL	CHARACTERISTIC	MIN	MAX	UNIT	CONDITION
	READ				
TACS	A0, $\overline{CS}$, Setup to $\overline{RE}\downarrow$	100		nsec	
TRDV	$\overline{RE}\downarrow$ to DAL (CDP) Valid		500	nsec	CLOAD = 50pf
TRD	$\overline{RE}$ Pulse Width	500		nsec	
TDF	$\overline{RE}\uparrow$ to DAL Float	50	250	nsec	
TACH	A0, $\overline{CS}$ Hold from $\overline{RE}\uparrow$	0		nsec	
	WRITE				
TACS	A0, $\overline{CS}$ Setup to $\overline{WE}\downarrow$	100		nsec	
TDVW	DAL (CDP) Setup to $\overline{WE}\uparrow$	300		nsec	
TRW	$\overline{WE}$ Pulse Width	300		nsec	
TDH	DAL (CDP) Hold from $\overline{WE}\uparrow$	90		nsec	
TACH	A0, $\overline{CS}$ Hold from $\overline{WE}\uparrow$	0		nsec	
	HANDSHAKE				
TD	KR(DIR)$\downarrow$ $\overline{KA}(\overline{DIA})\downarrow$ from $\overline{WE}\downarrow$		700	nsec	CLOAD = 50pf
	KR(DIR)$\uparrow$ $\overline{KA}(\overline{DIA})\uparrow$ from $\overline{WE}\uparrow$				
	DOR$\downarrow$ $\overline{DOA}\downarrow$ from $\overline{RE}\downarrow$				
	DOR$\uparrow$ $\overline{DOA}\uparrow$ from $\overline{RE}\uparrow$				

NOTE: All output timing specifications reflect the following:
High Output 2.0V
Low Output 0.8V

TABLE 8. AC OPERATING CHARACTERISTICS WD2001/2002-20 2MHz CLOCK

T_A = 0°C (32°F) to 70°C (158°F), V_{DD} = +12V ±.6V, V_{CC} = +5V ±.25V, V_{SS} = 0V

SYMBOL	CHARACTERISTIC	MIN	MAX	UNIT	CONDITION
	READ				
TACS	A0, $\overline{CS}$, Setup to $\overline{RE}\downarrow$	80		nsec	
TRDV	$\overline{RE}\downarrow$ to DAL (CDP) Valid		330	nsec	CLOAD = 50pf
TRD	$\overline{RE}$ Pulse Width	330		nsec	
TDF	$\overline{RE}\uparrow$ to DAL Float	30	200	nsec	
TACH	A0, $\overline{CS}$ Hold from $\overline{RE}\uparrow$	0		nsec	
	WRITE				
TACS	A0, $\overline{CS}$ Setup to $\overline{WE}\downarrow$	80		nsec	
TDVW	DAL (CDP) Setup to WE↑	200		nsec	
TRW	WE Pulse Width	200		nsec	
TDH	DAL (CDP) Hold from $\overline{WE}\uparrow$	90		nsec	
TACH	A0, $\overline{CS}$ Hold from $\overline{WE}\uparrow$	0		nsec	
	HANDSHAKE				
TD	KR(DIR)↓ $\overline{KA}(\overline{DIA})\downarrow$ from $\overline{WE}\downarrow$		450	nsec	CLOAD = 50pf
	KR(DIR)↑ $\overline{KA}(\overline{DIA})\uparrow$ from $\overline{WE}\uparrow$				
	DOR↓ $\overline{DOA}\downarrow$ from $\overline{RE}\downarrow$				
	DOR↑ $\overline{DOA}\uparrow$ from $\overline{RE}\uparrow$				

NOTE: All output timing specifications reflect the following:
High Output 2.0V
Low Output 0.8V

TABLE 9. AC OPERATING CHARACTERISTICS WD2001/2002-30 3MHz CLOCK

T_A = 0°C (32°F) to 70°C (158°F) V_{DD} = +12V ±.6V, V_{CC} = +5V ±.25V, V_{SS} = 0V

SYMBOL	CHARACTERISTIC	MIN	MAX	UNIT	CONDITION
	READ				
TACS	A0, $\overline{CS}$, Setup to $\overline{RE}\downarrow$	50		nsec	
TRDV	$\overline{RE}\downarrow$ to DAL (CDP) Valid		220	nsec	CLOAD = 50pf
TRD	$\overline{RE}$ Pulse Width	300		nsec	
TDF	$\overline{RE}\uparrow$ to DAL Float	20	130	nsec	
TACH	A0, $\overline{CS}$ Hold from $\overline{RE}\uparrow$	0		nsec	
	WRITE				
TACS	A0, $\overline{CS}$ Setup to $\overline{WE}\downarrow$	50		nsec	
TDVW	DAL (CDP) Setup to $\overline{WE}\uparrow$	130		nsec	
TRW	$\overline{WE}$ Pulse Width	175		nsec	
TDH	DAL (CDP) Hold from $\overline{WE}\uparrow$	60		nsec	
TACH	A0, CS Hold from $\overline{WE}\uparrow$	0		nsec	
	HANDSHAKE				
TD	KR(DIR)↓ $\overline{KA(DIA)}\downarrow$ from $\overline{WE}\downarrow$		300	nsec	CLOAD = 50pf
	KR(DIR)↑ $\overline{KA(DIA)}\uparrow$ from $\overline{WE}\uparrow$				
	DOR↓ $\overline{DOA}\downarrow$ from $\overline{RE}\downarrow$				
	DOR↑ $\overline{DOA}\uparrow$ from $\overline{RE}\uparrow$				

NOTE: All output timing specifications reflect the following:
High Output 2.0V
Low Output 0.8V

MISCELLANEOUS TIMING (WD2001/2002 ONLY)

1. CLOCK INPUT.

FREQUENCY MAX.	FREQUENCY MIN.	PULSE WIDTH MIN.
500KHz	100KHz	500nsec
2MHz	100KHz	250nsec
3MHz	100KHz	165nsec

2. MASTER RESET PULSE WIDTH: 10 Clock Periods.
3. Time between consecutive $\overline{RE}$ or $\overline{WE}$ pulses: TBR = TBW = 2 CLOCK PERIODS MINIMUM.
4. ACT, $\overline{E}$/D, KEOE OUTPUTS
   These pins will be valid within 2 CLK ↓ +450 nsec from $\overline{WE}\uparrow$ of a COMMAND REGISTER write operation.
5. $\overline{KPE}$ OUTPUT
   This pin will be active within 2 CLK ↓ +450 nsec from $\overline{WE}\uparrow$ of a write of a KEY WORD byte that results in a parity error.
6. $\overline{CRPS}$, $\overline{DPS}$, $\overline{E}$/D INPUTS require a 300 nsec setup time.
7. The initial KR activation will be valid within 3 CLK↓ +450 nsec from $\overline{WE}\uparrow$ of a write operation that programs a 1 into the COMMAND REGISTER ACTIVATE bit (or a 2 CLK v +450 nsec from ACT input↑, if $\overline{CRPS}$ = 0).
8. The initial DIR activation will be valid within 2 CLK↓ +450 nsec from $\overline{WE}\uparrow$ of the 8th write into the KEY REGISTER.
9. The initial DOR activation will be valid within 49 CLK↓ +450 nsec from $\overline{WE}\uparrow$ of the 8th write into the DATA REGISTER.
10. When reading the DATA REGISTER (in response to DOR), subsequent data bytes are made available internally to the DA (CDP) output buffers within 2 CLK↓ +450 nsec from $\overline{RE}\uparrow$.
11. After reading the DATA REGISTER in response to DORs, DIR will be activated and valid within 2 CLK↓ +450 nsec from $\overline{RE}\uparrow$ of the 8th read from the DATA REGISTER.

    NOTE: All output timings assume CLOAD = 50pf.

TABLE 10. AC OPERATING CHARACTERISTICS WD20C03A 5MHz CLOCK

T_A = 0°C (32°F) to 70°C (158°F), V_{DD} = +12V ±.6V, V_{CC} = +5V ±.25V, V_{SS} = 0V

SYMBOL	CHARACTERISTIC	MIN	MAX	UNIT	CONDITION
	READ				
TACS	A0, A1, $\overline{CS}$, Setup to $\overline{RE}\downarrow$	30		nsec	
TRDV	$\overline{RE}\downarrow$ to DAL Valid		150	nsec	CLOAD = 50pf
TRD	$\overline{RE}$ Pulse Width	220		nsec	
TDF	$\overline{RE}\uparrow$ to DAL Float	20	100	nsec	
TACH	A0, A1, $\overline{CS}$ Hold from $\overline{RE}\uparrow$	0		nsec	
	WRITE				
TACS	A0, A1, $\overline{CS}$ Setup to $\overline{WE}\downarrow$	30		nsec	
TDVW	DAL Setup to $\overline{WE}\uparrow$	80		nsec	
TRW	$\overline{WE}$ Pulse Width	125		nsec	
TDH	DAL Hold from $\overline{WE}\uparrow$	30		nsec	
TACH	A0, A1, $\overline{CS}$ Hold from $\overline{WE}\uparrow$	0		nsec	
	HANDSHAKE				
TDD-W	KR↓ DIR↓ IVIR↓ SPIR↓ from $\overline{WE}\downarrow$		150	nsec	CLOAD = 50pf
TDD-R	DOR↓ from $\overline{RE}\downarrow$		150	nsec	
TDS-W	$\overline{DIA}\downarrow$ from $\overline{WE}\uparrow$		1CLK+ 120	nsec	
TDS-R	$\overline{DOA}\downarrow$ from $\overline{RE}\uparrow$		1CLK+ 25	nsec	
TDA-W	KR↑ DIR↑ IVIR↑ SPIR↑ KA↑ and $\overline{DIA}\uparrow$ from $\overline{WE}\uparrow$		2CLK+ 140	nsec	
TDA-R	DOR↑ $\overline{DOA}\uparrow$ from $\overline{RE}\uparrow$		2CLK+ 45	nsec	
TCY	Clock Cycle Time	200			
TMR	Master Reset Pulse Width	1		μsec	

NOTE: All output timing specifications reflect the following:
High Output 2.0V
Low Output 0.8V

TABLE 11. AC OPERATING CHARACTERISTICS WD20C03A 8MHz CLOCK

T_A = 0°C (32°F) to 70°C (158°F), V_{DD} = +12V ±.6V, V_{CC} = +5V ±.25V, V_{SS} = 0V

SYMBOL	CHARACTERISTIC	MIN	MAX	UNIT	CONDITION
	READ				
TACS	A0, A1, $\overline{CS}$, Setup to $\overline{RE}\downarrow$	25		nsec	
TRDV	$\overline{RE}\downarrow$ to DAL Valid		115	nsec	CLOAD = 50pf
TRD	$\overline{RE}$ Pulse Width	150		nsec	
TDF	$\overline{RE}\uparrow$ to DAL Float	17	50	nsec	
TACH	A0, A1, $\overline{CS}$ Hold from $\overline{RE}\uparrow$	0		nsec	
	WRITE				
TACS	A0, A1, $\overline{CS}$ Setup to $\overline{WE}\downarrow$	25		nsec	
TDVW	DAL Setup to $\overline{WE}\uparrow$	40		nsec	
TRW	$\overline{WE}$ Pulse Width	100		nsec	
TDH	DAL Hold from $\overline{WE}\uparrow$	25		nsec	
TACH	A0, A1, $\overline{CS}$ Hold from $\overline{WE}\uparrow$	0		nsec	
	HANDSHAKE				
TDD-W	KR↓ DIR↓ IVIR↓ SPIR↓ from $\overline{WE}\downarrow$		100	nsec	CLOAD = 50pf
TDD-R	DOR↓ from $\overline{RE}\downarrow$		100	nsec	
TDS-W	KA↓ $\overline{DIA}\downarrow$ from $\overline{WE}\uparrow$		1CLK+ 80	nsec	
TDS-R	$\overline{DOA}\downarrow$ from $\overline{RE}\uparrow$		1CLK+ 20	nsec	
TDA-W	KR↑ DIR↑ IVIR↑ SPIR↑ KA↑ and $\overline{DIA}\uparrow$ from $\overline{WE}\uparrow$		2CLK+ 80	nsec	
TDA-R	DOR↑ $\overline{DOA}\uparrow$ from $\overline{RE}\uparrow$		2CLK+ 20	nsec	
TCY	Clock Cycle Time	125			
TMR	Master Reset Pulse Width	1		μsec	

NOTE: All output timing specifications reflect the following:
High Output 2.0V
Low Output 0.8V

TABLE 12. AC OPERATING CHARACTERISTICS WD20C03A 10MHz CLOCK

T_A = 0°C (32°F) to 70°C (158°F), V_{DD} = +12V ±.6V, V_{CC} = +5V ±.25V, V_{SS} = 0V

SYMBOL	CHARACTERISTIC	MIN	MAX	UNIT	CONDITION
READ					
TACS	A0, A1, $\overline{CS}$, Setup to $\overline{RE}$	25		nsec	
TRDV	$\overline{RE}$ to DAL Valid		90	nsec	CLOAD = 50pf
TRD	$\overline{RE}$ Pulse Width	110		nsec	
TDF	$\overline{RE}$ to DAL Float	15	45	nsec	
TACH	A0, A1, $\overline{CS}$ Hold from $\overline{RE}$	0		nsec	
WRITE					
TACS	A0, A1, $\overline{CS}$ Setup to $\overline{WE}$	20		nsec	
TDVW	DAL Setup to $\overline{WE}$	30		nsec	
TRW	$\overline{WE}$ Pulse Width	95		nsec	
TDH	DAL Hold from $\overline{WE}$	20		nsec	
TACH	A0, A1, $\overline{CS}$ Hold from $\overline{WE}$	0		nsec	
HANDSHAKE					
TDD-W	KR↓ DIR↓ IVIR↓ SPIR↓ from $\overline{WE}$↓		80	nsec	CLOAD = 50pf
TDD-R	DOR↓ from $\overline{RE}$↓		80	nsec	
TDS-W	$\overline{DIA}$↓ from $\overline{WE}$↑		1CLK+ 30	nsec	
TDS-R	$\overline{DOA}$↓ from $\overline{RE}$↑		1CLK+ 15	nsec	
TDA-W	KR↑ DIR↑ IVIR↑ SPIR↑ KA↑ and $\overline{DIA}$↑ from $\overline{WE}$↑		1CLK+ 25	nsec	
TDA-R	DOR↑ $\overline{DOA}$↑ from $\overline{RE}$↑		2CLK+ 10	nsec	
TCY	Clock Cycle Time	100		nsec	
TMR	Master Reset Pulse Width	1		μsec	

NOTE: All output timing specifications reflect the following:
High Output 2.0V
Low Output 0.8V

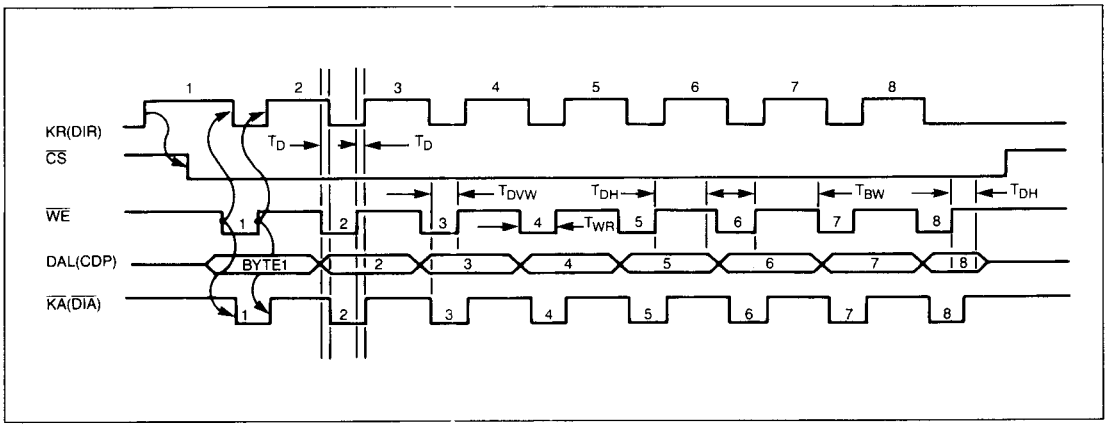


FIGURE 11. WD2001/2002 TYPICAL KEY OR DATA REGISTER LOAD

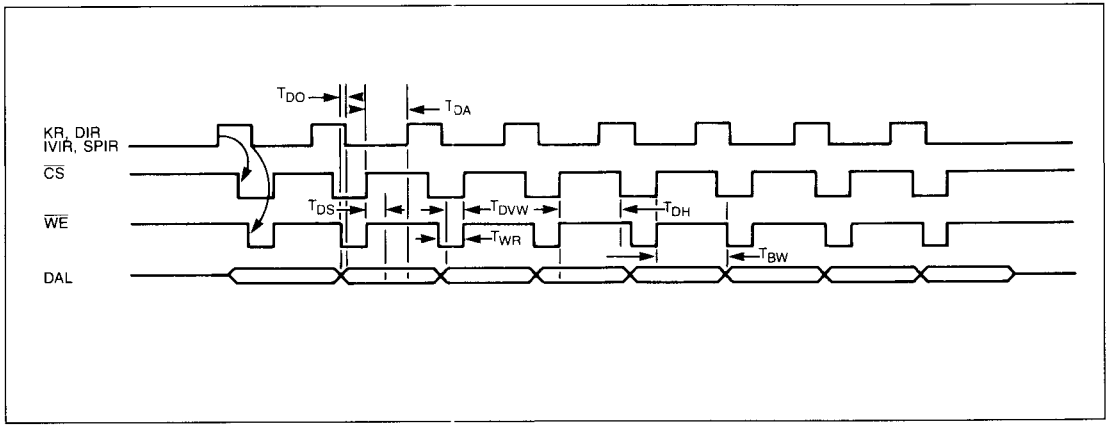


FIGURE 12. WD20C03A TYPICAL KEY OR DATA REGISTER LOAD

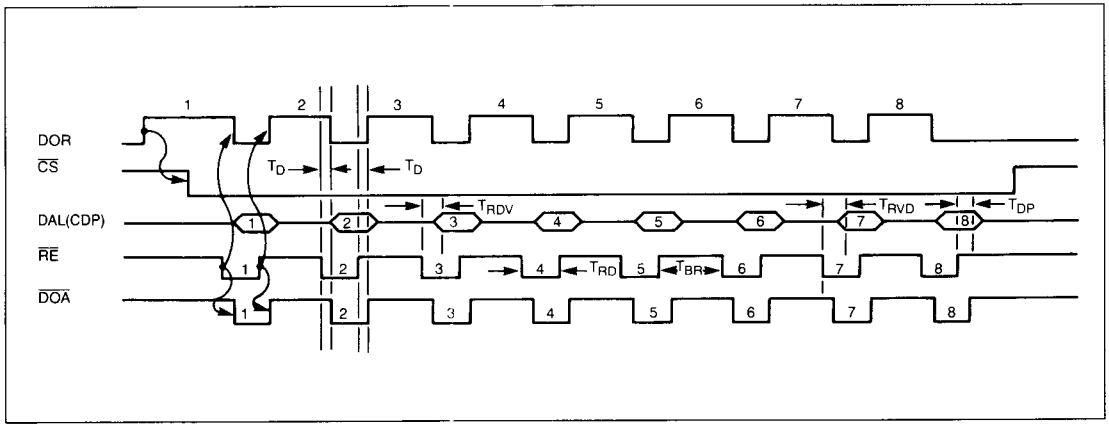


FIGURE 13. WD2001/2002 TYPICAL DATA REGISTER READ AND TIMING

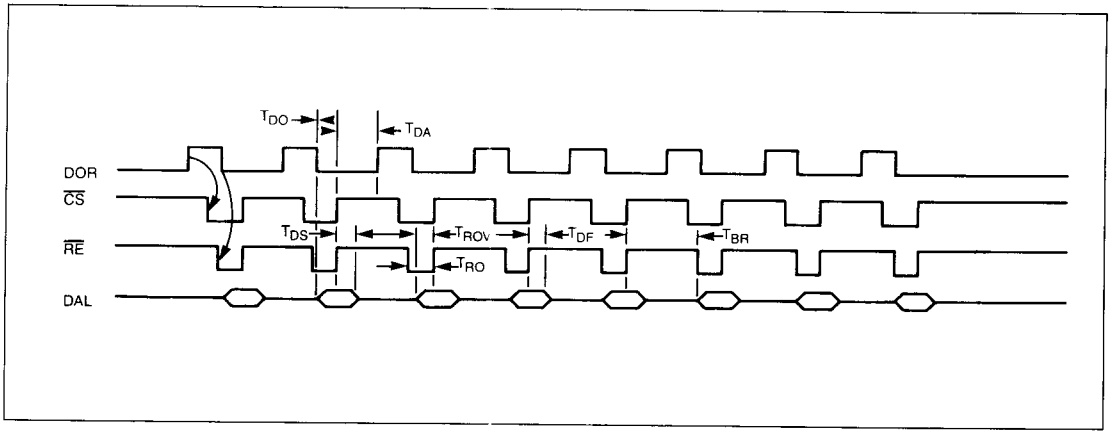


FIGURE 14. WD20C03A TYPICAL DATA REGISTER READ AND TIMING

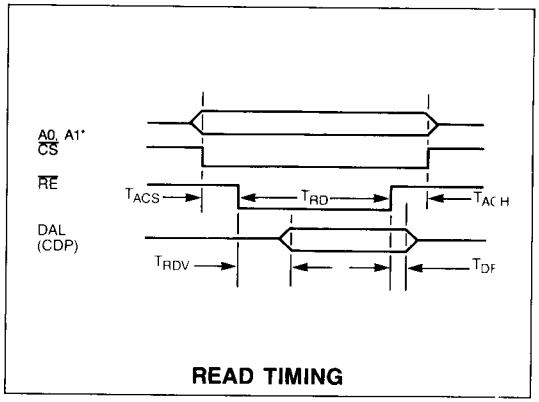


FIGURE 15. WD2001/2002/20C03A READ TIMING

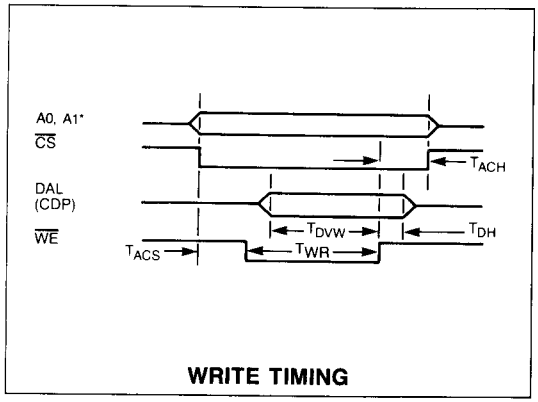
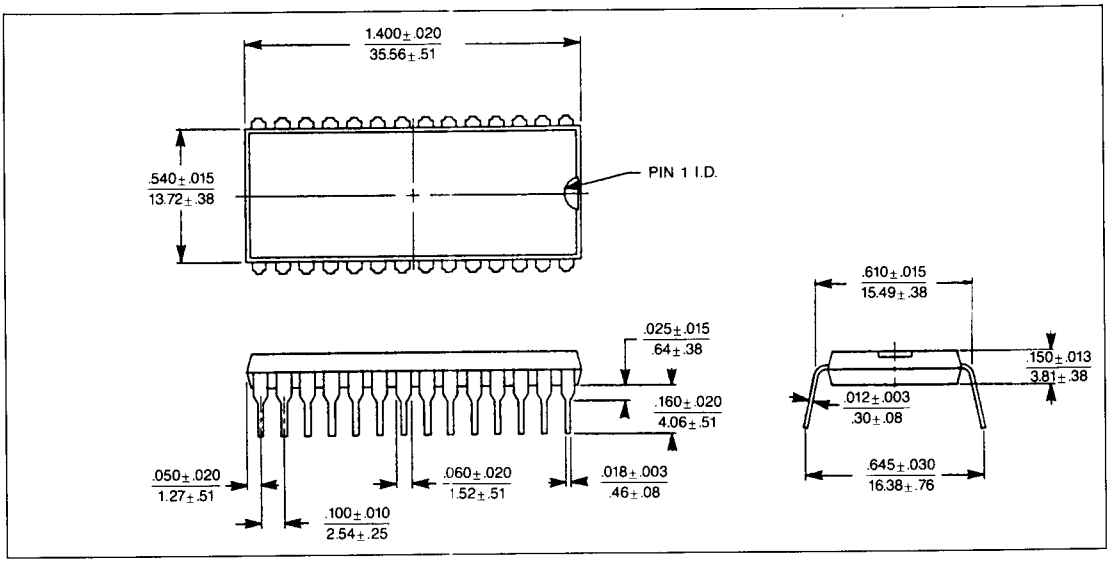
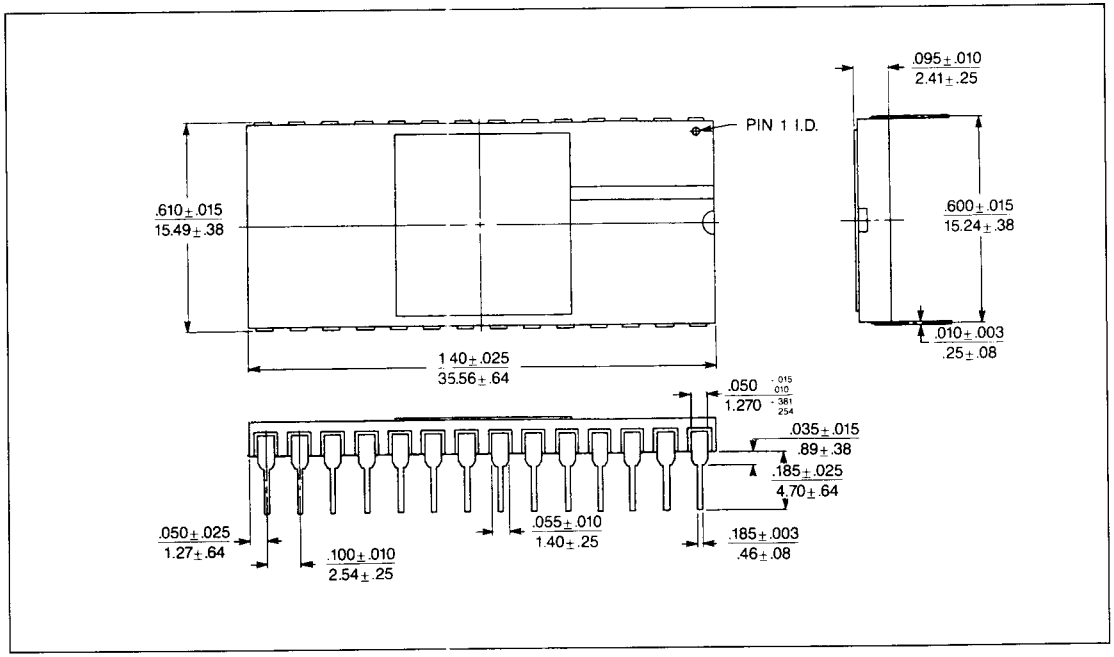


FIGURE 16. WD2001/2002/20C03A WRITE TIMING

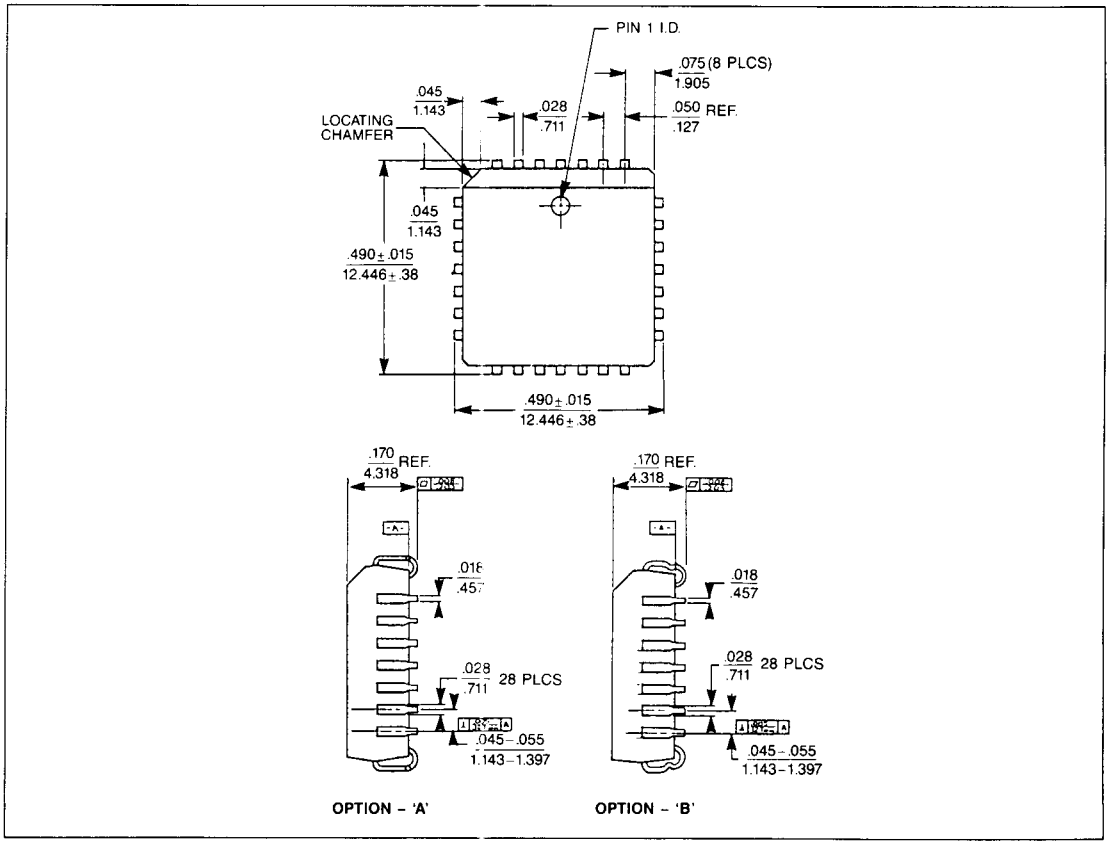
* WD20C03A ONLY.



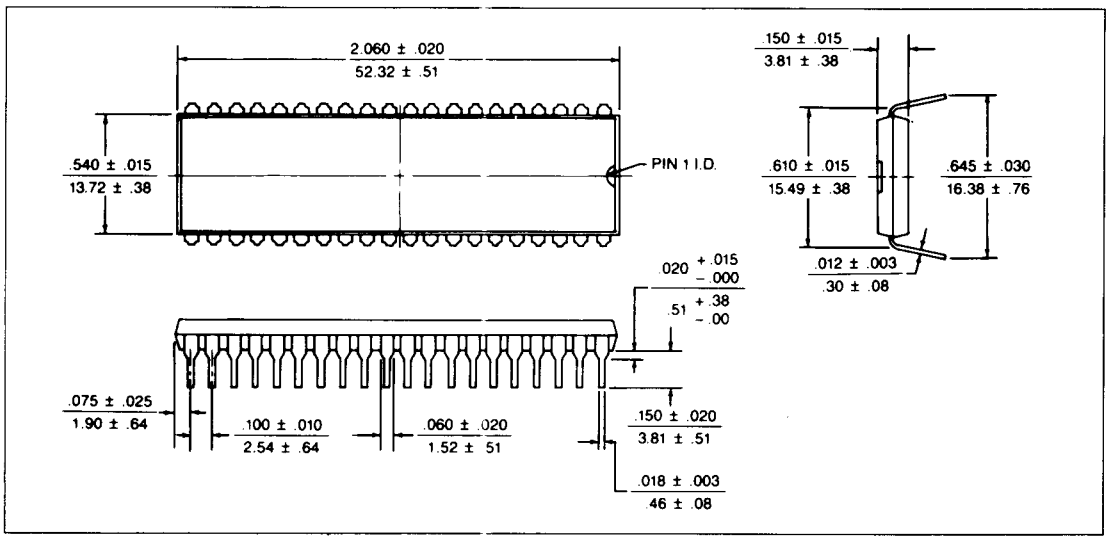
28 LEAD PLASTIC PH



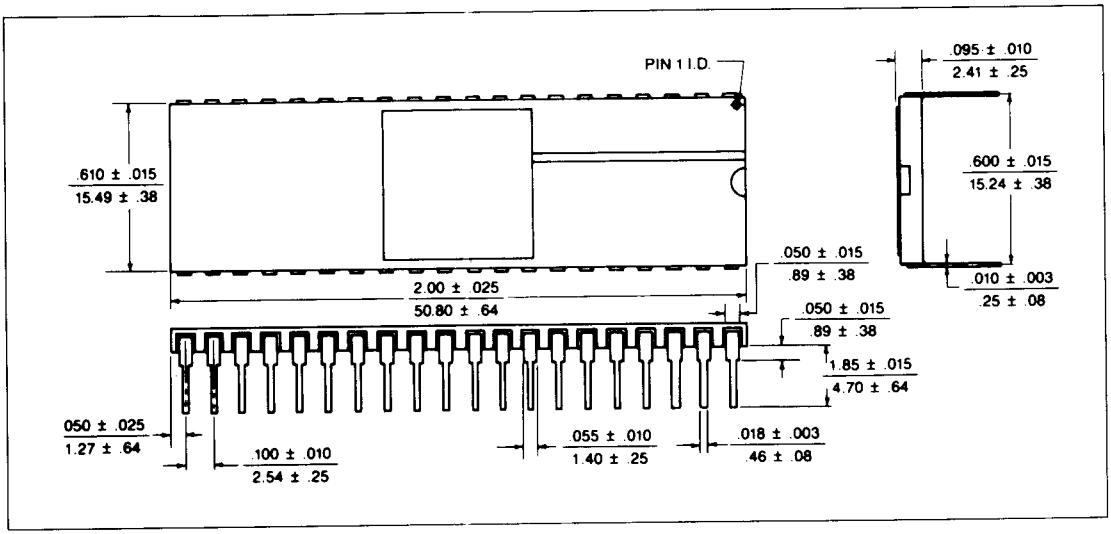
28 LEAD CERAMIC "AH"



28 LEAD PLASTIC QUAD JH



40 LEAD PLASTIC "PL"



40 LEAD CERAMIC "AL"

ORDERING INFORMATION

WD2001/20C03 PH/AH/JH
WD2002 PL/AL

PH = Plastic (Encap), 28-Lead
AH = Ceramic Side Braze, 28-Lead
JH = Plastic Chip Carrier-Leaded, 28-Lead

PL = Plastic (Encap), 40-Lead
AL = Ceramic Side Braze, 40-Lead

Please contact your local Western Digital Sales Representative or call Toll Free 1-800-847-6181 for package availability and price information.

Western Digital
2445 McCabe Way
Irvine, California 92714
(714) 474-2033 (714) 863-0102
FAX 714-660-4909 TLX 910-595-1139

For Information on WD Communications Products
Call: 1-800-NET LEADER (1-800-638-5323)

WD1347C 1/88 2.5M

WESTERN DIGITAL