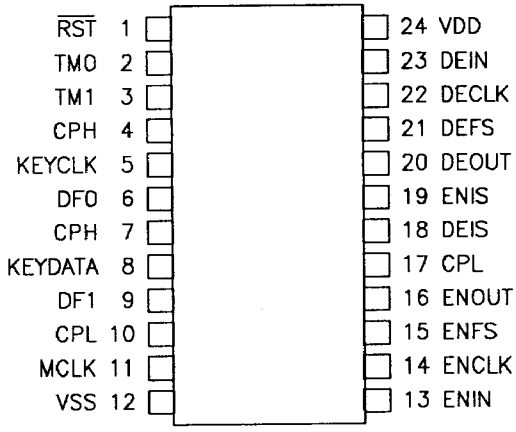
DALLAS SEMICONDUCTOR

DS2160
DES PROCESSOR

FEATURES

- Performs voice/data encryption and decryption according to the Data Encryption Standard (DES)
- Full duplex operation; one encrypt channel, one decrypt channel
- Each channel can process up to 64K bits per second
- Connects directly to combo-codec devices
- Simple key entry
- Uses Cipher Feedback Mode (CFB) of the DES standard
- Can encrypt/decrypt either 8 bits, 7 bits, 6 bits, or 4 bits
- Single +5V supply; low-power CMOS technology
- Available in 24-pin DIP and 28-pin PLCC

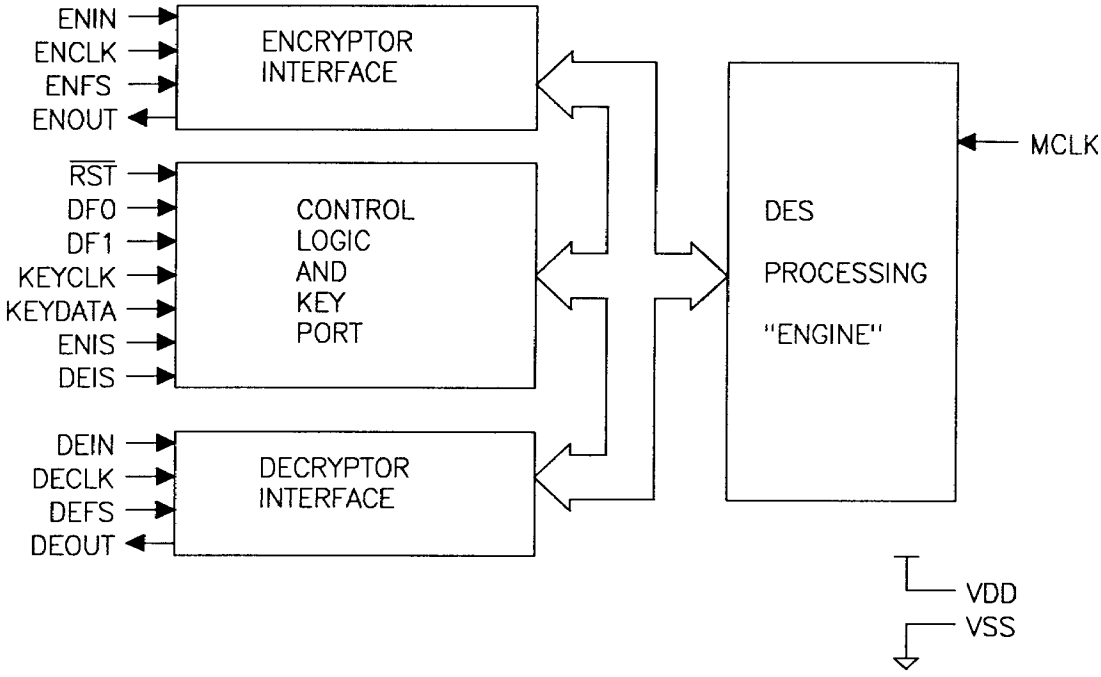
PIN CONNECTIONS



DESCRIPTION

The DS2160 is a dedicated Digital Signal Processing (DSP) CMOS chip optimized for the National Bureau of Standard's Data Encryption Standard (DES) algorithm. The DS2160 has two channels: one for encryption and one for decryption. The chip performs encipher/decipher operations on 64-bit words at a rate of up to 64K bits per second per channel. To provide security as specified in DES, a 64-bit key is necessary. The key is entered into the DS2160 through a simple serial port and cannot be accessed externally. The DES algorithm is used in both governmental and commercial applications where sensitive information is passed though unsecured media.

DS2160 BLOCK DIAGRAM Figure 1



3

PIN	SYMBOL	TYPE	DESCRIPTION
1	RST	I	**Reset.** A high-low transition resets the algorithm. The device should be reset on power-up.
2 3	TMO TM1	I	**Test Modes 0 and 1.** Tie to VSS for normal operation.
4	CPH	I	**Configure Pin High.** Tie to VDD for normal operation.
5	KEYCLK	I	**Key Clock.** Used in conjunction with the KEYDATA pin to enter the 64-bit DES key.
6	DF0	I	**Data Format 0.** Used in conjunction with the DF1 pin to select whether the device will encrypt/decrypt 8 bits, 7 bits, 6 bits, or 4 bits. See Table 2.
7	CPH	I	**Configure Pin High.** Tie to VDD for normal operation.
8	KEYDATA	I	**Key Data.** Used in conjunction with the KEYCLK pin to enter the 64-bit DES key.
9	DF1	I	**Data Format 1.** Used in conjunction with the DF0 pin to select whether the device will encrypt/decrypt 8 bits, 7 bits, 6 bits, or 4 bits. See Table 2.
10	CPL	I	**Configure Pin Low.** Tie to VSS for normal operation.
11	MCLK	I	**Master Clock.** 12MHz clock for the DES processing engine; may be asynchronous to ENCLK and DECLK.
12	VSS	-	**Signal Ground.** 0.0 volts.
13	ENIN	I	**Encrypt Channel Data Input.** Input PCM word is sampled on the first eight falling edges of ENCLK after the ENFS signal.
14	ENCLK	I	**Encrypt Channel Clock.** Data I/O clock for the encryption channel; must be tied to DECLK.
15	ENFS	I	**Encrypt Channel Frame Sync.** Frame sync for the encryption channel; must be tied to DEFS. A two ENCLK wide pulse here indicates a 64-bit word boundary.
16	ENOUT	O	**Encrypt Channel Data Output.** Updated on the first eight rising edges of ENCLK after the ENFS signal.
17	CPL	I	**Configure Pin Low.** Tie to VSS for normal operation.
18	DEIS	I	**Decrypt Channel Idle Select.** High state will idle the decryption channel causing the DEOUT pin to 3-state.

19	**ENIS**	i	**Encrypt Channel Idle Select.** High state will idle the encryption channel causing the ENOUT pin to 3-state.
20	**DEOUT**	0	**Decrypt Channel Data Output.** Updated on the first eight rising edges of DECLK after the DEFS signal.
21	**DEFS**	i	**Decrypt Channel Frame Sync.** Frame sync for the decryption channel; must be tied to ENFS. A two DECLK wide pulse here indicates a 64-bit word boundary.
22	**DECLK**	i	**Decrypt Channel Clock.** Data I/O clock fo the decryption channel; must be tied to ENCLK.
23	**DEIN**	i	**Decrypt Channel Data Input.** Input PCM word is sampled on the first eight edges of DECLK after the DEFS signal.
24	**VDD**	-	**Positive Supply.** 5.0 volts.

RESET AND CONTROL BITS

The RST pin must be held low for at least 1 millisecond on system power-up after the master clock (MCLK) is stable to insure proper initialization of the device. The control bits on the DS2160 (ENIS, DEIS, DF0, and DF1) can be changed without a reset being issued. If both ENIS and DEIS pins are tied high, then the DS2160 will enter a power-down state that consumes much less current. When either ENIS or DEIS is taken low, the DS2160 will exit the power-down condition in less than 200 milliseconds.

DATA FORMAT

The DS2160 has four separate data formats. The chip can be configured via the DF0 and DF1 pins to encrypt/decrypt either 4 bits, 6 bits, 7 bits, or 8 bits of the PCM word. (See Table 2). For example, if DF0 is strapped low and the DF1 pin is strapped high, then the DES processor will be in the 7-bit mode. In this mode, the encrypt channel of the processor will only encrypt the seven most significant bits of the PCM word that it receives, or in other words, the first seven bits of each 8-bit PCM word that it receives. The remaining bit, which is the least significant bit, will pass through the processor untouched. In the 7-bit mode, the decrypt channel knows that only the seven most significant bits are encrypted and it will decode the incoming encrypted PCM word accordingly. As with the encrypt channel, the LSB of the encrypted PCM word will pass though the decrypt channel unaffected.

DS2160 DATA FORMATS Table 2

Data Format	DF0 (pin 6)	DF1 (pin 9)
8-Bit	0	0
7-Bit	0	1
6-Bit	1	0
4-Bit	1	1

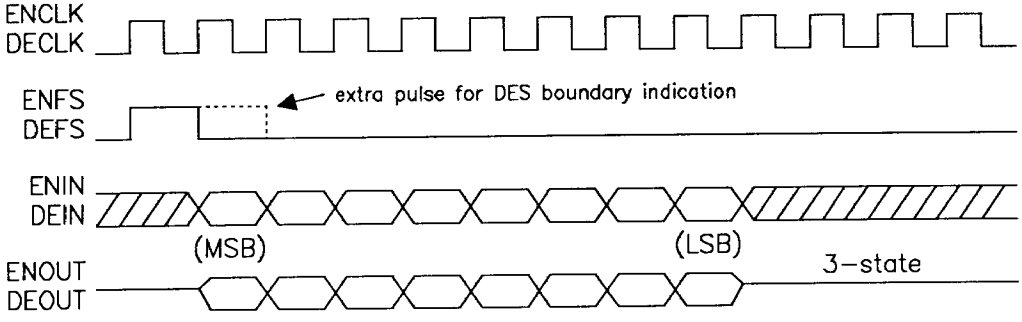
When bits are to pass through the DS2160 unaffected, the processor handles the transfer as follows:

1. The one, two, or four bits in each PCM word that are not to be touched are extracted.
2. Their bit positions are replaced by logical ones.
3. The encrypt/decrypt algorithm is performed.
4. The extracted bits are replaced into their original positions.

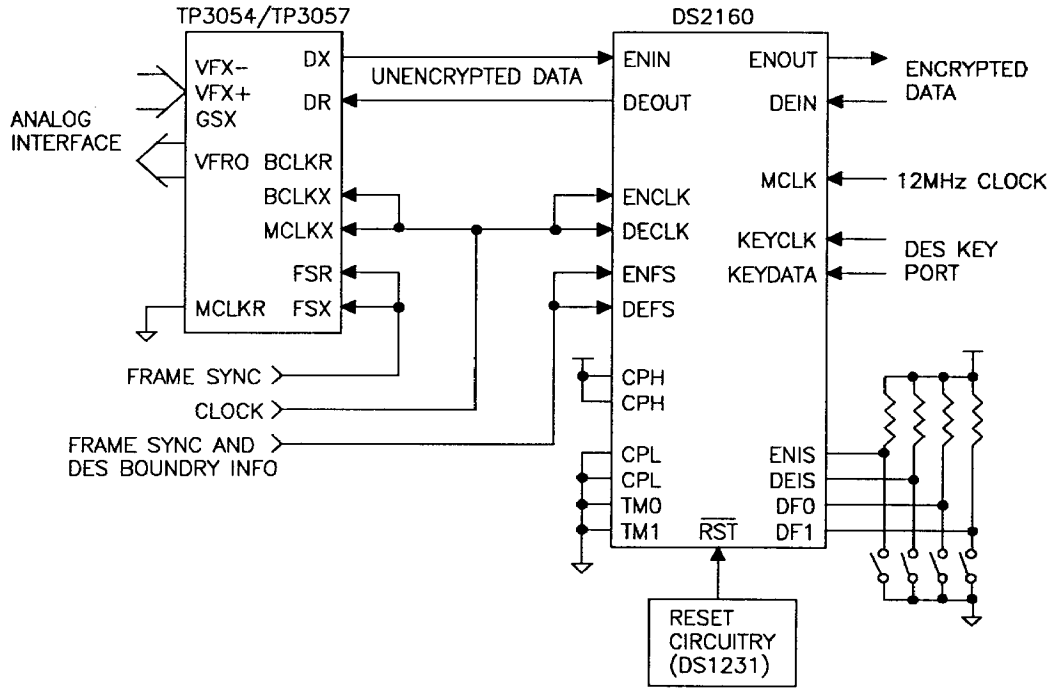
PCM INTERFACE

The DS2160 operates directly with a standard PCM type interface. (See Figure 2.) The processor samples the PCM data to be processed (encrypted or decrypted) on the first eight falling edges of ENCLK/DECLK after the ENFS/DEFS signal. All other data on ENIN and DEIN is ignored. The output of the encrypting or decrypting is placed on the ENOUT and DEOUT pins, respectively, on the first eight rising edges of ENCLK/DECLK after the ENFS/DEFS signal. The ENOUT and DEOUT pins are 3-stated except for the 8-bit period when they are outputting data. The I/O clocks ENCLK and DECLK on the DS2160 can operate at speeds from 256KHz to 4.096 MHz. The DS2160 interprets a two-bit wide frame sync pulse to indicate a DES word boundary. More on this issue is covered in the DES word synchronization section.

DS2160 PCM INTERFACE Figure 2



DS2160 CONNECTION TO COMBO CODEC Figure 3



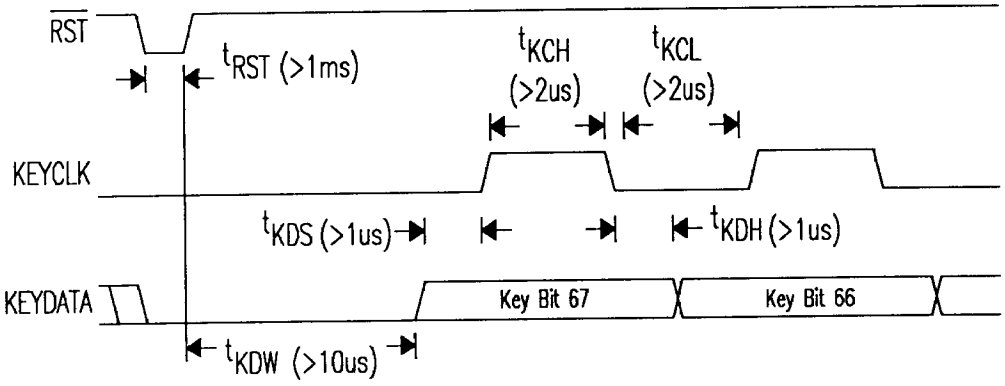
NOTE:
TP3054 and TP3057 are National Semiconductor Combo Codecs.

KEY MANAGEMENT

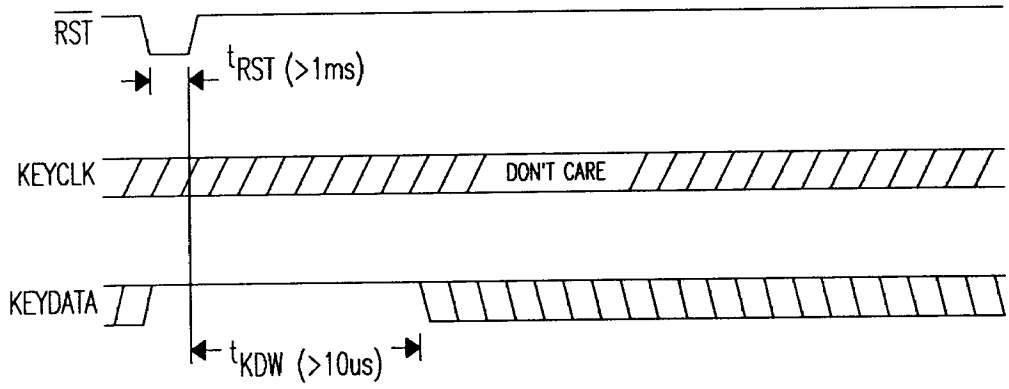
The 64-bit key (56 bits plus eight parity bits) is entered into the DS2160 through a simple two-pin serial port. Figure 4 details the operation of the DES key port. To enter a key into the DS2160, the KEYDATA pin must be held low during and after a Reset. Once the RST pin is returned high, then the key can begin to be entered after a wait time of at least 10 us. (NOTE: the DS2160 will wait indefinitely after a reset for a key to be entered.) After the wait period, data is clocked in using the KEYCLK pin. The key data has a minimum setup and hold time of 1 us and the key clock must be held high and low for at least 2 us. The DS2160 expects that 68 bits of data will be clocked in: the 64-bit key plus a leading 4 bit header that must be all zeros. The header is clocked in first, followed by the key. If a reset is to be issued, and the user wishes not to disturb to the key currently in the DS2160, then the KEYDATA pin must be held high during and after the reset. (See Figure 5.)

In order to maintain the highest level of security possible, the DES key cannot be accessed in any manner once it is clocked into the DS2160. Also, the key is not stored in the DS2160 in its original form.

DS2160 KEY ENTRY SEQUENCE Figure 4



RESET OF DS2160 WITHOUT DISTURBANCE OF THE DES KEY Figure 5

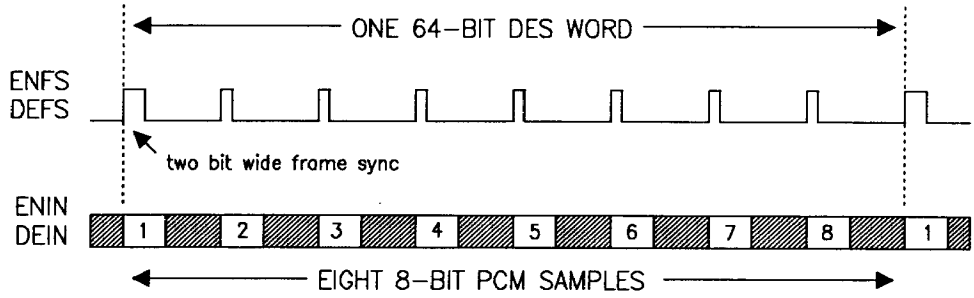


DES 64-BIT WORD BOUNDARY SYNCHRONIZATION

The DES algorithm encrypts/decrypts 64-bit words. In a DES system, it is necessary that the encryptor and decryptor realize where in a contiguous data stream the 64-bit words begin and end so that they can properly encode and decode the data. In the PCM environment in which the DS2160 operates, the data stream is made up of a continuing series of 8-bit samples. The DS2160 will combine eight consecutive PCM samples to create a single DES word.

In the DS2160, the user defines the boundaries of the 64-bit DES words via the ENFS and DEFS pins. The beginning of a 64-bit DES word are indicated by a frame sync pulse that is two bits wide instead of its normal width of one bit. When the DS2160 receives a two-bit wide frame sync pulse at ENFS and DEFS, it realizes that the next eight PCM words that it receives make up the 64-bit DES word. (See Figure 6.)

DS2160 DES WORD FRAMEWORK Figure 6



The DS2160 contains an internal counter that eliminates the need to have double-wide ENFS and DEFS signals every eighth frame. Hence, the wide frame sync pulse can be applied at any multiple of eight from zero to infinity.

DES SYNCHRONIZATION USING T1/CEPT MULTIFRAMES

If the DS2160 is used to encrypt voice or data that is to be transmitted over T1 or CEPT lines, the user can take advantage of an existing multiframe arrangement to provide the necessary synchronizaton of the 64-bit DES words between the encryptor and the decryptor. In T1, multiframes are made up of either 12 or 24 frames depending on whether the framing mode is Superframe (D4) or Extended Superframe (ESF), respectively. In CEPT environments, the multiframe is always made up of 16 frames. If each of these frames per multiframe numbers is multiplied by two, they become candidates for the indication of DES word boundaries needed by the DS2160 because they will be multiples of eight.

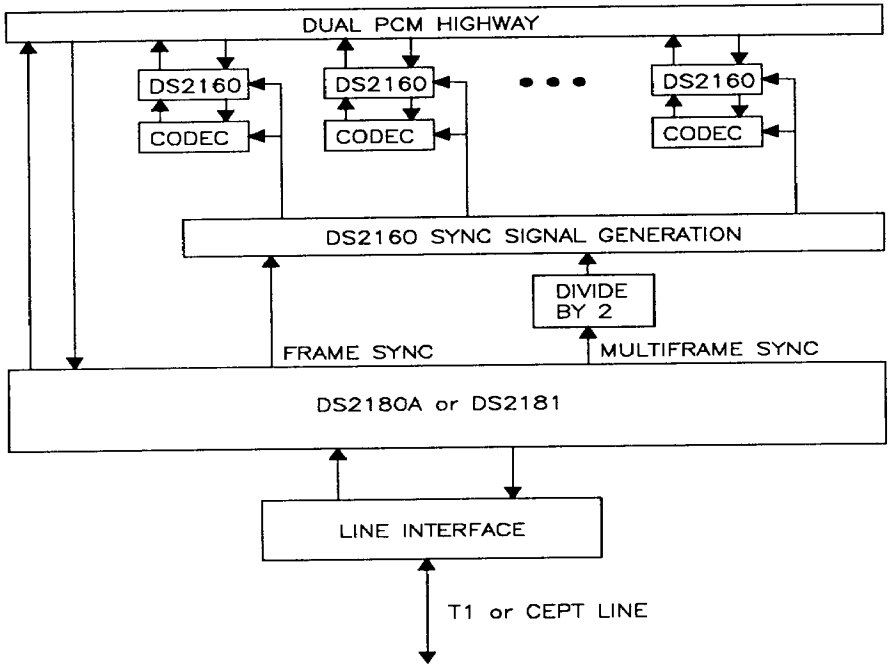
Figure 7 shows an arrangement that could use the existing multiframe scheme for DES synchronization. Either the DS2180A or DS2181 transceiver will synchronize to the T1 or CEPT data stream at both the multiframe and frame level. The frame sync signal is sent to a Time Slot Assignment Circuit (TSAC) where it will be moved in time to allow numerous DS2160s to connect to the same PCM highway. The multiframe signal is divided by two to create a signal that is a multiple of eight. This signal will be used to establish DES word boundaries on the DS2160. The output of the TSAC and the divide by two are combined to create a signal that will provide a one-bit wide frame sync pulse every frame, along with a two-bit wide frame sync pulse at some multiple of eight frames.

CIPHER FEEDBACK MODE

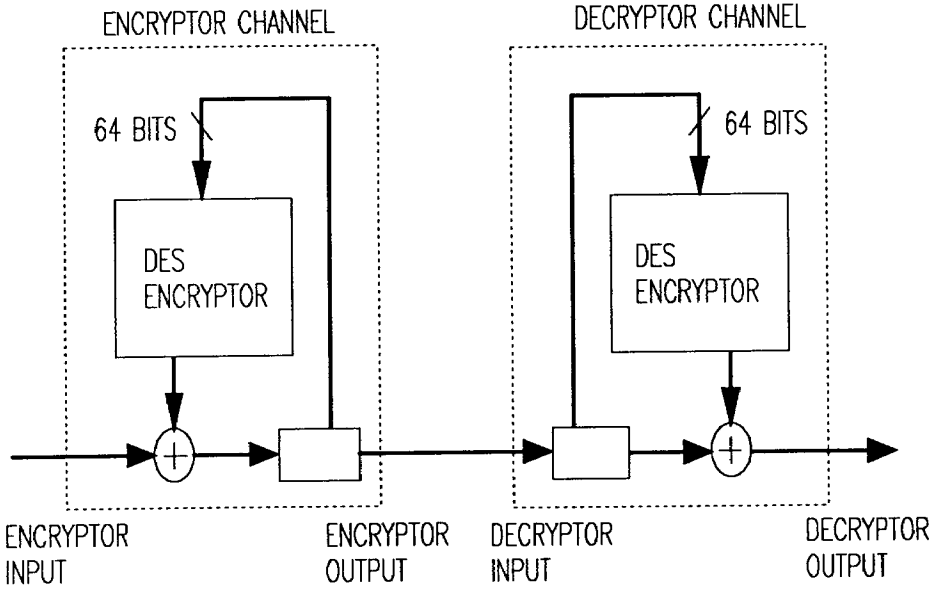
The DS2160 uses the Cipher Feedback Mode (CFB) as described by the Data Encryption Standard to encode and decode data. The CFB mode uses a DES encryptor to both encrypt and decrypt data. (See Figure 8.) Data is encrypted by logically exclusive-ORing the input data with the pseudorandom output of a DES encryptor. This XOR'ed output is the ciphered data and on the DS2160 it is output through the ENOUT pin. The XOR'ed output is also fed back to the DES encryptor where it serves as input to generate another pseudorandom bit code that will be XOR'ed with the next input sample.

To decode the ciphered data, the input 64-bit word is XOR'ed with the pseudorandom output of a DES encryptor. The ciphered input is also fed to the input of the DES encryptor where it serves at input to generate a pseudorandom bit code that will be used to decode the next ciphered input.

USE OF MULTIFRAME TO ESTABLISH DES SYNCHRONIZATION Figure 7



DS2160 CIPHER FEEDBACK MODE Figure 8



More information on CFB and the DES algorithm can be found in the Federal Information Processing Standards Publications or FIPS PUBs for short. The relevant documents are FIPS PUB 46-1, FIPS PUB 74, and FIPS PUB 81.

ABSOLUTE MAXIMUM RATINGS*

Voltage on any Pin Relative to Ground	-1.0V to +7.0V
Operating Temperature	0°C to 70°C
Storage Temperature	-55°C to +125°C
Soldering Temperature	260°C for 10 seconds

* This is a stress rating only and functional operation of the device at these or any other conditions outside those indicated in the operation sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods of time may affect reliability.

3

RECOMMENDED DC OPERATING CONDITIONS

(0°C to 70°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Logic 1	VIH	2.0		VCC+0.3	V	
Logic 0	VIL	-0.3		+0.8	V	
Supply	V_{DD}	4.5		5.5	V	

CAPACITANCE

(t_A=25°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Input Capacitance	C_{IN}			5	pF	
Output Capacitance	C_{OUT}			10	pF	

DC ELECTRICAL CHARACTERISTICS

(0°C to 70°C; V_{DD}=5V +/- 10%)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Active Supply Current	I_{DDA}		30		mA	1, 2
Idle Supply Current	I_{DDPD}		1		mA	1, 2, 3
Input Leakage	I_I	-1.0		+1.0	uA	
Output Leakage	I_O	-1.0		+1.0	uA	4
Output Current (2.4V)	I_{OH}	-1.0			mA	
Output Current (0.4V)	I_{OL}	+4.0			mA	

NOTES::

1. ENCLK = DECLK = 1.544MHz; MCLK = 12MHz
2. Outputs open; inputs swinging full supply levels
3. ENIS = DEIS = 5V
4. ENOUT and DEOUT are 3-stated

PCM INTERFACE
AC ELECTRICAL CHARACTERISTIC

(0°C to 70°C, V_{CC} = 5V+/- 10%)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
ENCLK, DECLK Period	t_{PED}	244		3906	ns	1
ENCLK, DECLK Pulse Width	t_{WEDL} t_{WEDH}	100			ns	
ENCLK, DECLK Rise Fall Times	t_{RED} t_{FED}		10	20	ns	
Hold Time from ENCLK, DECLK to ENFS, DEFS	t_{HOLD}	0			ns	2
SetUp Time from ENFS, DEFS high to ENCLK, DECLK low	t_{SF}	50			ns	2
Hold Time from ENCLK, DECLK low to ENFS, DEFS low	t_{HF}	100			ns	2
SetUp Time for ENIN, DEIN to ENCLK, DECLK low	t_{SD}	50			ns	2
Hold Time for ENIN, DEIN to ENCLK, DECLK low	t_{HD}	50			ns	2
Delay Time from ENCLK, DECLK to Valid ENOUT, DEOUT	t_{DEDO}	10		150	ns	3
Delay Time from ENCLK, DECLK to ENOUT, DEOUT 3-stated	t_{DEDZ}	20		150	ns	2, 3, 4

NOTES::

1. Maximum width of ENFS and DEFS is one ENCLK or DECLK period (except for frames where edge boundaries for the 64-bit DES words are defined).
2. Measured at V_{IH} = 2.0V, V_{IL} = 0.8V, and 10ns maximum rise and fall times.
3. Load = 150pF + 2 LSTTL loads.
4. For LSB of PCM byte.

MASTER CLOCK/RESET AC ELECTRICAL CHARACTERISTIC

(0°C to 70°C, V_{CC} = 5V+/- 10%)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
MCLK Period	t_{PM}		83.3		ns	1
MCLK Pulse Width	t_{WMH} t_{WML}	33		50	ns	
MCLK Rise/ Fall Times	t_{RM} t_{FM}			10	ns	
RST Pulse Width	t_{RST}	1			ms	

3

NOTE:

1. MCLK = 12MHz +/- 500ppm