ANALOG DEVICES

SafeNet™ DSP

Preliminary Technical Data ADSP-2141L

APPLICATIONS

- Security co-processor for High-Speed Networking Products (Routers, Switches, Hubs, etc.)
- Cryptographic Core for Firewalls, Hardware Encryptors, etc.
- Crypto peripheral for implementing secure NIC adapters (10/100 Ethernet, Token Ring, ISDN, etc.)
- Secure Modem-on-a-Chip (V.34, ADSL, etc.)

FEATURES

DES CRYPTO BLOCK

- 640 Mbps Sustained Performance – Single DES
- 214 Mbps Sustained Performance – Triple DES
- Supports all Modes: ECB; CBC; 64-OFB; and 1, 8, 64-bit CFB. Includes automatic Padding
- Implements IPSec ESP Transforms Autonomously at OC-3 (155 Mbps) rates (3-DES, SHA-1)

HASH BLOCK

- Hardware-based SHA-1 and MD-5 Hashing
- 253 Mbps Sustained Performance – SHA-1
- 315 Mbps Sustained Performance – MD-5
- Implements IPSec AH and HMAC Transforms

SECURE KERNEL CONTROL

- Tamper-resistant isolation of Cryptographic Functions
- Enforces Security Perimeter around Crypto Functions and Crypto Storage Locations
- Anti-Cloning Protection
- Secure Algorithm Download

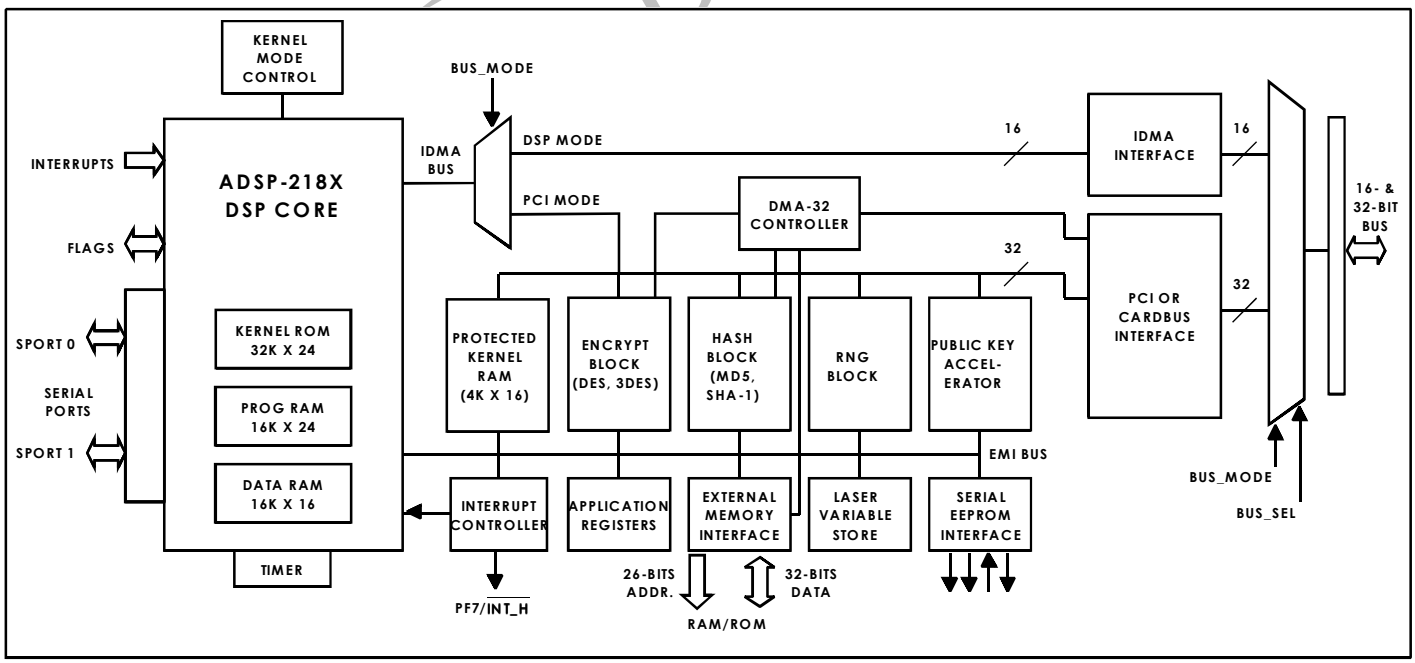


Figure 1 ADSP-2141 Functional Block Diagram

REV. PrB

Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood MA 02062-9106, U.S.A
http://www.analog.com/dsp

SafeNet CGX LIBRARY

- On-chip SafeNet CGX crypto library with flexible CGX API
- Includes *Chained* and *Parallel Execution* Commands such as Hash-and-Encrypt
- Embodied as 32K Words (32k x 24) Kernel Program Mask-Programmed into On-chip ROM
- On-Chip protected 4k x 16 Security Scratchpad RAM

RANDOM NUMBER GENERATOR

- Hardware-based Non-Deterministic Random Number Generator
- Generates internal Session Keys which are never exposed outside of the SafeNet DSP
- Redundant Fail-Safe Design
- Up to 1.3 Mbits of Random Data Available per Second

PUBLIC KEY ACCELERATOR

- Accelerator for Math-Intensive Public Key operations
- Diffie-Hellman Negotiate: <29 ms (1024-bit Modulus, 180-bit Exponent)
- RSA™ 1024-bit Sign: <29 ms; RSA 1024-bit Verify: 6 ms
- DSA Sign: <39ms; DSA Verify: <66 ms

KEY MANAGEMENT BLOCK

- Laser-Programmed Unique Triple-DES Cryptovariable Protects Off-Chip storage
- Support for Secure Storage of both Secret Keys and Public Keys
- Trust-Model Rules Enforcement
- Only Encrypted Keys may be Exported off of the Chip
- Internal Key Cache for 15 Keys – can be Expanded to 700 Keys on-chip
- Keys may also be stored securely off-chip, allowing unlimited storage

DSP CORE

- 40 MIPS Sustained Performance
- Single-Cycle Instruction Execution
- Single-Cycle Context Switch
- Zero-Overhead Looping
- Low Power Dissipation
- 16k Words (16k x 24) On-Chip Program RAM
- 16k Words (16k x 16) On-Chip Data RAM
- 64M Words Off-Chip Program & Data Memory
- Programmable 16-bit Interval Timer with Prescale

PCI BUS/CARDBUS INTERFACE

- 32-bit 3.3V Bus Interface
- 33 or 66[1] MHz Bus speed
- Bus Master and Target Modes
- Can directly DMA between Crypto Functions and other PCI Bus Agents

[1] 66 MHz speed pending chip characterization

GENERAL DESCRIPTION

The ADSP-2141 SafeNet DSP is a highly integrated embedded Security Processor which incorporates a sophisticated, general purpose DSP, along with a number of high-performance Cryptographic function blocks, as well as PCI, DMA, and Serial EEPROM interfaces. It is fabricated in .35µ CMOS triple-layer metal technology and utilizes a 3.3V Power Supply. It is available in a 208-pin MQFP package with a Commercial (0° – 70° C) Temperature Range. The part number ADSP-2141 is used throughout this data sheet and refers to the ADSP-2141L.

DSP Core

The DSP is a standard Analog Devices ADSP-218x Core with full ADSP-2100 family compatibility. The ADSP-218x Core combines the base DSP components from the ADSP-2100 family with the addition of two serial ports, a 16-bit internal DMA port, a byte DMA port, a programmable timer, Flag I/O, extensive interrupt capabilities, and on-chip program and data memory. The External Memory Interface of the 218x Core has been extended to support up to 64M-words addressing for both Program and Data memory. Some core enhancements have been added in the ADSP-2141, including on-chip Security ROM and Interrupt functions. Refer to the Analog Devices ADSP-2183 datasheet for further information.

SafeNet CGX Library - Secure Kernel

The SafeNet CGX Library is a crypto library embodied as firmware (a secure kernel) that is mask-programmed into ROM within the DSP. This solution protects the library from tampering. The CGX Library provides the Application Programming Interface (API) to applications which require security services from the ADSP-2141. Those applications may be software executing in User Mode on the DSP, or they may be external Host software accessing the ADSP-2141 via a PCI bus. Approximately 40 Crypto commands – called CGX (CryptoGraphic eXtensions) – are provided at the API and a simple Control Block structure is used to pass arguments into the secure kernel and return Status. The CGX library includes integrated drivers for the various hardware crypto blocks on the chip. This allows the programmer to ignore those details and concentrate on other product design issues.

The CGX Library firmware runs under a *Protected Mode* state of the DSP as described in "Kernal Mode Control" below. This guarantees the security integrity of the system during the execution of CGX processes and, for example, prevents disclosure of Cryptographic Key data or tampering with a security operation.

Kernel Mode Control

The Kernel Mode Control subsystem is responsible for enforcing the Security Perimeter around the cryptographic functions of the ADSP-2141. The device may operate in either *User Mode* (Kernel Space is not accessible) or *Kernel Mode* (Kernel Space is accessible) at a given time. When in Kernel mode, the Kernel RAM and certain protected Crypto registers and functions (Kernel Space) are accessible only to the CGX Library firmware. The CGX Library executes Host-requested Macro-level functions and then returns control to the calling application. The Kernel Mode Control subsystem resets the DSP should any security violation occur, such as attempting to access a protected memory location while in User mode.

Protected Kernel RAM

The 4K x 16 Kernel RAM provides a secure storage area on the ADSP-2141 for sensitive data such as Keys or intermediate calculations during Public Key operations. The Kernel Mode Control subsystem (above) enforces the protection by only allowing internal Secure Kernel Mode accesses to this RAM. A Public Keyset and a cache of up to 15 Secret keys may be stored in Kernel RAM. Secure Key storage may be expanded to 700 Secret Keys by assigning segments of the DSP's internal Data RAM to be protected. Furthermore, a virtually unlimited number of data encryption keys may be stored in an encrypted form in off-chip memory.

Encrypt Block

The Encrypt Block performs high-speed DES and Triple-DES encrypt/decrypt operations. All 4 standard modes of DES are supported: Electronic Code Book (ECB), Cipher Block Chaining (CBC), 64-bit Output Feedback (OFB) and 1-bit, 8-bit and 64-bit Cipher Feedback (CFB). The DES encrypt/decrypt operations are highly pipelined and execute full 16-round DES in only 4 clock cycles. Hardware support for Padding insertion, verification and removal further accelerates the encryption operation. Context Switching is provided to minimize the overhead of changing crypto Keys and Initialization Vectors (IVs) to nearly zero.

Hash Block

The Secure Hash Block is tightly coupled with the Encrypt Block and provides hardware accelerated one-way Hash functions. Both the MD-5 and SHA-1 algorithms are supported. Combined operations which chain both Hashing and Encrypt/Decrypt functions are provided in order to significantly reduce the processing time for data which needs both operations applied. For `Hash-then-Encrypt` and `Hash-then-Decrypt` operations, the ADSP-2141 can perform parallel execution of both functions from the same source and destination buffers. For `Encrypt-then-Hash` and `Decrypt-then-Hash` operations, the processing must be sequential, however minimum latency is still provided through the pipeline chaining design. An Offset may be specified between the start of Hashing and the start of Encryption to support certain protocols such as IPsec. A 'mutable bit handler' is also provided on the Hash engine to facilitate IPSec AH processing.

Random Number Generator (RNG) Block

The hardware Random Number Generator provides a true, non-deterministic noise source for the purpose of Generating Keys, Initialization Vectors (IVs), and other random number requirements. Random numbers are provided as 16-bit words to the Kernel. The CGX Kernel requests Random Numbers as needed to perform requested CGX commands such as `CGX_Gen_Key`, and can also directly supply from 1 to 65,535 Random Bytes to a host application via the `CGX_Random` command.

Public Key Accelerator

The Public Key Accelerator module works in concert with the CGX Kernel firmware to provide full Public Key services to the host application. The Kernel provides Macro-level functions to perform Diffie-Hellman Key Agreement, RSA Encrypt or Decrypt, DSA Compute and Verify Digital Signatures, etc. The hardware accelerator block speeds computation-intensive operations such as large vector multiply, add, subtract, square, etc.

PCI/Cardbus Interface

A full 66/33 MHz PCI bus interface has been added to the core DSP functions. The 32-bit PCI interface supports both Bus Master and Target modes. The ADSP-2141 is capable of using DMA to directly access data on other PCI entities and pass that data through its Encryption/Hash engines.

32-Bit DMA Controller

The ADSP-2141 incorporates a high-performance 32-bit DMA controller which can be setup to move data efficiently between Host PCI memory, the Hash/Encrypt blocks, and/or External Memory. The DMA controller can be used with the PCI bus in Master mode, thus autonomously moving 32-bit data with minimal DSP intervention. Up to 255 long words (1020 bytes) can be moved in a burst at up to 160Mbytes per second.

Application Registers

The Application Registers are a set of memory-mapped registers which facilitate communications between the ADSP-2141 and a Host processor via the PCI bus. One of the Registers is a mailbox which is 44 bytes long and is setup to hold the CGX command structure passed between the Host and DSP processors. The Application Registers also provide the mechanism which allows the DSP and the external Host to negotiate ownership of the Hash/Encrypt block.

Serial EEPROM Interface

The Serial EEPROM interface allows an external non-volatile memory to be connected to the ADSP-2141 for storing PCI configuration information (Plug and Play), as well as general-purpose non-volatile storage. For example, encrypted (Black) Keys could be stored into EEPROM for fast recovery after a power outage.

Interrupt Controller

The DSP core provides support for 14 interrupt sources, including 6 external and 8 internal. All interrupts are prioritized into 12 levels and interrupt nesting may be enabled or disabled under software control. The Security Block Interrupt Controller provides enhancements to the DSP Interrupt Functions.

Primarily, the Interrupt Controller provides a new Interrupt Generation capability to the DSP or to an external Host Processor. Under programmable configuration control, a *Crypto Interrupt* may be generated due to completion of certain operations such as `Encrypt Complete`, `Hash Complete`, etc. The interrupt may be directed either at the DSP core (on `IRQ2`), or provided on an output line (`PF7/INT_H`) to a Host subsystem.

Laser Variable Storage

The Laser Variable Storage consists of 256 bits of Tamper-Proof Factory programmed data which is only accessible to the internal function blocks and the Security Kernel. Included in these Laser Variable bits are:

- Local Storage Variable (Master Key-Encryption-Key)
- Randomizer Seed (to supplement the true entropy fed into the RNG)

- Program Control Data (Enables/Disables various features and configures the ADSP-2141)
- CRC of the Laser Data (to verify laser data integrity)

The Program Control Data Bits (PCDBs) include configuration for permitted Key Lengths, Algorithm Enables, Red KEK loading, etc. Most of the PCDB settings may be overridden with a Digitally Signed Token which may be loaded into the ADSP-2141 when it boots. These Tokens are created by IRE and each is targeted to a specific ADSP-2141 using a Hash of its unique identity.

Downloadable Secure Code

The ADSP-2141 allows additional Security Functions to be added to the device through a Secure Download feature. Up to 16k words of code may be downloaded into internal memory within the DSP and this code can be given the security privileges of the CGX Kernel firmware. All downloaded firmware is authenticated with a Digital Signature and verified with an on-chip Public Key. Additional functions could include new Encryption, Hash or Public Key algorithms such as IDEA, RC-4®, RIPEMD, Elliptic Curve, or any other application that needs direct control over the protected cryptographic hardware.

ARCHITECTURE OVERVIEW

This section provides an Architecture-level description of the unique function blocks within the ADSP-2141.

Memory Map

The ADSP-2141 memory map is very similar to that of the ADSP-2183 DSP, except that it includes significantly more Off-Chip memory addressing, and has additional Crypto Registers which are accessible to the user.

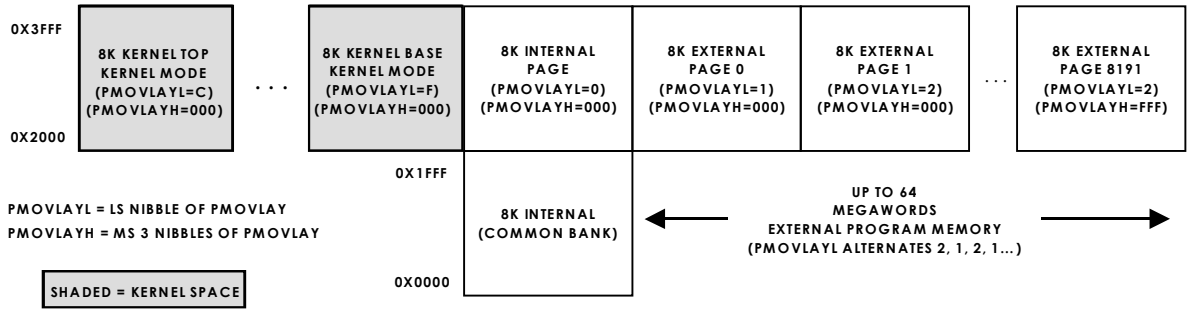


Figure 2 Program Memory (MMAP = 0)

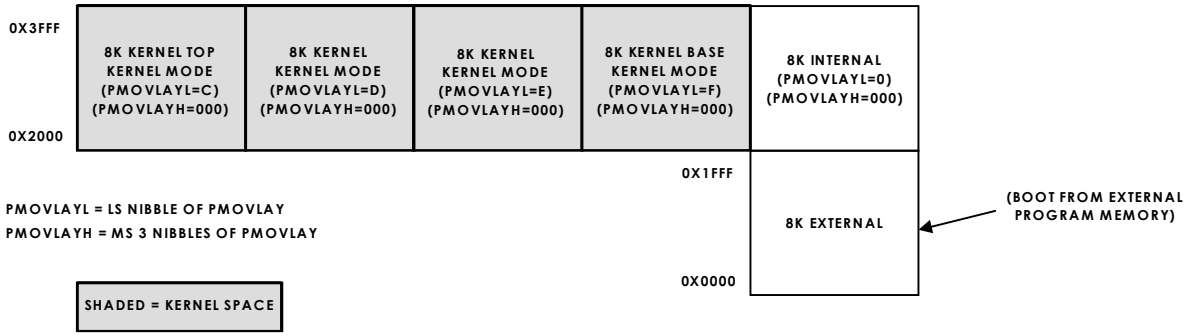


Figure 3 Program Memory (MMAP = 1)

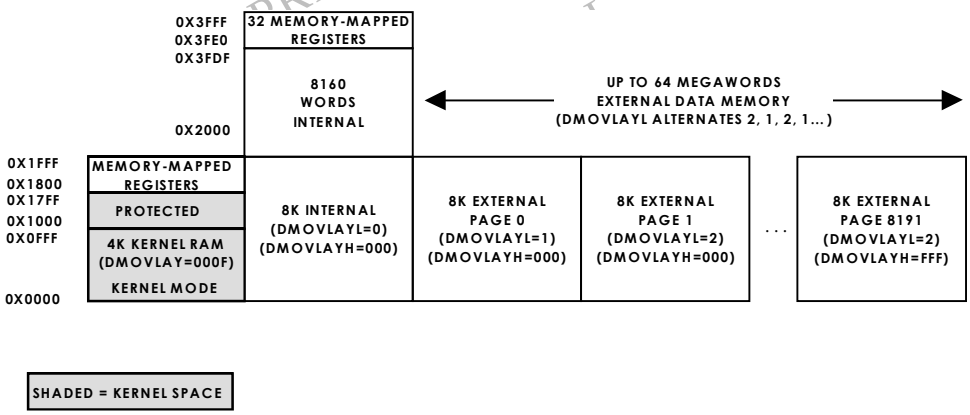


Figure 4 Data Memory

DSP Core

The DSP Core is Architecturally identical to the ADSP-218x with a few exceptions.

- The memory map includes additional External memory addressing through the PMOVLAY and DMOVLAY mechanisms. For more information, see “Memory Map” on page 6.
- Additional memory-mapped Crypto Registers are available in the Kernel data RAM space.
- The PF7/$\overline{\text{INT\_H}}$ flag pin may be reassigned to be the Host Interrupt output.
- IRQ2 now can include interrupt sources from the Crypto subsystem, depending on Interrupt Mask registers.
- A new Read register has been added to indicate the state of Interrupt Enable and Interrupt Masks.

- The Kernel Mode Control subsystem has been added to supervise the Protected Mode of operation of the DSP core.
- Internal RAM protection logic has been added to allow the Kernel to seize increments of 1 kword of internal PRAM and DRAM.
- Bus Mode configuration (218x vs. PCI) pins have been added.
- 32k-words of Kernel Program ROM has been added to the DSP memory space. (See "Memory Map" on page 6.)

Kernel Mode Control

The Kernel Mode Control subsystem provides the following functions which serve to enforce the Security integrity of the ADSP-2141:

- Provide a means to securely enter the Kernel Mode.
- Provide a means to properly exit the Kernel Mode.
- Prevent User Mode access to Protected memory and register locations.
- Manage Interrupts during Kernel Mode executions.
- Manage the Reset function to ensure that sensitive variables in DSP registers are erased.

Most of the Kernel Mode control functions are implemented in the hardware of the ADSP-2141 and are not directly visible to non-Kernel applications (User Mode). Any attempt by a User Mode application program running on the DSP to access a Kernel Space addresses (PRAM 0x2001 – 0x3FFF, PMOVLAY 000C – 000F; or DRAM 0x0000 – 0x17FF, DMOVLAY 000F) results in an immediate chip reset and all sensitive registers and memory locations are erased. Kernel Mode may only be entered via a Call, Jump or Increment to address 0x2000 with PMOVLAY set to 0x000F. Once in Kernel Mode, any branch to non-Kernel Space program memory causes the DSP to return to User Mode. (Note: For security reasons when in Kernel Mode, the DSP does not respond to Emulator bus requests.)

The Kernel Mode can be interrupted during execution, however during certain periods where sensitive data is being moved, all interrupts are disabled. Within the interrupt service routine, another call to the Kernel (CGX call) may be made if desired, although there are limitations on which CGX commands may preempt another. (For information, see the *ADSP-2141 CGX Interface Programmer's Guide*, available from IRE.) Only one level of Kernel Mode nesting is permitted. An interrupt to a User Mode vector location while in Nested Kernel Mode will also trigger the violation reset logic.

Once the interrupt service routine is finished, the return-from-interrupt must return control back to the Kernel at the address/overlay which was originally interrupted, otherwise the protection logic will issue a chip reset.

Hash and Encrypt Block Overview

The Encrypt Block is tightly coupled to the Hash Block in the ADSP-2141 and therefore the two are discussed together. Refer to Figure 5, "Hash/Encrypt Functional Block Diagram," on page 9 for the following description.

The algorithms implemented in the Combined Hash and Encryption Block are: DES, Triple DES, MD5 and SHA-1. Data can be transferred to and from the module once to perform both hashing and encryption on the same data stream. The DES encrypt/decrypt operations are highly paralleled and pipelined, and execute full 16-round DES in only 4 clock cycles. The internal data flow and buffering

allows parallel execution of hashing and encryption where possible, and allows processing of data concurrently with I/O of previous and subsequent blocks. Context switching is optimized to minimize the overhead of changing cryptographic keys to near zero.

The software interface to the module consists of a set of memory-mapped registers, all of which are visible to the DSP and most of which can be enabled for Host access via the PCI bus. A set of five, 16-bit registers define the operation to be performed, the length of the data buffer to be processed, in bytes, the offset between the start of hashing and encryption (or vice versa), and the Padding operation. If the data length is unknown at the time the encrypt/decrypt operation is started, the Data Length register may be set to zero which specifies special handling. In this case, data may be passed to the Hash/Encrypt block indefinitely until the end of data is encountered. At that time, the operation is terminated by writing a new control word to the Hash/Encrypt Control Register (either to process the next packet or to invoke the idle state if there is no further work to do). This will closeout the processing for the packet, including the addition of the selected crypto padding.

A set of seven status registers provides information on when a new operation can be started, when there is space available to accept new data, when there is data available to be read out, and the results from the Padding operation.

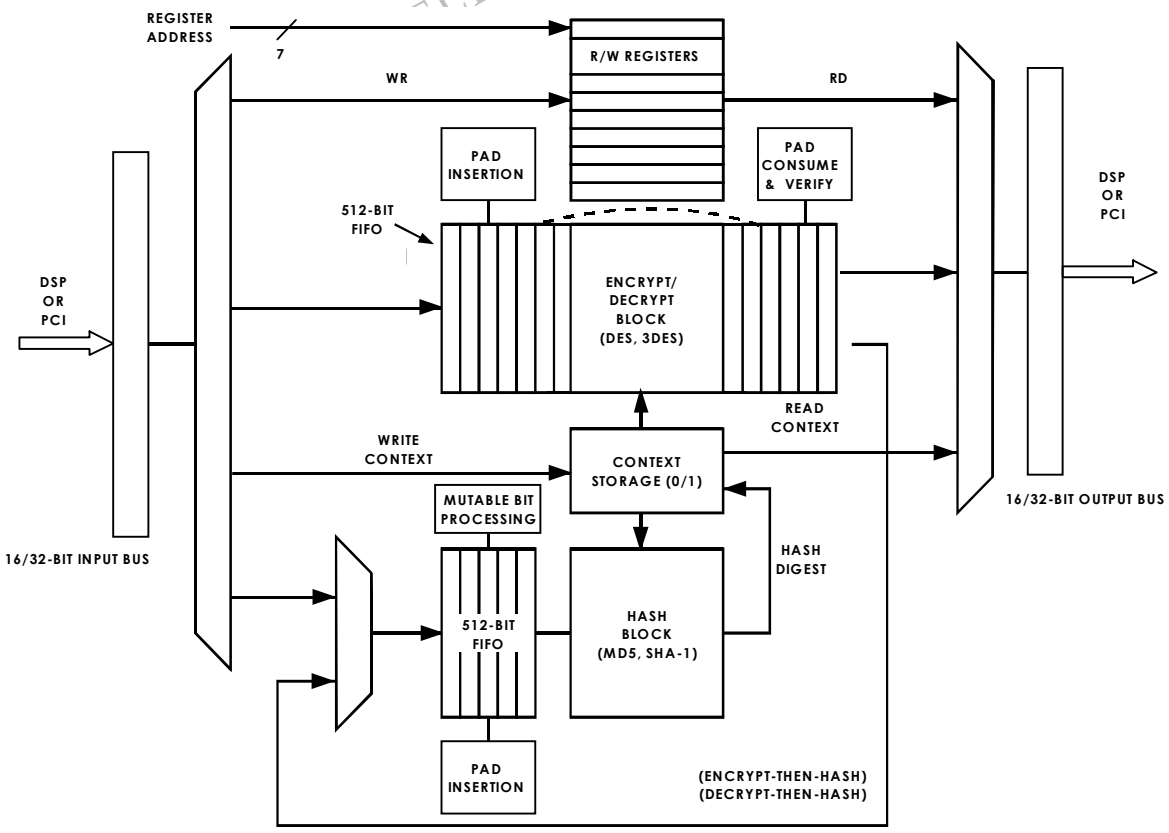


Figure 5 Hash/Encrypt Functional Block Diagram

Crypto Contexts

There are two sets of *crypto-context* registers. Each context contains a DES or Triple DES key, Initialization Vector (IV), and pre-computed hashes (inner and outer) of the Authentication key for HMAC operations. The contexts also contain registers to reload the byte count from a previous operation (which is part of the hashing context), as well as an IV (also called *salt*) for decrypting a Black key, if necessary.

Once a crypto-context has been loaded, and the operation defined, data is processed by writing it to a data input FIFO. At the I/O interface, data is always written to, or read from, the same address. Internally, the hash and encryption functions have separate 512-bit FIFOs, each with their own FIFO management pointers. Incoming data is automatically routed to one or both of these FIFOs depending on the operation in progress.

Output from the encryption block is read from the data output FIFO. In encrypt-hash or decrypt-hash operations, the data is also automatically passed to the hashing data input FIFO. Output from the hash function is always read from the digest register of the appropriate crypto-context.

The Initialization Vector (IV) to be used for a crypto operation can be loaded as part of a crypto-context. When an operation is complete, the same context will contain the resulting IV produced at the end, which can be saved away and restored later to continue the operation with more data.

In certain packet-based applications such as IPsec, a feature is available that avoids the need for the control software to generate and load random IVs for outgoing (encrypted) packets. Effectively, the IV register can be configured to automatically get updated with new random numbers for each encrypted packet with almost no software intervention.

Padding

When the input data is not a multiple of 8 bytes (a 64-bit DES block), the encrypt module can be configured to automatically append pad bytes. There are several options for how the padding is constructed, which are specified using the pad control word of the operation description. Options include zero padding, pad-length character padding (PKCS #7), incrementing count, with trailing pad length and next header byte (for IPsec), or fixed character padding. Note that for the IPsec and PKCS#7 pad protocols, there are cases where the padding not only fills-out the last 8-byte block, but also causes an additional 8-byte block of padding to be added.

For the Hash operations, padding is automatically added as specified in the MD-5 and SHA-1 standards. When the `Hash Final` command is issued indicating the last of the input data, the algorithm-specified padding and data count bits are added to the end of the hash input buffer prior to computing the hash.

Data Offsets

Certain security protocols, including IPsec, require portions of a data packet to be Hashed while the remainder of the data is both hashed and encrypted. The ADSP-2141 supports this requirement through the `OFFSET` register which allows specifying the number of 32-bit dwords of offset between the hash and encrypt/decrypt operations.

Black Key Loads

The cryptographic keys loaded as part of a crypto-context can be stored off-chip in a *black*, or encrypted, form. If the appropriate control bit is set (HECNTL bit 15), the DES or 3DES key will be decrypted immediately after it is written into the Context register. The hardware handles this decryption automatically. The KEK that covers the black keys is loaded in a dedicated write-only KEK register within the ADSP-2141. The IV for decrypting the Black secret key is called 'Salt' and must be stored along with the black key (as part of the context). Note that 3DES CBC mode is used for protecting 3DES Black keys and single-DES CBC is used for single-DES Black keys.

When Black keys are used, the key-decrypt operation adds a 6-cycle overhead (0.15µs @ 40MHz) for DES keys or 36-cycle overhead (0.9µs @ 40MHz) for triple-DES keys each time a new crypto-context is loaded. (Note that if the same Context is used for more than one packet operation, the Key decryption does not need to be performed again.) Depending on the sequencing of operations, this key decryption may in fact be hidden (from a performance impact perspective) if other operations are underway. This is because the Black key decryption process only requires that the DES hardware be available. For example, if the DSP is reading the previous Hash result out of the output FIFO, the Black Key decryption can be going on in parallel. Also note that the data driver firmware does NOT have to wait for the key to be decrypted before writing data to the input FIFO. The hardware automatically waits for the key to be decrypted before beginning to process data for a given packet. So it is possible to make the impact of black key essentially zero with efficient pipeline programming.

The Key Encryption Key (KEK) for key decryption is loaded via the Secure Kernel firmware using one of the CGX Key Manipulation commands. (For more information, see “Command Summary” on page 26.) This KEK is typically the same for all black keys, since it is usually protecting local storage only. It is designated the DKEK in the CGX API.

One of the Laser Programmed configuration bits specifies whether Red (Plaintext) keys are allowed to be loaded into the ADSP-2141 from a Host. If the AllowRedKeyLoad Laser bit is not set, keys may only be loaded in their *Black* form. This is useful in systems where export restrictions limit the key length which may be used or where the external storage environment is untrusted. If the AllowRedKeyLoad bit is set, then keys may either be loaded either in their Black form, or in the *Red* or unencrypted form. Note that the Laser Configuration bit may be overridden with a signed Enabler Token. (For more information, see “Laser Variable Storage” on page 14.)

Depending on the definition of the 'Security Module Boundary' in a given application, FIPS 140-1 may require the use of black key to protect key material. In other words, if the Security Boundary does not enclose the database where keys are stored, then those keys must be protected from compromise. Black key is a satisfactory way to meet this FIPS requirement.

Random Number Generator (RNG) Block

The Random Number Generator is designed to provide highly random, non-deterministic binary numbers at a high delivery rate with little software intervention. The random numbers are accessible to the Kernel firmware in a 16-bit register which may be read by the DSP in Kernel mode. Once the register is read, the RNG immediately generates a new 16-bit value which is available within 3.2µs.

All Application-level access to Random numbers should occur through the Kernels CGX_RANDOM command (see “Command Summary” on page 26).

The Random Number Generator is designed using a “shot noise” true entropy source which is sampled by the master 40MHz clock of the ADSP-2141. The entropy source then feeds a complex non-linear combinatorial circuit which produces the final RNG output based on the interaction of the entropy source and the 40 MHz system clock. Over 200 stages of Linear Feedback Shift Register (LFSR) are incorporated into the RNG design.

In order to facilitate FIPS 140-1 compliance, an option may be selected during CGX Kernel initialization to enable an ANSI X9.17 Annex C post-randomizer to be applied to the output of the RNG. This randomizer applies the DES ECB algorithm multiple times to further disperse and whiten the random source. Although this is not necessary to insure the quality of the random numbers, it meets the criteria for a NIST-approved random number generation algorithm.

Public Key Accelerator (PKAC)

The Public Key Arithmetic Coprocessor (otherwise known as a *BigNum* processor) is designed to support long vector calculations of the kind needed to perform RSA, Diffie-Hellman, and Elliptic Curve operations.

The PKAC can perform multiplication, squaring, addition, and subtraction on arbitrary length bit vectors. The CGX software is responsible for setting the address register for the operands and result, as well as specifying the length and operation type. Once the operation type field is written, the processor polls the Operation Complete status while the calculation is carried out.

The PKAC utilizes the Protected Kernel RAM for input, output, and intermediate variable storage. It may only be accessed from the Secure Kernel mode. Since Public Key computations typically take many milliseconds to complete, they may be preempted using a DSP interrupt.

Most application interaction with the Public Key Accelerator will occur via the CGX software interface (see “COMMAND INTERFACE” on page 25). Both high-level Public Key operations such as RSA Sign or Create Diffie-Hellman Key, as well as Primitive operations such as Multiply Vector, Add Long Vector, etc. are presented via the CGX interface.

PCI/Cardbus Interface

The ADSP-2141 appears as a Target on the PCI Bus as a single contiguous memory space of 128k bytes. In this memory space, the Host can access the following:

- The unprotected internal crypto registers of the ADSP-2141
- IDMA access to the DSP’s internal program memory (PM) and data memory (DM)
- Paged access to external memory connected to the ADSP-2141
- The Kernel RAM (KRAM) if it has been unprotected by an Extended Mode Program

As a PCI Master, the ADSP-2141 can transfer data between:

- The unprotected internal crypto registers and FIFO’s of the ADSP-2141 and PCI Host memory
- External memory and PCI Host memory

A 32-bit DMA engine within the ADSP-2141 facilitates these transfers and permits full PCI bandwidth use.

Serial EEPROM Interface

The Serial EEPROM interface allows the ADSP-2141 to automatically read the PCI configuration parameters at chip power-up. IRE can provide the data content for the EEPROM to properly set the chip device Vendor ID, Type, and Properties for full compliance with the PCI Plug and Play standards.

In addition to being used for storage of Host bus parameters, any extra space in the EEPROM may be accessed by the DSP, either in User Mode or Kernel Mode. Support for this function is not included in the standard CGX command set, however IRE can provide details of operation in order for an application on the DSP to access EEPROM memory.

Interrupt Controller

The DSP core of the ADSP-2141 provides a powerful set of interrupt sources. A total of 14 interrupt sources are available, although two pairs are multiplexed, yielding 12 simultaneous sources.

Table 1 Interrupt Sources

Internal Interrupt Sources		External Interrupt Sources	
Interrupt	Notes	Interrupt	Notes
Reset	or Power Up (PUCR=1)	$\overline{\text{IRQ2}}$	Edge or level sensitive
Power Down		$\overline{\text{IRQL1}}$	Level sensitive
SPORT0 Transmit		$\overline{\text{IRQL0}}$	Level sensitive
SPORT0 Receive		$\overline{\text{IRQE}}$	Edge sensitive
BDMA Interrupt		IRQ1	Edge or level sensitive
SPORT1 Transmit	Mixed with IRQ1	IRQ0	Edge or level sensitive
SPORT1 Receive	Mixed with IRQ0		
Timer			

The ADSP-2141 enhances the existing Interrupt controller within the ADSP-218x DSP Core with some additional functions related to the Crypto functional blocks and the external Host bus interfaces. Two additional Interrupt Controller subsystems have been added to the basic Interrupt Controller as shown in Figure 6 below:

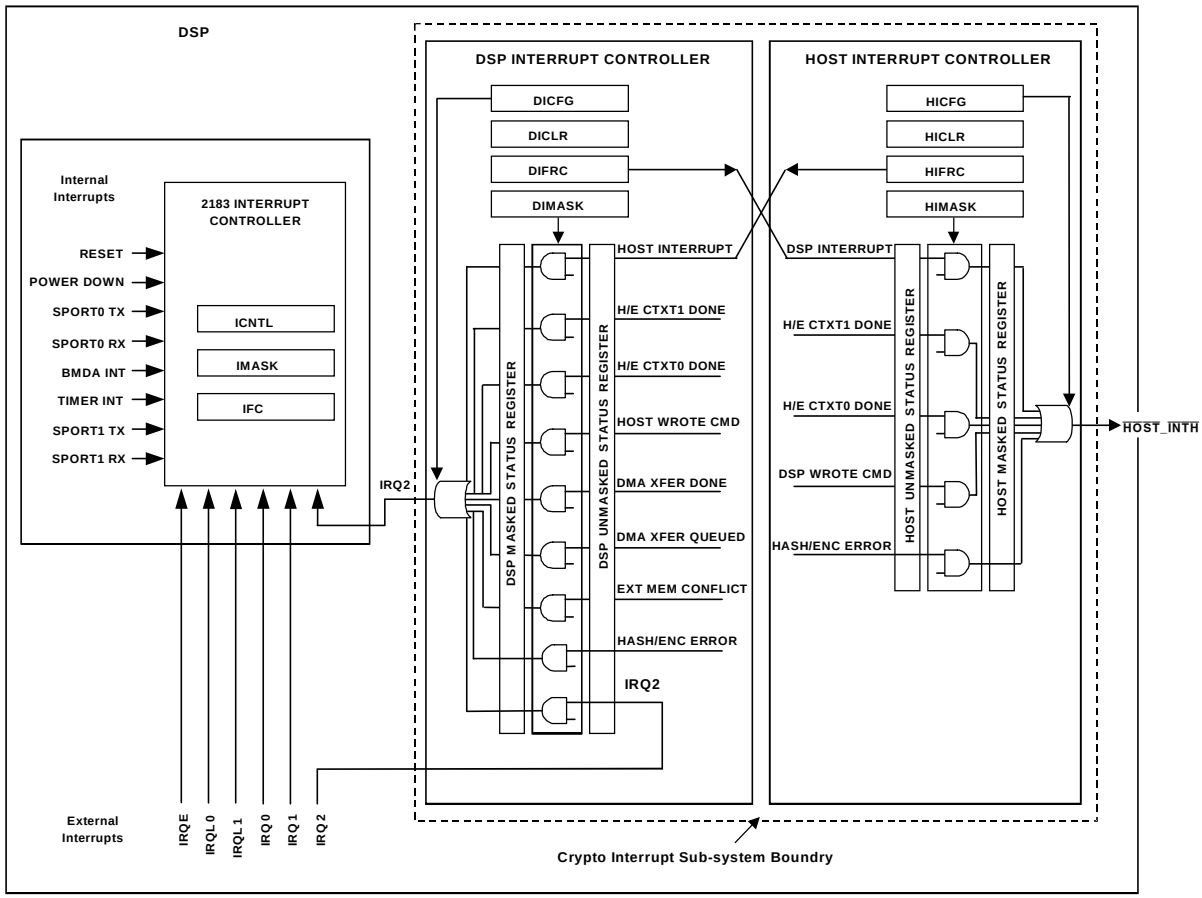


Figure 6 Interrupt Controller Block Diagram

The DSP Interrupt Controller allows programming between 1 and 9 sources for the IRQ2 interrupt to the DSP. The DMASK register provides the Mask to select which interrupt source is enabled. A pair of status registers, DUMSTAT and DMSTAT, allow the DSP firmware to read the status of any interrupt source either before or after the Mask is applied.

The Host Interrupt Controller allows programming between 1 and 5 sources for the PF7/$\overline{\text{INT\_H}}$ interrupt output signal (which may be connected to the interrupt input of the Host system). The HMASK register provides the Mask to select which interrupt source is enabled. A pair of status registers, HUMSTAT and HMSTAT, allow the Host firmware to read the status of any interrupt source either before or after the Mask is applied.

Laser Variable Storage

The Laser Variables are configured through 256 Fuses in the ADSP-2141 which are programmed during IC manufacture. Each ADSP-2141 produced is programmed with a unique set of Laser Variables.

- Local Storage Variable (LSV – the Master Key-Encryption-Key)
- Internal Seed Variable

- 48-bits Program Control Data (Enables/Disables various features and configures the ADSP-2141)
- CRC of the Laser Data (to verify integrity of the laser bits)

The Local Storage Variable (LSV) is a unique Triple DES Master Key-Encrypting-Key which allows the ADSP-2141 to securely store data (primarily other Keys) off-chip for later reloading. This is necessary if more storage space is needed than is available with on-chip RAM, or if Keys need to be saved and restored after a power outage. Each ADSP-2141 produced is programmed with a unique, randomly generated Local Storage Variable.

The Internal Seed Variable is used to randomly initialize the RNG circuits before the entropy is mixed in. Each ADSP-2141 produced is programmed with a unique, randomly generated Internal Seed Variable which is loaded into the RNG at chip boot time and cannot ever be read by software.

The 48 Program Control Data Bits (PCDBs) include configuration for permitted Key Lengths, Algorithm Enables, Red KEK loading, Internal IC Pulse Timing Characteristics, etc. The PCDBs provide configuration data which falls into 3 categories:

- Internal IC pulse-timing characteristics
- ADSP-2141 Hardware Version Number field
- ADSP-2141 Feature Enables

The first two categories consist of data which cannot be altered once the ADSP-2141 has been fabricated.

The Feature Enables can be overridden using a Factory Token Enabler which may be passed to the CGX kernel as part of the `CGX_INIT` command. This token is digitally signed with an IRE Private key and verified internal to the ADSP-2141 with its Public Key. The `CGX_INIT` command is documented in the *ADSP-2141 CGX Interface Programmer's Guide* (available from IRE).

I/O DESCRIPTION

This section describes the physical I/O hardware on the ADSP-2141.

PIN FUNCTIONS

Table 2 Pin Function Descriptions

Pin Name	# of Pins	Input/ Output	Function
External Memory Bus			
Address [25:0]	26	O	Address Output Pins for Program, Data, Byte & I/O Spaces (13-bits 2183, 13-bits from overlay register)
Data [31:0]	32	I/O	Data I/O Pins for Program and Data Memory Spaces D31:0 are used for wide-bus data memory D23:0 are used for DSP Program RAM D15:0 are used for DSP Data RAM D15:8 are used for byte memory *D23:16 are also used as Byte Space Addresses*
Interrupts			
$\overline{\text{IRQ2}}$	1	I	Edge or Level-Sensitive Interrupt Request
$\overline{\text{IRQL0}}$ $\overline{\text{IRQL1}}$	2	I	Level-Sensitive Interrupt Requests
$\overline{\text{IRQE}}$	1	I	Edge-Sensitive Interrupt Request
Bus Signals			
$\overline{\text{BR}}$	1	I	Bus Request Input
$\overline{\text{BG}}$	1	O	Bus Grant Output
$\overline{\text{BGH}}$	1	O	Bus Grant Hung Output
$\overline{\text{PMS}}$	1	O	Program Memory Select Output
$\overline{\text{DMSL}}$	1	O	Data Memory Select Output (Lower 16 bits for 32-bit DM)
$\overline{\text{DMSH}}$	1	O	Upper Memory Select Output (Upper 16 bits for 32-bit DM, not used for 16-bit DM)
$\overline{\text{BMS}}$	1	O	Byte Memory Select Output
$\overline{\text{IOMS}}$	1	O	I/O Space Memory Select Output
$\overline{\text{CMS}}$	1	O	Combined Memory Select Output ($\overline{\text{PMS}}$, $\overline{\text{DMS}}$*, $\overline{\text{IOMS}}$, $\overline{\text{BMS}}$)
$\overline{\text{RD}}$	1	O	Memory Read Enable Output
$\overline{\text{WR}}$	1	O	Memory Write Enable Output

*When $\overline{\text{DMS}}$ is enabled for generation of $\overline{\text{CMS}}$, the $\overline{\text{CMS}}$ is activated for DSP access to external memory only, NOT for DMA controller accesses

Table 2 Pin Function Descriptions (Continued)

Pin Name	# of Pins	Input/ Output	Function	
Misc.				
MMAP	1	I	Memory Map Select Input (1 = overlay external at 0x0000)	
BMODE	1	I	Boot Option Control Input (0 = BDMA, 1 = IDMA)	
CLKIN, XTAL	2	I	Clock or Quartz Crystal Input (1/2 of the ADSP-2141 clock)	
CLKOUT	1	O	Processor Clock Output	
Serial Ports				
SPORT0				
SCLK0	1	I/O	Serial Port 0 Clock	
DR0	1	I	Serial Port 0 Receive Data Input	
RFS0	1	I/O	Serial Port 0 Receive Frame Sync	
DT0	1	O	Serial Port 0 Transmit Data Output	
TFS0	1	I/O	Serial Port 0 Transmit Frame Sync	
SPORT1				
Port Configuration (System Control Reg) —>			1 = Serial Port	0 = Other
SCLK1	1	I/O	Serial Port 1	Clock
DR1	1	I	Serial Port 1 Receive Data Input	Flag In
RFS1	1	I/O	Serial Port 1 Receive Frame Sync	IRQ0
DT1	1	O	Serial Port 1 Transmit Data Output	Flag Out
TFS1	1	I/O	Serial Port 1 Transmit Frame Sync	IRQ1
Power-Down				
$\overline{\text{PWD}}$	1	I	Power-Down Initiate Control	
PWDACK	1	O	Power-Down Acknowledge	
Flags				
PF6:0	7	I/O	Programmable I/O Pins	
PF7/$\overline{\text{INT\_H}}$	1	I/O	Programmable I/O Pin –or–Interrupt Output (Host mode)	
Emulator				

Table 2 Pin Function Descriptions (Continued)

Pin Name	# of Pins	Input/ Output	Function
EE	1		(Emulator Only)
$\overline{\text{EBR}}$	1		(Emulator Only)
$\overline{\text{EBG}}$	1		(Emulator Only)
$\overline{\text{ERESET}}$	1		(Emulator Only)
$\overline{\text{EMS}}$	1		(Emulator Only)
$\overline{\text{EINT}}$	1		(Emulator Only)
ECLK	1		(Emulator Only)
ELIN	1		(Emulator Only)
ELOUT	1		(Emulator Only)
Serial EEPROM Interface			
EE_DI	1	O	Serial EEPROM Data In
EE_DO	1	I	Serial EEPROM Data Out
EE_CS	1	O	Serial EEPROM Chip Select
EE_SK	1	O	Serial EEPROM Clock
Bus Select			
BUS_MODE	1	I	Processor Bus Select
BUS_SEL	1	I	Bus Select
PCI Bus (dedicated pins)			
PCI_CLK	1	I	PCI Clock
PCI_PAR	1	I/O	PCI Parity Bit
PCI_IRDY	1	I/O	PCI Initiator Ready
PCI_STOP	1	I/O	PCI Abort Transfer

Bus Mode Pin Descriptions

Table 3 shows the multiplexed pins in 2183 and PCI mode. For more information on the PCI pins listed in bold, see Table 5 on page 20.

Table 3 Pin Function Descriptions—Bus Mode

Bus Mode			2183 Mode (bus_mode = 0, bus_sel = 1)	PCI Mode (bus_mode = 1, bus_sel=0)
MPLX_RESET	1	I	RESET_1	Pci_$\overline{rst}$
MPLX1	1	I/O		Pci_$\overline{cbe3}$
MPLX2	1	I/O		Pci_$\overline{cbe2}$
MPLX3	1	I/O		Pci_$\overline{cbe1}$
MPLX4	1	I/O		Pci_$\overline{cbe0}$
MPLX5	1	I	$\overline{IRD}$	Pci_idsel
MPLX6	1	I	$\overline{IWR}$	Pci_$\overline{gnt}$
MPLX7	1	I/O	IS	Pci_$\overline{frame}$
MPLX8	1	I/O	IAL	Pci_$\overline{devsel}$
MPLX9	1	I/O	$\overline{IACK}$	Pci_$\overline{trdy}$
MPLX10	1	I/O	FL0	Pci_$\overline{perr}$
MPLX11	1	I/O	FL1	Pci_$\overline{serr}$
MPLX12	1	O	FL2	Pci_$\overline{req}$
MPLX_BUS[31:0]	32	I/O	IAD15:0 N/C31:16	Pci_ad15:0 Pci_ad31:16
Power				
GND	24	-	Ground Pins	
VDD	22	-	Power Supply Pins (3.3V)	
Total:	208	Includes the pins from Tables 2 & 3.		

IDMA Mode Multiplex Bus Pin Definition

Table 4 IDMA Mode Multiplex Bus Pin Definition

IDMA Port (218x Mode)				
Pin Name	IDMA Name	Pins	I/O	Description
MPLX5	$\overline{\text{IRD}}$	1	I	IDMA Port Read Input
MPLX6	$\overline{\text{IWR}}$	1	I	IDMA Port Write Input
MPLX7	IS	1	I	IDMA Port Select
MPLX8	IAL	1	I	IDMA Port Address Latch
MPLX9	$\overline{\text{IACK}}$	1	O	IDMA Port Access Ready Acknowledge
MPLX10	FL0	1	O	Output Flags
MPLX11	FL1	1	O	Output Flags
MPLX12	FL2	1	O	Output Flags
MPLX_BUS	IAD	16	I/O	IDMA Data I/O

Table 5 PCI Mode Multiplex Bus Pin Definitions

PCI Port				
Pin Name	IDMA Name	Pins	I/O	Description
MPLX1	Pci_$\overline{\text{cbe3}}$	1	I/O	Bus Command / Byte Enable 3
MPLX2	Pci_$\overline{\text{cbe2}}$	1	I/O	Bus Command / Byte Enable 2
MPLX3	Pci_$\overline{\text{cbe1}}$	1	I/O	Bus Command / Byte Enable 1
MPLX4	Pci_$\overline{\text{cbe0}}$	1	I/O	Bus Command / Byte Enable 0
MPLX5	Pci_idsel	1	I	Initialization Device Select
MPLX6	Pci_$\overline{\text{gnt}}$	1	I	Bus Grant
MPLX7	Pci_$\overline{\text{frame}}$	1	I/O	Cycle Frame
MPLX8	Pci_$\overline{\text{devsel}}$	1	I/O	Device Select
MPLX9	Pci_$\overline{\text{trdy}}$	1	I/O	Target Ready
MPLX10	Pci_$\overline{\text{perr}}$	1	I/O	Parity Error
MPLX11	Pci_$\overline{\text{serr}}$	1	I/O	System Error
MPLX12	Pci_$\overline{\text{req}}$	1	O	PCI Bus Request

Table 5 PCI Mode Multiplex Bus Pin Definitions

PCI Port				
MPLX_BUS	Pci_ad15:0 Pci_ad31:16	32	I/O	PCI Address/Data Bus
PF7/$\overline{\text{INT\_H}}$	Pci_$\overline{\text{intA}}$	1	O	PCI Interrupt A request

SYSTEM INTERFACE

The ADSP-2141 may be integrated into a wide variety of systems, including those which already have a microprocessor and those which will use the ADSP-2141 as the main processor. The device can be configured into one of 2 Host Bus modes: IDMA or PCI.

IDMA Bus Mode

The IDMA Bus Mode operates the same as in a native ADSP-218x device, as described in this section.

The IDMA Port provides an efficient means of communication between a host system and the ADSP-2141. The port is used to access the on-chip program memory and data memory of the DSP with only one DSP cycle per word overhead. The IDMA port cannot, however, be used to write to the DSP's memory-mapped control registers.

The IDMA port has a 16-bit multiplexed address and data bus, and supports reading or writing 16-bit data (DM) or 24-bit program memory (PM). The IDMA port is completely asynchronous and can be written to while the ADSP-2141 is operating at full speed.

The DSP memory address is latched and then automatically incremented after each IDMA transaction. An external device can therefore access a block of sequentially addressed memory by specifying only the starting address of the block. This increases throughput as the address does not have to be sent for each memory access.

The IDMA Port access occurs in two phases. The first is the IDMA Address Latch cycle. When the acknowledge is asserted, a 14-bit address and 1-bit destination type can be driven onto the bus by an external device. The address specifies an on-chip memory location; the destination type specifies whether it is a DM or PM access. The falling edge of the address latch signal latches this value to the IDMAA register.

Once the address is stored, data can either be read from or written to the ADSP-2141's on-chip memory. Asserting the select line ($\overline{\text{IS}}$) and the appropriate read or write line ($\overline{\text{IRD}}$ and $\overline{\text{IWR}}$ respectively) signals the ADSP-2141 that a particular transaction is required. In either case, there is a one-processor-cycle delay for synchronization. The memory access consumes an additional processor cycle.

Once an access has occurred, the latched address is automatically incremented and another access can occur.

Through the IDMAA register, the ADSP-2141 can also specify the starting address and data format for DMA operation.

Figure 7 below illustrates a typical system configuration for the IDMA mode.

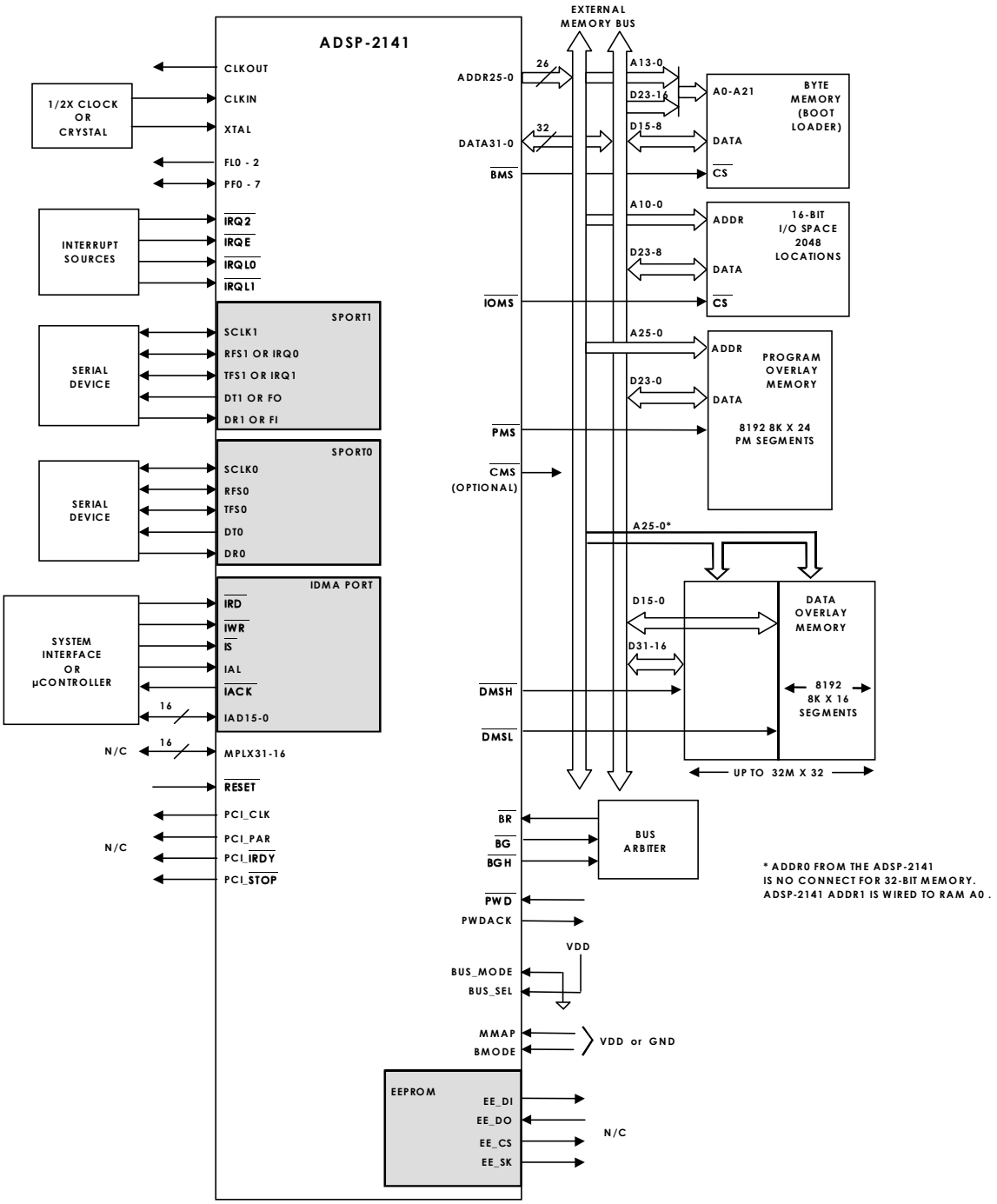


Figure 7 ADSP-2141 IDMA System Configuration

PCI Bus Mode

Figure 8 below illustrates a typical system configuration for the PCI mode.

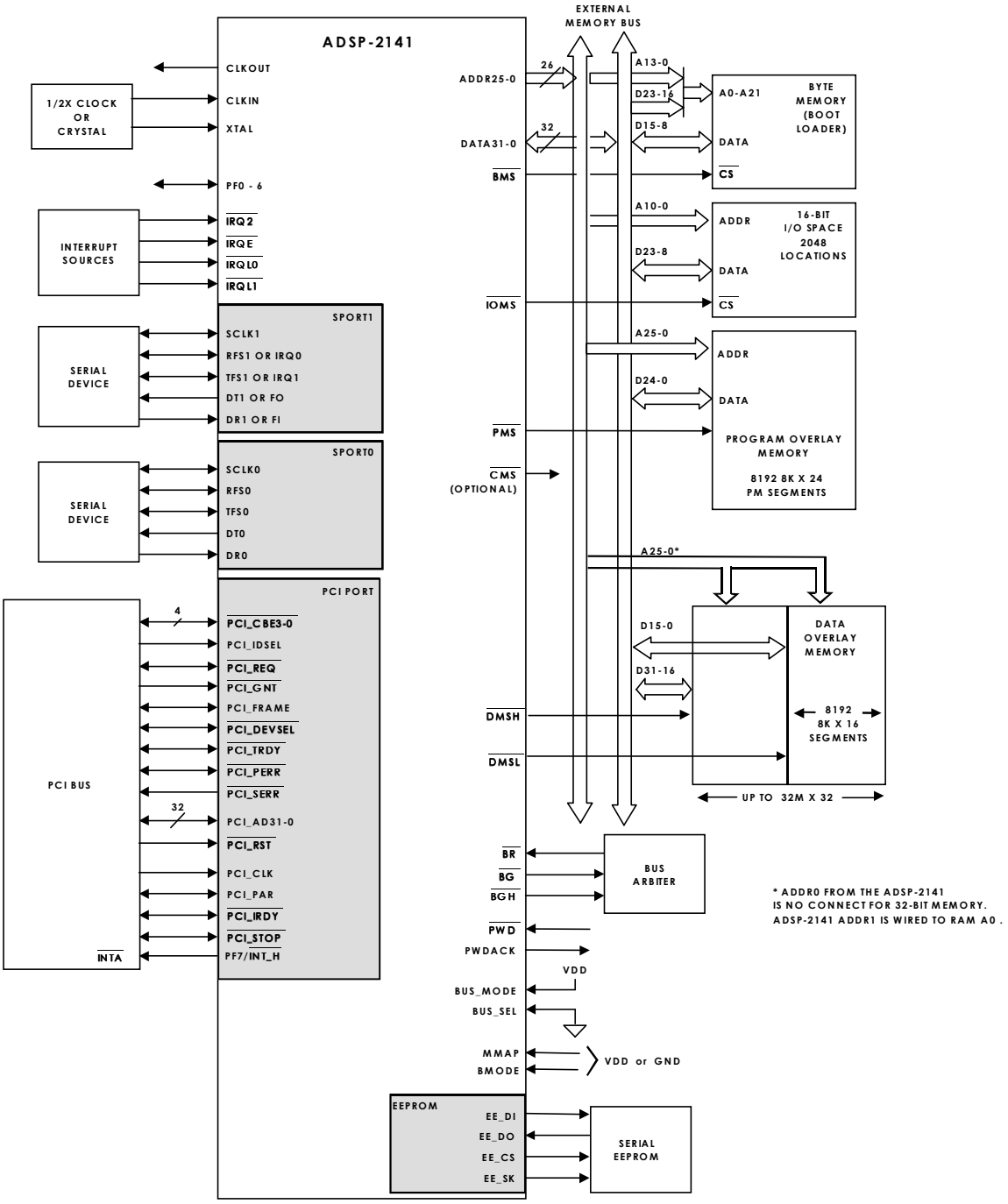


Figure 8 ADSP-2141 PCI System Configuration

DEVICE OPERATION

OPERATIONAL MODES

Security Modes

The ADSP-2141 operates in one of two Security Modes: Kernel Mode or User Mode. The mode switching is performed on-the-fly as Program execution proceeds. Kernel Mode is entered via a jump or Call to address 0x2000 with PMOVLAY set to 0x000F. Kernel Mode will exit on its own once it has completed a requested operation (or terminates due to an error).

Special Interrupt handling is performed if the DSP is executing in Kernel Mode. While executing a CGX command in Kernel Mode, it is possible to interrupt to a non-protected vector location and then invoke the Kernel again during the interrupt handler. The [IF CONDITION] RTI instruction must be used to return to the Kernel from the interrupt handler. The return address and PMOVLAY page must match the interrupted address and PMOVLAY page. If not, the violation reset logic will be triggered. Only one level of Kernel Mode nesting is permitted. An interrupt to a non-protected vector location while in Nested Kernel Mode will also trigger the violation reset logic.

While in Kernel Mode, it is possible to interrupt to a protected vector location. In this case, the processor remains in Kernel Mode. The [IF CONDITION] RTI instruction must be used to return the processor from the interrupt handler. There is no imposed limit to the number of nested interrupts to a protected vector location.

Bus Modes

The ADSP-2141 Host Bus may be configured for one of 2 personalities: IDMA Mode or PCI Bus Mode. The selection of mode is made with 2 Hardware control inputs BUS_MODE and BUS_SEL at boot time.

Table 6 Bus Mode Selection

Bus Mode Pins	BUS_MODE	BUS_SEL
IDMA Mode	0	1
PCI Bus Mode	1	0

This selection may not be changed after the ADSP-2141 comes out of power-up Reset. It is typically expected that the Bus Mode signals are tied to ground or V_{DD} on the PC Board.

Boot Modes

The ADSP-2141 may be bootstrap-loaded from one of 3 sources: Byte-wide memory, Host Processor Bus, or External Program memory. The selection of mode is made with 2 Hardware control inputs BMODE and MMAP. When the Host Processor boot mode is selected, any one of the 2 Bus Modes may be used.

Table 7 Boot Mode Selection

Boot Mode Pins	BMODE	MMAP
Byte-wide (BDMA) Boot Mode	0	0
Host Bus (IDMA) Boot Mode	1	0
External Program Boot Mode	0	1

The hardware pin states are not relevant after the ADSP-2141 comes out of power-up Reset.

Refer to the *ADSP-2141 User's Manual* (available from IRE) for information on BDMA, IDMA and External Program boot modes.

COMMAND INTERFACE

This section provides a general overview of the software Command Interface to the Crypto Functions in the ADSP-2141. Refer to the *ADSP-2141 CGX Interface Programmer's Guide* (available from IRE) for more details.

Overview

The ADSP-2141 provides an embedded crypto library which provides a Command Interface API (Application Programming Interface) to outside applications. These commands are referred to as CGX (CryptoGraphic eXtensions).

The CGX API simultaneously enforces certain security policies within the ADSP-2141 and insulates applications from the details of many complex cryptographic operations. The security policy built into the ADSP-2141 has some of the following rules:

- Unencrypted (Red) keys may never be retrieved from the ADSP-2141
- Keys within the ADSP-2141 are marked with an Attributes field which specifies key Type and Trust level
- A key's Type field must match the use in a requested operation (i.e. cannot use a KEK to encrypt traffic)
- Keys generated internal to the ADSP-2141 (i.e. from RNG) are marked as Trusted
- Keys which are negotiated or imported from outside systems are marked Untrusted (although they may still be quite secure)
- Separate Trusted and Untrusted key hierarchies may be maintained and customer applications may choose which trust level is required for a given command

For most key management operations, the CGX interface must be used. However, for certain high-performance encryption/hashing applications, the CGX interface may be bypassed and either the DSP or a Host processor may exercise direct control over the Hash/Encrypt block.

Command Summary

Approximately 40 CGX Commands are supported in the API to the ADSP-2141.

General Utilities

INIT	Initialize Secure Kernel and allow Re-configuration of the ADSP-2141
DEFAULT	Restore Factory Default Settings
RANDOM	Generate Random Numbers (between 1 and 64k bytes)
GET CHIPINFO	Return CryptoIC System Information
SELF TEST	Runs a suite of self-tests on the hardware and CGX

Symmetrical Key Management

UNCOVER KEY	Load and Decrypt a Secret Key
GEN KEY	Generate a Secret Key
GEN KEK	Generate an Internal Key Encryption Key
GEN RKEK	Generate a Key Recovery Key Encryption Key
SAVE KEY	Save a key protected by the Recovery Key (RKEK)
LOAD KEY	Import a Red (plaintext) User Secret Key
DERIVE KEY	Derive a Secret Key from a Pass Phrase
TRANSFORM KEY	Transform a Secret Key using IPSec
DESTROY KEY	Remove Secret Key from the KCR
EXPORT KEY	Export an IRE-format Secret Key
IMPORT KEY	Import an IRE-format Secret Key

Symmetrical Encryption

ENCRYPT	Encrypt Data
DECRYPT	Decrypt Data
LOAD KG	Load Secret Key into HW/SW Key Generator

Hash

HASH INIT	Initialize the Hash operator
HASH DATA	Hash Customer Data
HASH ENCRYPT	Hash and Encrypt Customer Data
HASH DECRYPT	Hash and Decrypt Customer Data

PRF Functions

MERGE KEY	Combine two secret keys into one key
MERGE LONG KEY	Combine two secret keys into a data string (long key)
EXTRACT LONG KEY	Create a secret key from a data string (long key)
PRF DATA	Hash multiple data items using HMAC
PRF KEY	Complete the above HMAC and create secret key

Asymmetrical Key Management

GEN PUBKEY	Generate a Public Keyset (Public & Private parts)
GEN NEWPUBKEY	Generate a part of a Public Keyset
GEN NEGKEY	Generate a Diffie-Hellman Derived Secret Key
EXPORT PUBKEY	Export an IRE-format Public Key
IMPORT PUBKEY	Import an IRE-format Public Key

Asymmetrical Encryption

PUBKEY ENCRYPT	Encrypt Data using RSA Public Key
PUBKEY DECRYPT	Decrypt Data using RSA Public Key

Digital Signatures

SIGN	Digitally Sign a Message
VERIFY	Verify a Digital Signature

Math Utilities

ADD VECTOR	Perform a Vector Add operation
SUB VECTOR	Perform a Vector Subtract operation
MULT VECTOR	Perform a Vector Multiply operation
EXP VECTOR	Perform a Vector Exponentiate operation
SHIFT VECTOR	Perform a Vector right or left shift operation

Extended Mode

LOAD EXTENDED	Load/Enable Extended (downloaded) Algorithm Block
EXECUTE EXTENDED	Execute Extended (downloaded) Algorithm Block

ABSOLUTE MAXIMUM RATINGS

Supply Voltage	–0.3 V to +4.6 V
Input Voltage	–0.5 V to VDD +0.5 V
Output Voltage Swing	–0.5 V to VDD +0.5 V
Operating Temperature Range (Ambient)	0^oC to $+70^oC$
Storage Temperature Range	$–65^oC$ to $+150^oC$
Lead Temperature (5 sec) MQFP	$+280^oC$

ENVIRONMENTAL CONDITIONS

The following figures assume a 4-layer JEDEC Printed Circuit Board:

$T_{AMB} = T_{CASE} – (PD \times \theta_{CA})$

T_{CASE} = Case temperature in ^oC

Table 8 Thermal Ratings: MQFP Package

Rating Description	Symbol	Value (MQFP still air)	Value (MQFP 9500fpm)
Thermal Resistance (Case to Ambient)	θ_{CA}	30.7° C/W	16.7 °C/W
Thermal Resistance (Junction to Ambient)	θ_{JA}	4.3 °C/W	4.3 °C/W
Thermal Resistance (Junction to Case)	θ_{JC}	35 °C/W	21 °C/W

Caution

ESD (electrostatic discharge) sensitive device. Electrostatic charges as high as 4000V readily accumulate on the human body and test equipment and can discharge without detection. Although the ADSP-2141L features proprietary ESD protection circuitry, permanent damage may occur on devices subjected to high energy electrostatic discharges. Therefore, proper ESD precautions are recommended to avoid performance degradation or loss of functionality.

Frequency Dependency For Timing Specifications

t_{CK} is defined as $0.5t_{CKI}$. The ADSP-2141L uses an input clock with a frequency equal to half the instruction rate: a 16.67 MHz input clock (which is equivalent to 60ns) yields a 30 ns processor cycle (equivalent to 33 MHz). t_{CK} values within the range of 0.5tCKI period should be substituted for all relevant timing parameters to obtain the specification value

Example: $t_{CKH} = 0.5t_{CK}$ - 7 ns = 0.5 (25 ns) - 7 ns = 8ns

ELECTRICAL SPECIFICATIONS

RECOMMENDED OPERATING CONDITIONS

Table 9 Recommended Operating Conditions

Parameter		K Grade Min	Max	Unit
V_{pp}	Supply Voltage	3.0	3.6	V
T_{amb}	Ambient Operating Temperature	0	+70	^oC

ELECTRICAL CHARACTERISTICS

DC Specifications

Table 10 DC Specifications

Parameter		Test Conditions	K Grades Min	Typ	Max	Unit
V_{IH}	Hi-Level Input Voltage [1, 2]	@ V_{DD} = max	2.0			V
V_{IH}	Hi-Level CLKIN Voltage	@ V_{DD} = max	2.2			V
V_{IL}	Lo-Level Input Voltage [1, 3]	@ V_{DD} = min			0.4	V
V_{OH}	Hi-Level Output Voltage [1, 4, 5]	@ V_{DD} = min I_{OH} = -0.5 mA @ V_{DD} = min I_{OH} = -100 µA[6]	2.4 V_{DD} –0.3			V V
V_{OL}	Lo-Level Output Voltage [1, 4, 5]	@ V_{DD} = min I_{OL} = 2 mA			0.4	V
V_{IH}	Hi-Level Input Current [3]	@ V_{DD} = max V_{IN} = V_{DD} max			10	µA
I_{IL}	Lo-Level Input Current [3]	3@ V_{DD} = max V_{IN} = 0 V			10	µA
I_{OZH}	Three-State Leakage Current [7]	@ V_{DD} = max V_{IN} = V_{DD} max [8]			10	µA
I_{OZL}	Three-State Leakage Current [7]	@ V_{DD} = max V_{IN} = 0 V [8]			8	µA

Table 10 DC Specifications (Continued)

Parameter	Test Conditions	K Grades Min	Typ	Max	Unit
I_{DD} Supply Current (Idle) [9, 10]	@ V_{DD} = 3.3 T_{AMB} = +25°C t_{CK} = 25 ns [11] t_{CK} = 30 ns [11] t_{CK} = 34.7 ns [11]		 22 21 20		 mA mA mA
I_{DD} Supply Current (Dynamic) [10, 12]	@ V_{DD} = 3.3 T_{AMB} = +25°C t_{CK} = 25 ns [11] t_{CK} = 30 ns [11] t_{CK} = 34.7 ns [11]		 210 180 160		 mA mA mA
C_I Input Pin Capacitance [3, 6, 13]	@ V_{IN} = 2.5 V f_{IN} = 1.0 MHz T_{AMB} = +25°C			8	pF
C_O Output Pin Capacitance [6, 7, 13, 14]	@ V_{IN} = 2.5 V f_{IN} = 1.0 MHz T_{AMB} = +25°C			8	pF

1 Bidirectional pins: D0-D31, RFS0, RFS1, SCLK0, SCLK1, TFS0, TFS1, IAD0-15, PF0-PF7

2 Input only pins: $\overline{\text{RESET}}$, $\overline{\text{IRQ2}}$, $\overline{\text{BR}}$, MMAP, DR0, DR1, $\overline{\text{PWD}}$, $\overline{\text{IRQL0}}$, $\overline{\text{IRQL1}}$, $\overline{\text{IRQE}}$, $\overline{\text{IS}}$, $\overline{\text{IRD}}$, $\overline{\text{IWR}}$, IAL.

3 Input only pins: CLKIN, $\overline{\text{RESET}}$, $\overline{\text{IRQ2}}$, $\overline{\text{BR}}$, MMAP, DR0, DR1, $\overline{\text{PWD}}$, $\overline{\text{IRQL0}}$, $\overline{\text{IRQL1}}$, $\overline{\text{IRQE}}$, $\overline{\text{IS}}$, $\overline{\text{IRD}}$, $\overline{\text{IWR}}$, IAL.

4 Output pins: $\overline{\text{BG}}$ $\overline{\text{BGH}}$, $\overline{\text{PMS}}$, $\overline{\text{DMSL}}$, $\overline{\text{DMSH}}$ $\overline{\text{BMS}}$, $\overline{\text{IOMS}}$, $\overline{\text{CMS}}$, $\overline{\text{RD}}$, $\overline{\text{WR}}$, $\overline{\text{IACK}}$, PWDACK, A0-A25, DT0, DT1, CLKOUT, FL2-0.

5 Although specified for TTL outputs, all ADSP-2141 outputs are CMOS-compatible and will drive to V_{DD} and GND, assuming no dc loads.

6 Guaranteed but not tested.

7 Output pins: $\overline{\text{BG}}$, $\overline{\text{BGH}}$ $\overline{\text{PMS}}$, $\overline{\text{DMSL}}$, $\overline{\text{BMS}}$, $\overline{\text{IOMS}}$, $\overline{\text{DMSH}}$, $\overline{\text{CMS}}$, $\overline{\text{RD}}$, $\overline{\text{WR}}$, $\overline{\text{IACK}}$, PWDACK, A0-A25, DT0, DT1, CLKOUT, FL2-0, EE_DI, EE_CS, EE_SK

8 Three-statable pins: A0-A25, D0-D31, $\overline{\text{PMS}}$, $\overline{\text{DMSL}}$, $\overline{\text{DMSH}}$ $\overline{\text{BMS}}$, $\overline{\text{IOMS}}$, $\overline{\text{CMS}}$, $\overline{\text{RD}}$, $\overline{\text{WR}}$, DT0, DT1, SCKL0, SCLK1, TFS0, TFS1, RFS0, RFS1, IAD0-IAD15, PF0-PF7.

9 Idle refers to ADSP-2141 state of operation during execution of IDLE Instruction. Deasserted pins are driven to either V_{DD} or GND.

10 Current reflects device operating with no output loads.

11 Applies to MQFP package type.

12 Output pin capacitance is the capacitive load for any three-stated output pin.

Specifications subject to change without notice.

DC Specifications – PCI Bus Pins

Table 11 DC Specifications - PCI Bus Pins

Parameter		Test Conditions	Min	Max	Unit
V_{IH}	Hi-Level Input Voltage [1,2]		0.5 V_{DD}	V_{DD} + 0.5	V
V_{IL}	Lo-Level Input Voltage [1,2]		-0.5	0.3 V_{DD}	V
V_{OH}	Hi-Level Output Voltage [1,3]	I_{OUT} = -500 µA	0.9 V_{DD}		V
V_{OL}	Lo-Level Output Voltage [1,3]	I_{OUT} = 1500 µA		0.1 V_{DD}	V
I_{IH}	Hi-Level Input Current [2]	0 < V_{IN} < V_{DD}		10	µA
I_{IL}	Lo-Level Input Current [2]	0 < V_{IN} < V_{DD}		10	µA
I_{OZH}	Three-State Leakage Current [1]	0 < V_{IN} < V_{DD}		10	µA
I_{OZL}	Three-State Leakage Current [1]	0 < V_{IN} < V_{DD}		10	µA
C_I	Input Pin Capacitance	T_{AMB} = +25°C		10	pF
C_{CLK}	PCI CLK Pin Capacitance	T_{AMB}= +25°C	5	12	pF
C_{IDSEL}	PCI IDSEL Pin Capacitance [5]	T_{AMB}= +25°C		8	pF
L_{pin}	Pin Inductance			20	nH

1 Bidirectional pins: MPLX_BUS [31:0}, MPLX1-4, MPLX7-10, MPLX12
2 Input only pins: MPLX_RESET, MPLX5, MPLX6, PCI_CLK, PCI_PAR, PCI_IRDY, PCI_STOP
3 Output only pins: MPLX11
4 Leakage currents include hi-Z output leakage for bi-directional buffers with three-state outputs.
5 Lower capacitance of IDSEL (MPLX_5) input-only pin allows for non-resistive connection to Address/Data bus.

TIMING PARAMETERS ADSP-2141L

PCI Clock (Guaranteed Over Operating Temperature and Digital Supply Range)

The ADSP-2141 is targeted for use in PCI add-on I/O slave card designs. It provides a glueless interface to the PCI bus. All bus drivers are compliant with PCI interface electrical switching and drive capability specifications.

The ADSP-2141 does not implement the following signals: $\overline{\text{LOCK}}$, $\overline{\text{REQ}}$, $\overline{\text{GNT}}$ $\overline{\text{INTB}}$, $\overline{\text{INTC}}$, $\overline{\text{INTD}}$, $\overline{\text{SBO}}$, $\overline{\text{SDONE}}$, $\overline{\text{CLKRUN}}$, AD[64:32], $\overline{\text{C/BE}}$[7:4], $\overline{\text{REQ}}$64, $\overline{\text{ACK}}$64, PAR64.

Parameter		Min	Max	Unit
Timing Requirements:				
t_{CYC}	CLK Cycle Time	30	100	ns
t_{HIGH}	CLK High Time	11		ns
t_{LOW}	CLK Low Time	11		ns
	CLK Slew Rate[1]	1	4	V/ns
	$\overline{\text{RST}}$ Slew Rate[2]	50		mV/ns

1. Rise and fall times are specified in terms of the edge rate measured in V/ns. This slew rate must be met across the minimum peak-to-peak portion of the waveform as shown in Figure 9
2. The Minimum $\overline{\text{RST}}$ slew rate applies only to the rising (deassertion) edge of the reset signal, and ensures that system noise cannot render an otherwise monotonic signal to appear to bounce in the switching range.

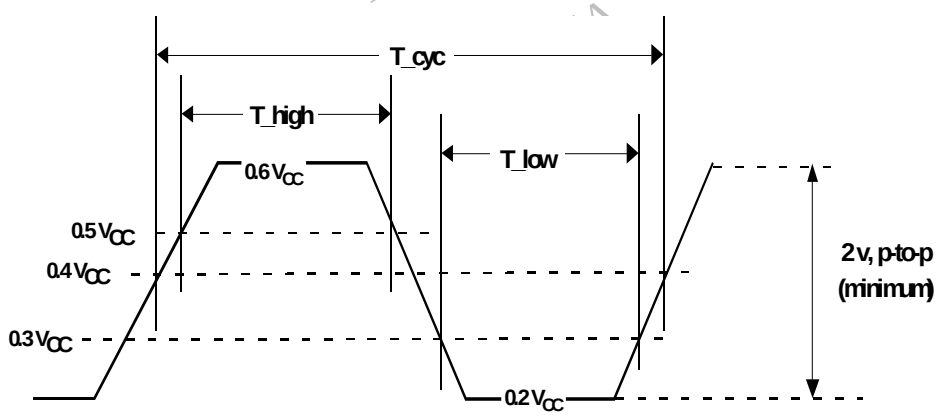


Figure 9 Clock Waveform

TIMING PARAMETERS ADSP-2141L

PCI Bus Interface

Parameter		Min	Max	Unit
Timing Requirements:				
t_{VAL}	CLK to Signal Valid	2	11	ns
t_{ON}	CLK to Low Z Delay	2		ns
t_{OFF}	CLK to High Z Delay		28	ns
t_{SU}	Input Setup to CLK	7		
t_H	Input Hold After CLK	0		ns
$t_{RST-OFF}$	RST# Active to Outputs High-Z		40	ns

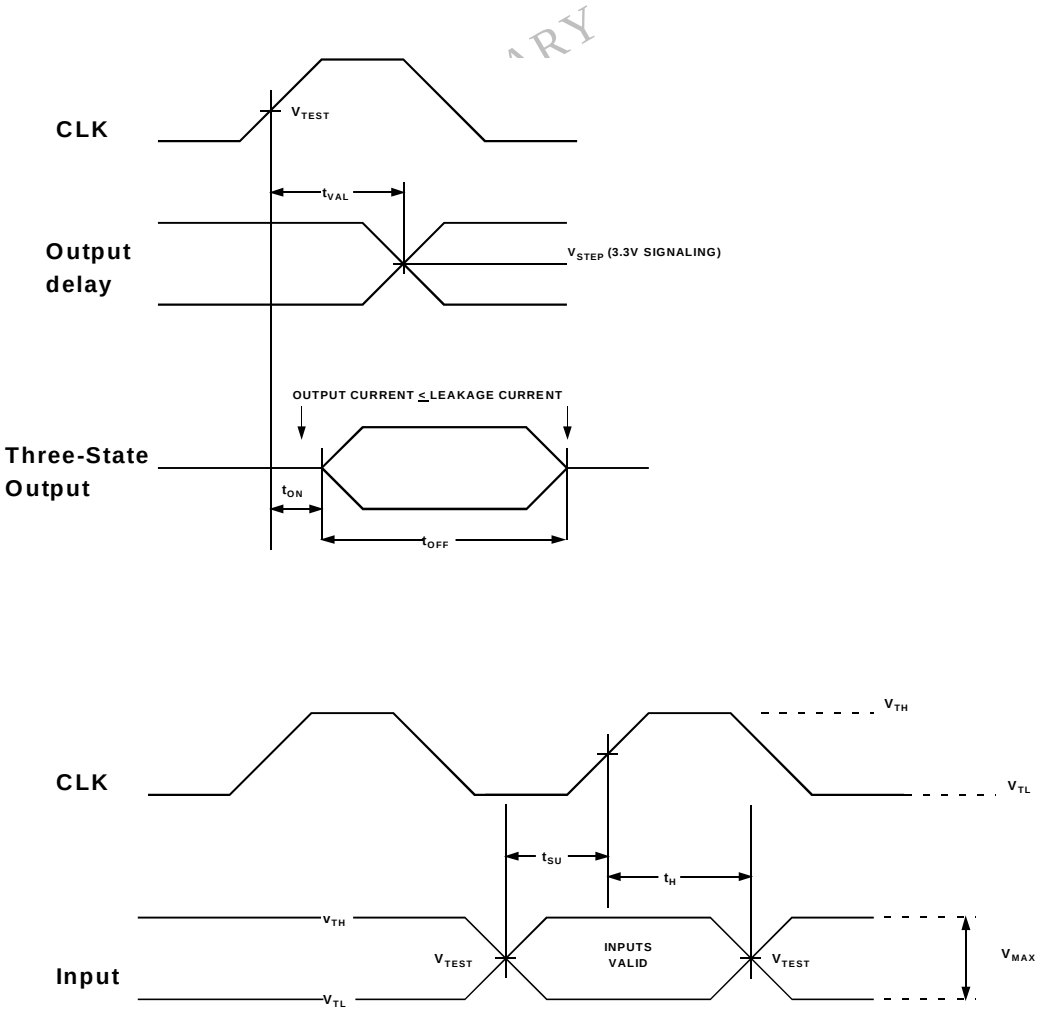


Figure 10 Output (top) and Input Timing Measurement Conditions

TIMING PARAMETERS ADSP-2141L

Clock Signals and Reset

Parameter		Min	Max	Unit
Timing Requirements:				
t_{CKI}	CLKIN Period	50	100	ns
t_{CKIL}	CLKIN Width Low	15		ns
t_{CKIH}	CLKIN Width High	15		ns
Switching Characteristics:				
t_{CKL}	CLKOUT Width Low	$0.5t_{CK}$ - 7		ns
t_{CKH}	CLKOUT Width High	$0.5t_{CK}$ - 7		ns
t_{CKOH}	CLKIN High to CLKOUT High	0	20	ns
Control Signals Timing Requirements:				
t_{RSP}	$\overline{\text{RESET}}$ Width Low[1]	$5t_{CK}$		ns

NOTE:

1. Applies after powerup sequence is complete. Internal phase lock loop requires no more than 2000 CLKIN cycles assuming stable CLKIN (not including crystal oscillator start-up time)

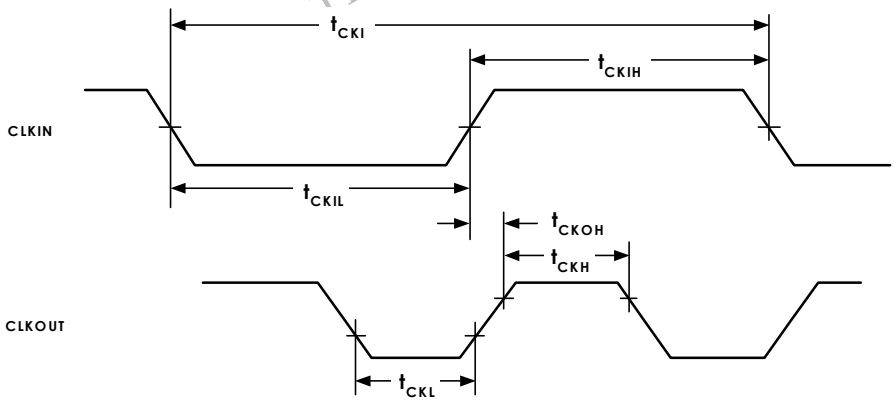


Figure 11 Clock Signals and Reset

TIMING PARAMETERS ADSP-2141L

Interrupts and Flags

Parameter		Min	Max	Unit
Timing Requirements:				
t_{IFS}	$\overline{IRQx}$, FI, or PFx Setup before CLKOUT Low[1, 2, 3, 4]	$0.25t_{CK}$ + 15		ns
t_{IFH}	$\overline{IRQx}$, FI, or PFx Hold after CLKOUT High[1, 2, 3, 4]	$0.25t_{CK}$		ns
Switching Characteristics:				
t_{FOH}	Flag Output Hold after CLKOUT Low[5]	$0.25t_{CK}$ - 7		ns
t_{FOD}	Flag Output Delay from CLKOUT Low[5]		$0.5t_{CK}$ + 5	ns

NOTES

1. If $\overline{IRQx}$ and FI inputs meet t_{IFS} and t_{IFH} setup/hold requirements, they will be recognized during the current clock cycle; otherwise the signals will be recognized on the following cycle. (Refer to "Interrupt Controller Operation" in the Program Control chapter of the *ADSP-2100 Family User's Manual* for further information on interrupt servicing.)
2. Edge-sensitive interrupts require pulse widths greater than 10ns; level-sensitive interrupts must be held low until serviced.
3. $\overline{IRQx}$ = $\overline{IRQ0}$, $\overline{IRQ1}$, $\overline{IRQ2}$, $\overline{IRQL0}$, $\overline{IRQL1}$, $\overline{IRQE}$.
4. PFx = PF0, PF1, PF2, PF3, PF4, PF5, PF6, PF7.
5. Flag Outputs = PFx, FL0, FL1, FL2, Flag_out.

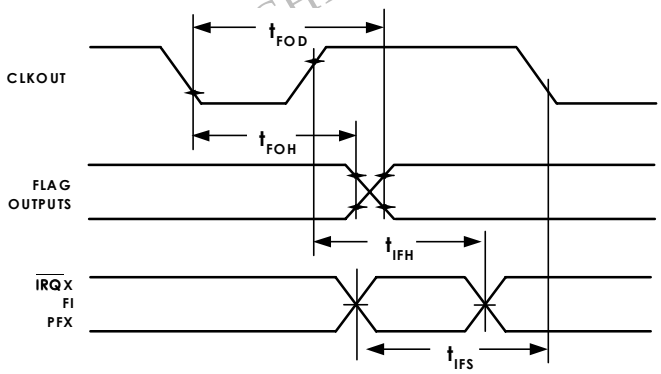


Figure 12 Interrupts and Flags

TIMING PARAMETERS ADSP-2141L

Bus Request/Bus Grant

Parameter		Min	Max	Unit
Timing Requirements:				
t_{BH}	$\overline{BR}$ Hold after CLKOUT High[1]	$0.25t_{CK} + 2$		ns
t_{BS}	$\overline{BR}$ Setup before CLKOUT Low[1]	$0.25t_{CK} + 17$		ns
Switching Characteristics:				
t_{SD}	CLKOUT High to $\overline{xMS}$, $\overline{RD}$, $\overline{WR}$ Disable		$0.25t_{CK} + 10$	ns
t_{SDB}	$\overline{xMS}$, $\overline{RD}$, $\overline{WR}$ Disable to BG Low	0		ns
t_{SE}	BG High to $\overline{xMS}$, $\overline{RD}$, $\overline{WR}$ Enable	0		ns
t_{SEC}	$\overline{xMS}$, $\overline{RD}$, $\overline{WR}$ Enable to CLKOUT High	$0.25t_{CK} - 4$		ns
t_{SDBH}	$\overline{xMS}$, $\overline{RD}$, $\overline{WR}$ Disable to BGH Low[2]	0		ns
t_{SEH}	$\overline{BGH}$ High to $\overline{xMS}$, $\overline{RD}$, $\overline{WR}$ Enable[2]	0		ns

NOTES

$\overline{xMS}$ = $\overline{PMS}$, $\overline{DMSL}$, $\overline{DMSH}$, $\overline{CMS}$, $\overline{IOMS}$, $\overline{BMS}$

1. $\overline{BR}$ is an asynchronous signal. If BR meets the setup/hold requirements, it will be recognized during the current clock cycle; otherwise the signal will be recognized on the following cycle. Refer to the *ADSP-2100 Family User's Manual* for $\overline{BR}$/$\overline{BG}$ cycle relationships.
2. $\overline{BGH}$ is asserted when the bus is granted and the processor requires control of the bus to continue.

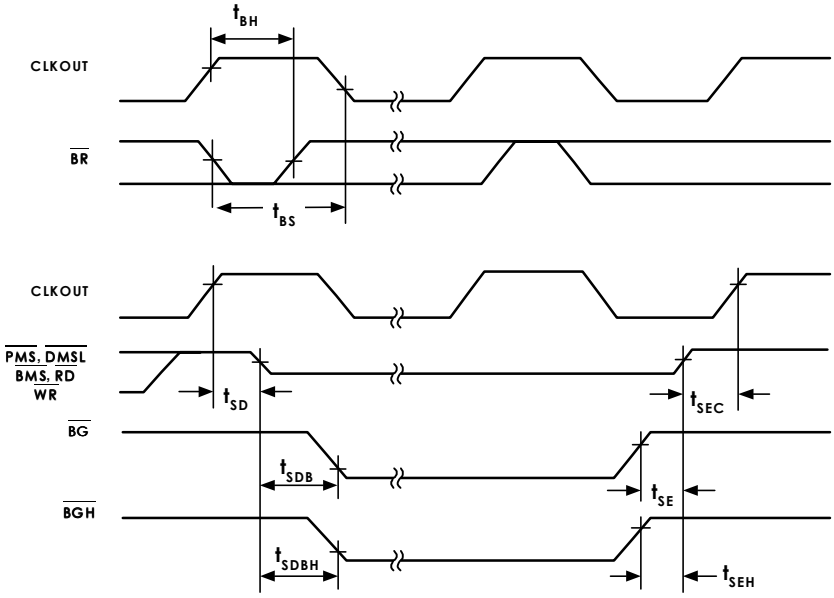


Figure 13 Bus Request/Bus Grant

TIMING PARAMETERS ADSP-2141L

External Memory Write: ADSP-2141L DMA Initiated

Parameter		Min	Max	Unit
Switching Characteristics:				
t_A	Clock to Address & DMSx	4	8	ns
t_{DW}	Data Setup before Write Deasserted	$0.5t_{CK}$ - 2 + w		ns
t_{DH}	Data Hold after Write Deasserted	$0.5t_{CK}$ - 7		ns
t_{WP}	Write Pulse Width	$0.5t_{CK}$ - 5 + w		ns
t_{WDE}	Write Low to Data Enabled	0		ns
t_{ASW}	Address, DMSx Setup before Write Low	1		ns
t_{DDR}	Data Disable before Write/Read Low	TBD		ns
t_{CWR}	Clock High to Write Low	6	12	ns
t_{AW}	Address, DMSx Setup Before Write High	$0.5t_{CK}$ - 2 + w		ns
t_{AH}	Address & DMSx Hold after Clock	3		ns
t_{WRA}	Address, DMSx Hold after Write High	$0.5t_{CK}$ - 7		ns
t_{WWR}	Write High to Read/Write Low	$0.5t_{CK}$ - 3		ns

1. If wait-state(s) added, then referenced to last wait-state clock interval
2. w = wait states x t_{CK}

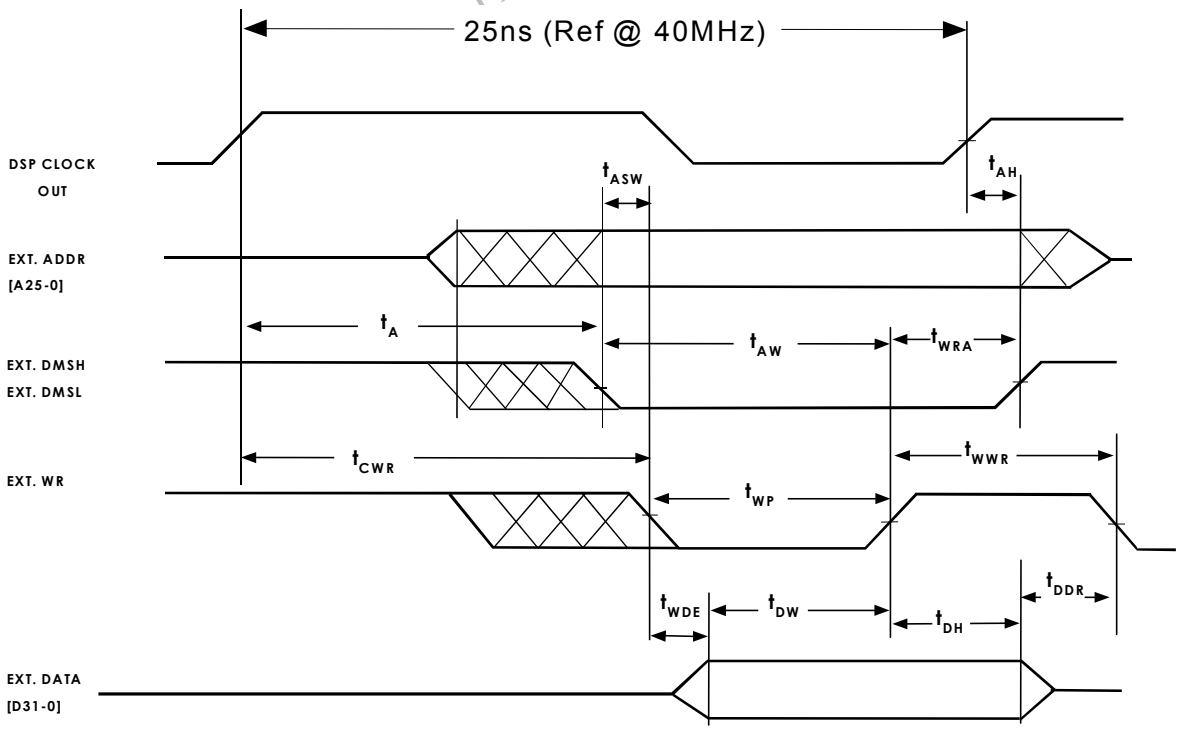


Figure 14 External Memory Write: ADSP-2141L DMA Initiated

TIMING PARAMETERS ADSP-2141L

External Memory Read – ADSP-2141L DMA Initiated

Parameter		Min	Max	Unit
Timing Requirements:				
t_{RDD}	Read Low to Data Valid		$0.5t_{CK}$ - 8 + w	ns
t_{AA}	Address, DMSx Valid to Data Valid		$0.5t_{CK}$ - 3 + w	ns
t_{SUR}	Data Valid before Read Deasserted	4		ns
t_{RDH}	Data Hold after Read Deasserted	0		ns
Switching Characteristics:				
t_A	Clock to Address & DMSx Active	4	8	ns
t_{ASR}	Address, DMSx Setup before Read Low	3		ns
t_{AH}	Address & DMSx Hold after Clock[1]	3		ns
t_{RDA}	Address, DMSx Hold after Read High	$0.5t_{CK}$ - 7		ns
t_{CRD}	Clock High to $\overline{RD}$ Low	8	14	ns
t_{RP}	Read Pulse Width	$0.5t_{CK}$ - 5 + w		ns
t_{RWR}	RD High to Read or Write Low	$0.5t_{CK}$ - 3		ns

1. If wait-state(s) added, then referenced to last wait-state clock interval
2. w = DMA wait state x t_{CK}

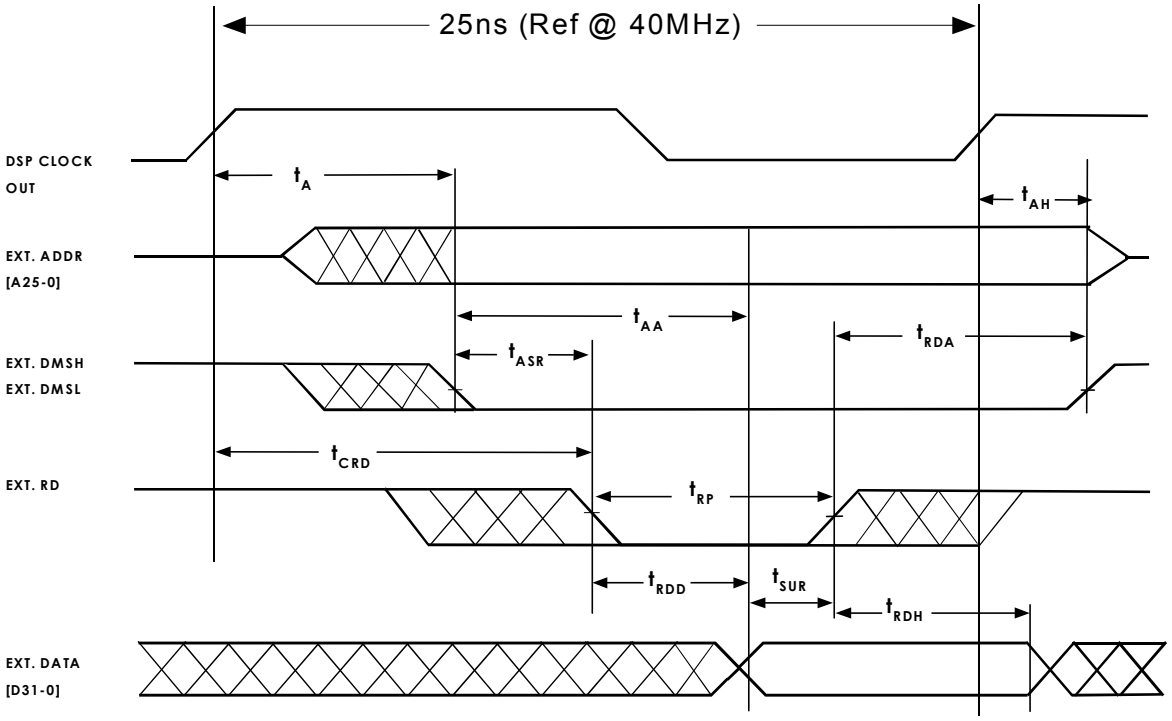


Figure 15 External Memory Read – ADSP-2141L DMA Initiated

TIMING PARAMETERS ADSP-2141L

External Memory Write: ADSP-2141L DSP Initiated

Parameter		Min	Max	Unit
Switching Characteristics:				
t_A	Clock to Address, $\overline{xMS}$	1	6	ns
t_{DW}	Data Setup before Write Deasserted	$0.5t_{CK}$ - 7 + w		ns
t_{DH}	Data Hold after Write Deasserted	$0.25t_{CK}$ - 2		ns
t_{WP}	Write Pulse Width	$0.5t_{CK}$ - 5 + w		ns
t_{WDE}	Write Low to Data Enabled	0		ns
t_{ASW}	Address, $\overline{xMS}$ Setup before Write Low	$0.25t_{CK}$ - 4		ns
t_{DDR}	Data Disable before Write/Read Low	$0.25t_{CK}$ - 4		ns
t_{CWR}	Clock High to Write Low	$0.25t_{CK}$	$0.5t_{CK}$ + 9	ns
t_{AW}	Address, $\overline{xMS}$ Setup Before Write High	$0.75t_{CK}$ - 6 + w		ns
t_{AH}	Address, $\overline{xMS}$ Hold after Clock	3		ns
t_{WRA}	Address, $\overline{xMS}$ Hold after Write High	$0.25t_{CK}$ - 4		ns
t_{WWR}	Write High to Read/Write Low	$0.5t_{CK}$ - 5		ns

1. If wait-state(s) added, then referenced to last wait-state clock interval
2. w = wait states x t_{CK}

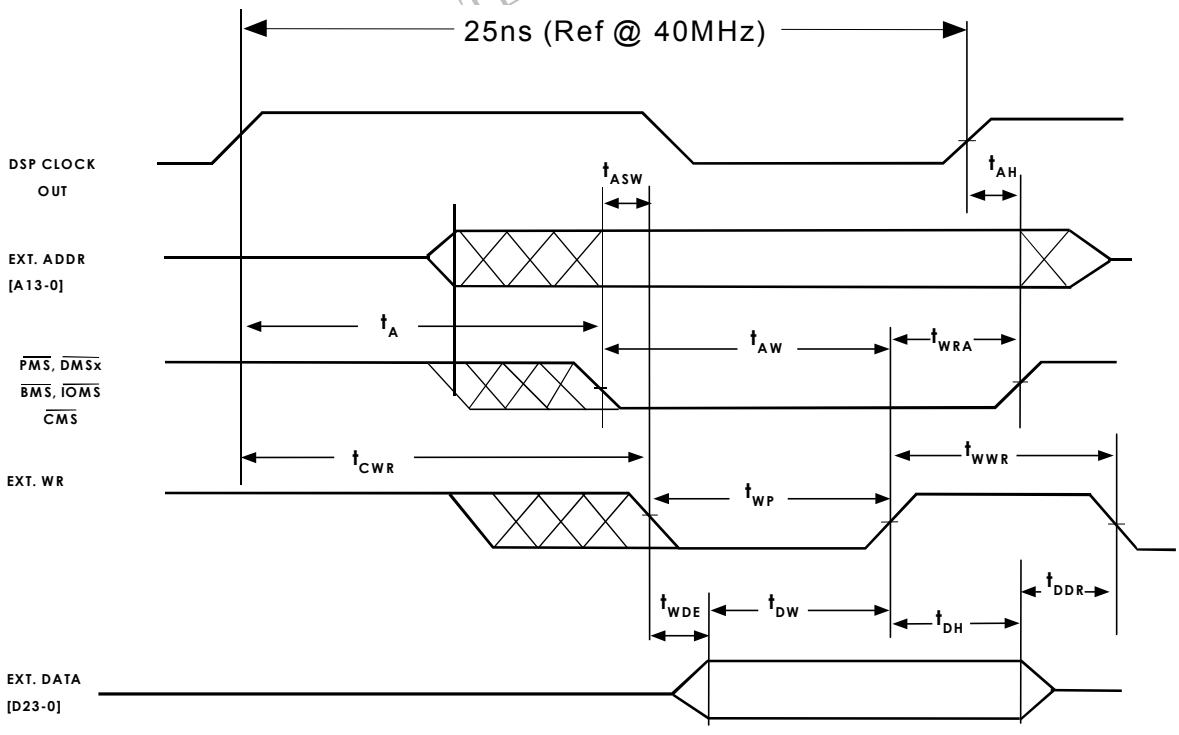


Figure 16 External Memory Write: ADSP-2141L DSP Initiated

TIMING PARAMETERS ADSP-2141L

External Memory Read – ADSP-2141L DSP Initiated

Parameter		Min	Max	Unit
Timing Requirements:				
t_{RDD}	Read Low to Data Valid		$0.5t_{CK}$ - 10 + w	ns
t_{AA}	Address, $\overline{xMS}$ Valid to Data Valid		$0.75t_{CK}$ - 10.5 + w	ns
t_{SUR}	Data Valid before Read Deasserted	8		ns
t_{RDH}	Data Hold after Read Deasserted	0		ns
Switching Characteristics:				
t_A	Clock to Address, $\overline{xMS}$ Active	1	6	ns
t_{ASR}	Address, $\overline{xMS}$ Setup before Read Low	$0.25t_{CK}$ - 4		ns
t_{AH}	Address, $\overline{xMS}$ Hold after Clock[1]	3		ns
t_{RDA}	Address, $\overline{xMS}$ Hold after Read High	$0.25t_{CK}$ - 3		ns
t_{CRD}	Clock High to $\overline{RD}$ Low	$0.25t_{CK}$ - 2	$0.25t_{CK}$ + 7	ns
t_{RP}	Read Pulse Width	$0.5t_{CK}$ - 5 + w		ns

1. If wait-state(s) added, then referenced to last wait-state clock interval
2. w = DMA wait state x t_{CK}

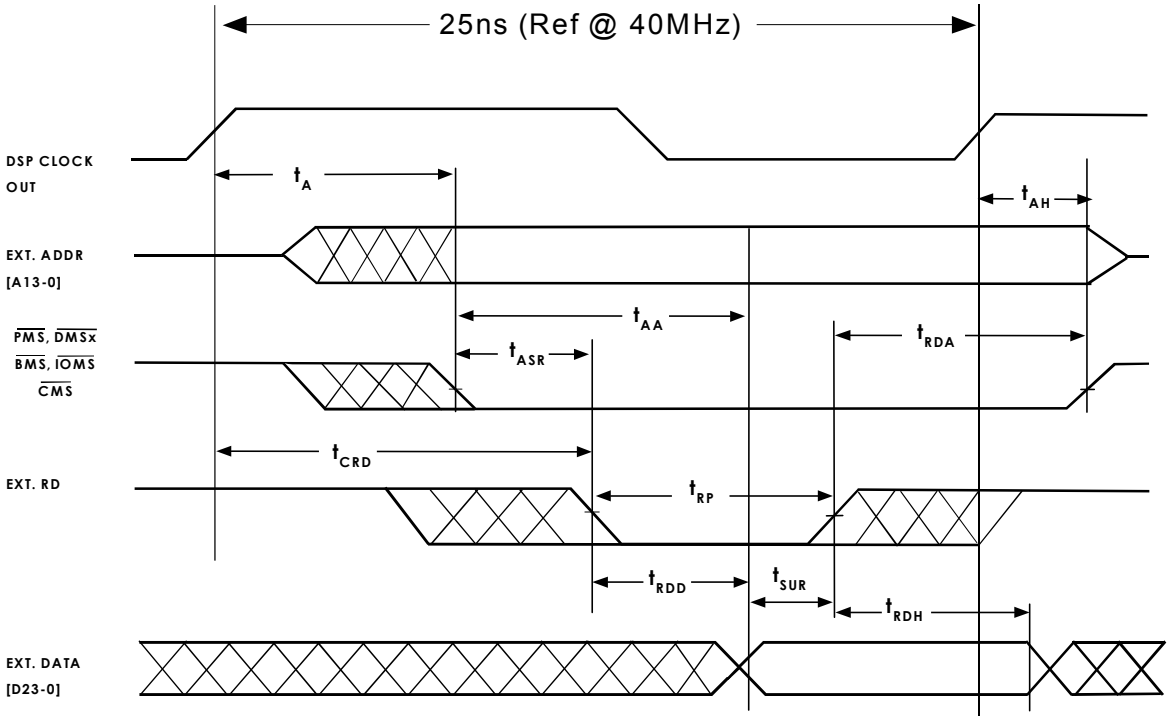


Figure 17 External Memory Read – ADSP-2141L DSP Initiated

TIMING PARAMETERS ADSP-2141L

Serial Ports

Parameter		Min	Max	Unit
Timing Requirements:				
t_{SCK}	SCLK Period	50		ns
t_{SCS}	DR/TFS/RFS Setup before SCLK Low	4		ns
t_{SCH}	DR/TFS/RFS Hold after SCLK Low	7		ns
t_{SCP}	$SCLK_{IN}$ Width	15		ns
Switching Characteristics:				
t_{CC}	CLKOUT High to $SCLK_{OUT}$	$0.25t_{CK}$	$0.25t_{CK} + 10$	ns
t_{SCDE}	SCLK High to DT Enable	0		ns
t_{SCDV}	SCLK High to DT Valid		15	ns
t_{RH}	TFS/RFS_{OUT} Hold after SCLK High	0		ns
t_{RD}	TFS/RFS_{OUT} Delay from SCLK High		15	ns
t_{SCDH}	DT Hold after SCLK High	0		ns
t_{TDE}	TFS (Alt) to DT Enable	0		ns
t_{TDV}	TFS (Alt) to DT Valid		14	ns
t_{SCDD}	SCLK High to DT Disable		15	ns
t_{RDV}	RFS (Multichannel, Frame Delay Zero) to DT Valid		15	ns

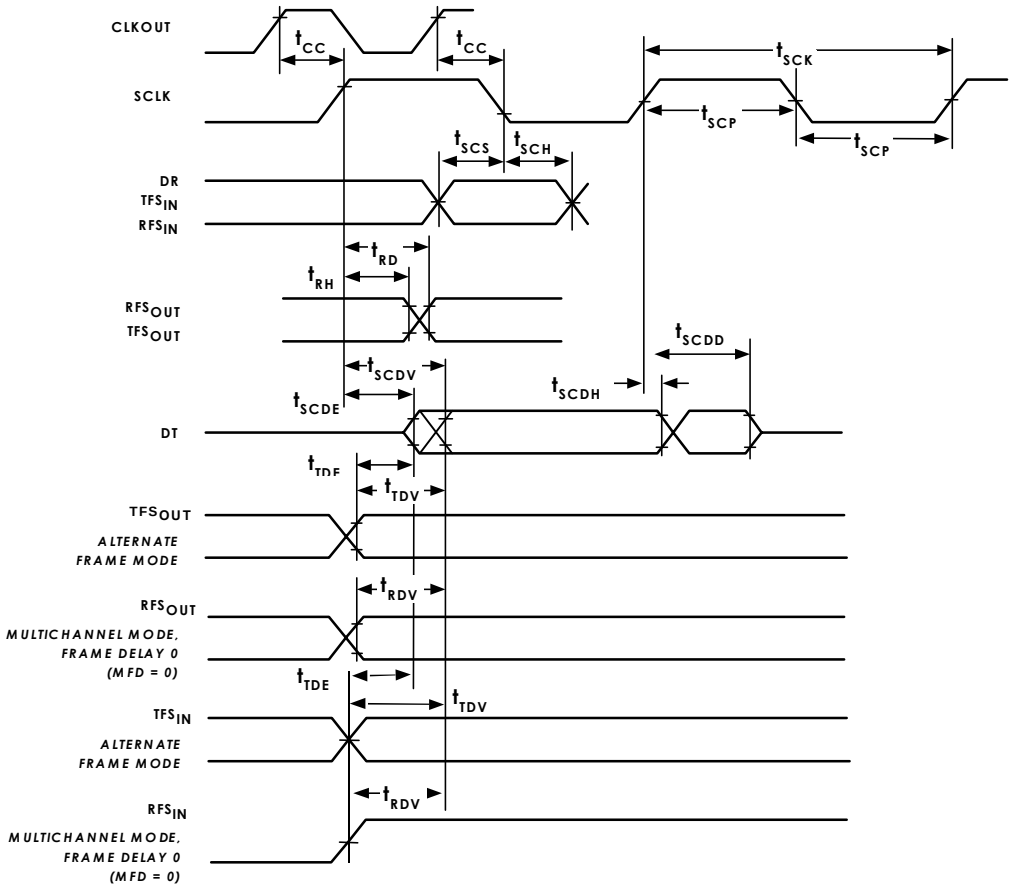


Figure 18 Serial Ports

TIMING PARAMETERS ADSP-2141L

IDMA Address Latch (IDMA Mode Multiplex Bus)

Parameter		Min	Max	Unit
Timing Requirements:				
t_{IALP}	Duration of Address Latch[1, 3]	10		ns
t_{IASU}	MPLX_BUS Address Setup before Address Latch End[3]	5		ns
t_{IAH}	MPLX_BUS Address Hold after Address Latch End[3]	2		ns
t_{IKA}	MPLX9 Low before Start of Address Latch[2, 3]	0		ns
t_{IALS}	Start of Write or Read after Address Latch End[2, 3]	3		ns

NOTES
1. Start of Address Latch = MPLX7 Low and MPLX8 High.
2. End of Address Latch = MPLX7 High or MPLX8 Low.
3. Start of Write or Read = MPLX7 Low and MPLX6 Low or MPLX5 Low.

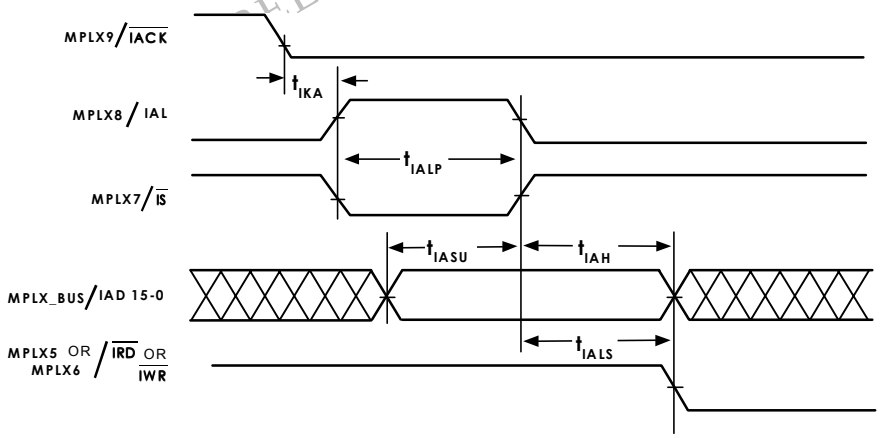


Figure 19 IDMA Address Latch (IDMA Mode Multiplex Bus)

TIMING PARAMETERS ADSP-2141L

IDMA Write, Short Write Cycle (IDMA Mode, Multiplex Bus)

Parameter		Min	Max	Unit
Timing Requirements:				
t_{IKW}	MPLX9 Low before Start of Write[1]	0		ns
t_{IWP}	Duration of Write[1, 2]	15		ns
t_{IDSU}	MPLX_BUS Data Setup before End of Write[2, 3, 4]	5		ns
t_{IDH}	MPLX_BUS Hold after End of Write[2, 3, 4]	2		ns
Switching Characteristics:				
t_{IKHW}	Start of Write to MPLX9 High		15	ns

NOTES
1. Start of Write = MPLX7 Low and MPLX6 Low.
2. End of Write = MPLX7 High or MPLX6 High.
3. If Write Pulse ends before MPLX9 Low, use specifications t_{IDSU}, t_{IDH}.
4. If Write Pulse ends after MPLX9 Low, use specifications t_{IKSU}, t_{IKH}.

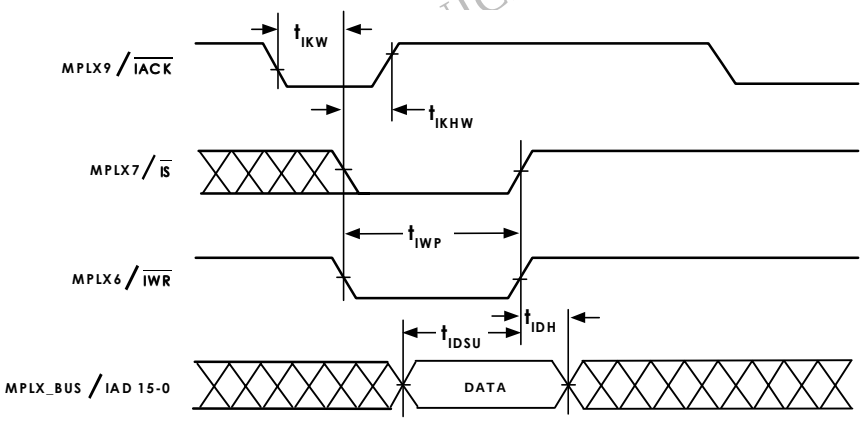


Figure 20 IDMA Write, Short Write Cycle (IDMA Mode, Multiplex Bus)

TIMING PARAMETERS ADSP-2141L

IDMA Write, Long Write Cycle (IDMA Mode, Multiplex Bus)

Parameter		Min	Max	Unit
Timing Requirements:				
t_{IKW}	MPLX9 Low before Start of Write[1]	0		ns
t_{IKSU}	MPLX_BUS Data Setup before MPLX9 Low[2, 3, 4]	$0.5t_{CK}$ + 10		ns
t_{IKH}	MPLX_BUS Data Hold after MPLX9 Low[2, 3, 4]	2		ns
Switching Characteristics:				
t_{IKLW}	Start of Write to MPLX9 Low[4]	$1.5t_{CK}$		ns
t_{IKHW}	Start of Write to MPLX9 High		15	ns

NOTES
1. Start of Write = MPLX7 Low and MPLX6 Low.
2. If Write Pulse ends before MPLX9 Low, use specifications t_{IDSU}, t_{IDH}.
3. If Write Pulse ends after MPLX9 Low, use specifications t_{IKSU}, t_{IKH}.
4. This is the earliest time for MPLX9 Low from Start of Write. For IDMA Write cycle relationships, please refer to the *ADSP-2100 Family User's Manual*.

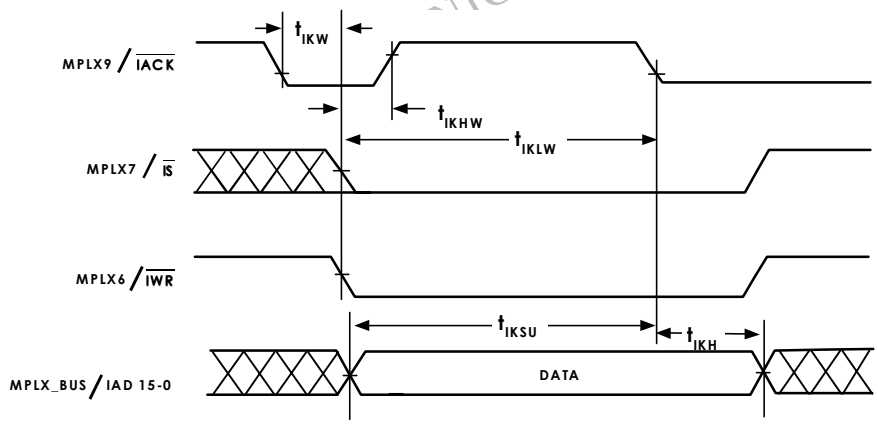


Figure 21 IDMA Write, Long Write Cycle (IDMA Mode, Multiplex Bus)

TIMING PARAMETERS ADSP-2141L

IDMA Read, Long Read Cycle (IDMA Mode, Multiplex Bus)

Parameter		Min	Max	Unit
Timing Requirements:				
t_{IKR}	MPLX9 Low before Start of Read[1]	0		ns
t_{IRP}	Duration of Read[1]	15		ns
Switching Characteristics:				
t_{IKHR}	MPLX9 High after Start of Read[1]		15	ns
t_{IKDS}	MPLX_BUS Data Setup before MPLX9 Low	$0.5t_{CK}$ - 7		ns
t_{IKDH}	MPLX_BUS Data Hold after End of Read[2]	0		ns
t_{IKDD}	MPLX_BUS Data Disabled after End of Read[2]		10	ns
t_{IRDE}	MPLX_BUS Previous Data Enabled after Start of Read	0		ns
t_{IRDV}	MPLX_BUS Previous Data Valid after Start of Read		15	ns
t_{IRDH1}	MPLX_BUS Previous Data Hold after Start of Read (DM/PM1)[3]	$2t_{CK}$ - 5		ns
t_{IRDH2}	MPLX_BUS Previous Data Hold after Start of Read (PM2)[4]	t_{CK} - 5		ns

NOTES
1. Start of Read = MPLX7 Low and MPLX5 Low.
2. End of Read = MPLX7 High or MPLX5 High.
3. DM read or first half of PM read.
4. Second half of PM read.

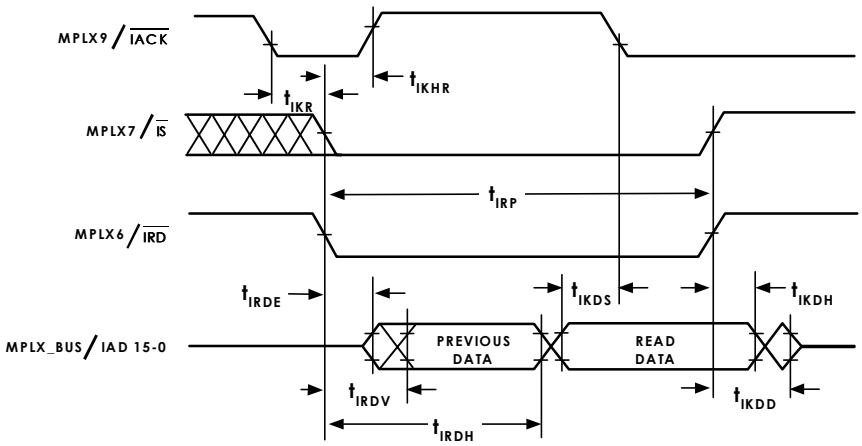


Figure 22 IDMA Read, Long Read Cycle (IDMA Mode, Multiplex Bus)

TIMING PARAMETERS ADSP-2141L

IDMA Read, Short Read Cycle (IDMA Mode, Multiplex Bus)

Parameter		Min	Max	Unit
Timing Requirements:				
t_{IKR}	MPLX9 Low before Start of Read[1]	0		ns
t_{IRP}	Duration of Read	15		ns
Switching Characteristics:				
t_{IKHR}	MPLX9 High after Start of Read[1]		15	ns
t_{IKDH}	MPLX_BUS Data Hold after End of Read[2]	0		ns
t_{IKDD}	MPLX_BUS Data Disabled after End of Read[2]		10	ns
t_{IRDE}	MPLX_BUS Previous Data Enabled after Start of Read	0		ns
t_{IRDV}	MPLX_BUS Previous Data Valid after Start of Read	15		ns

NOTES
[1]Start of Read = MPLX7 Low and MPLX5 Low.
[2]End of Read = MPLX7 High or MPLX5 High.

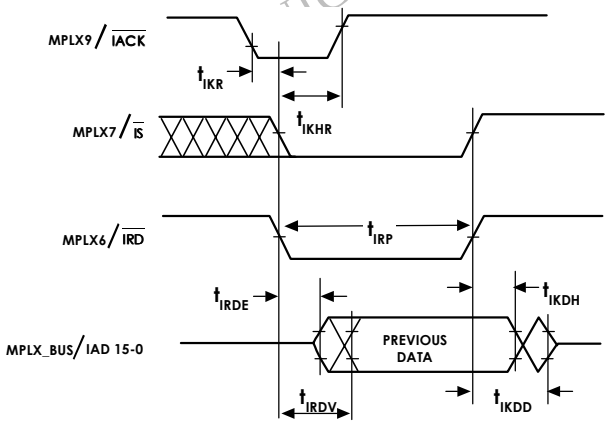
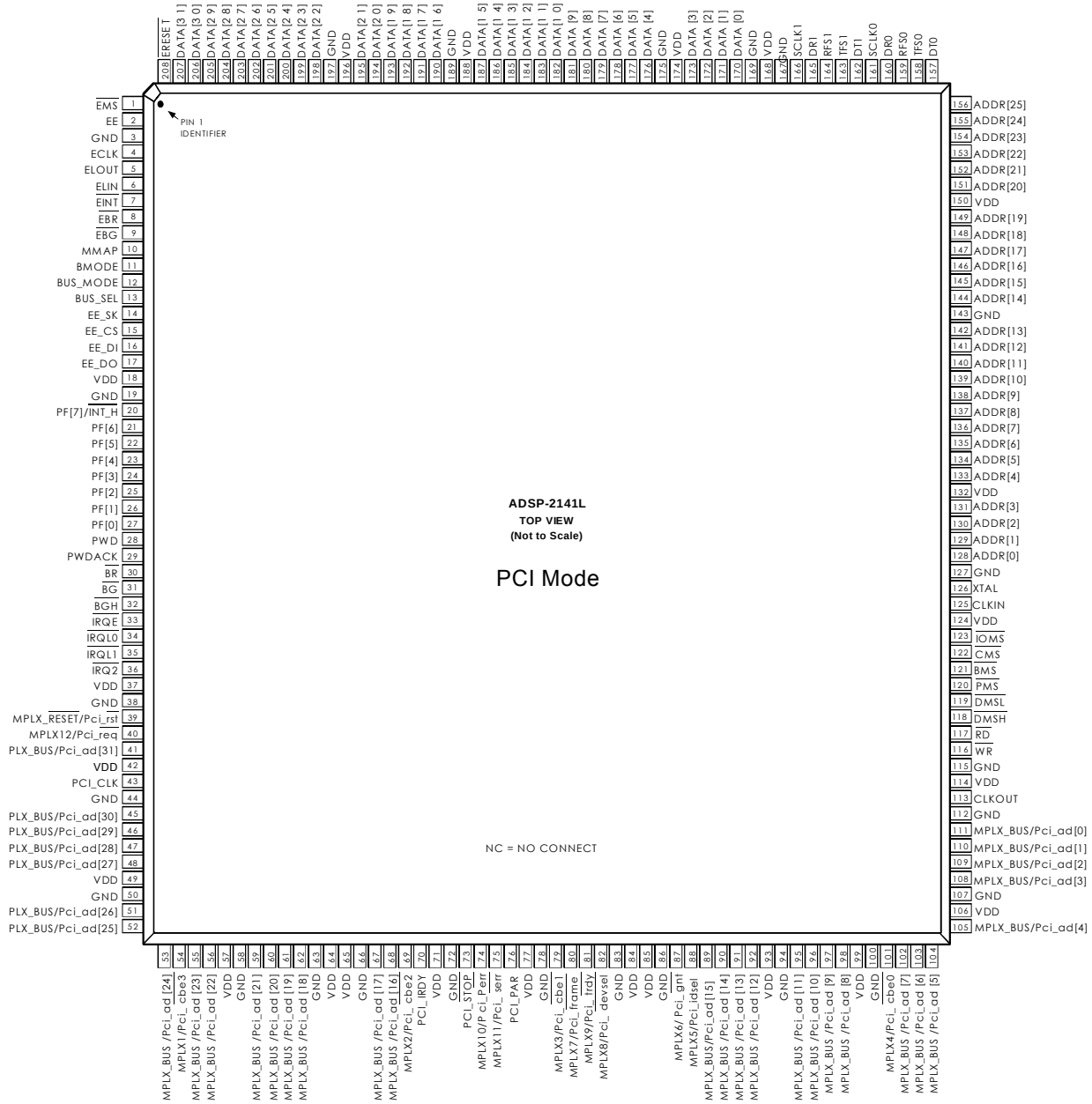


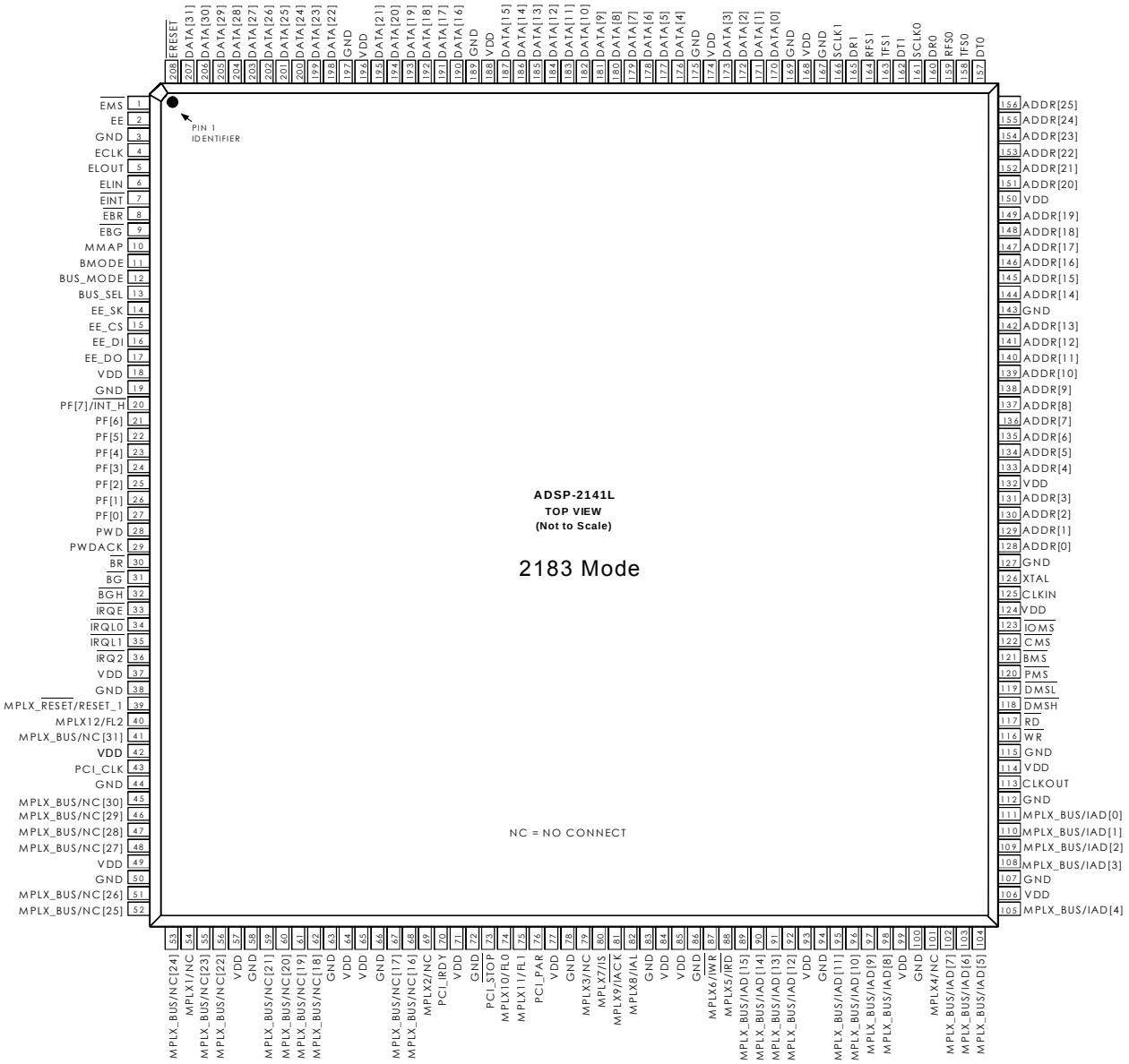
Figure 23 IDMA Read, Short Read Cycle (IDMA Mode, Multiplex Bus)

PACKAGE PINOUT

For all multiplexed pins the active sense is determined by the mode selected. See Tables 3 and 4.

Pin #	Pin Name	Pin #	Pin Name	Pin #	Pin Name	Pin #	Pin Name	Pin #	Pin Name
1	$\overline{\text{EMS}}$	43	PCI_CLK	85	VDD	127	GND	169	GND
2	EE	44	GND	86	GND	128	ADDR[0]	170	DATA[0]
3	GND	45	MPLX_BUS[30]	87	MPLX6	129	ADDR[1]	171	DATA[1]
4	ECLK	46	MPLX_BUS[29]	88	MPLX5	130	ADDR[2]	172	DATA[2]
5	ELOUT	47	MPLX_BUS[28]	89	MPLX_BUS[15]	131	ADDR[3]	173	DATA[3]
6	ELIN	48	MPLX_BUS[27]	90	MPLX_BUS[14]	132	VDD	174	VDD
7	$\overline{\text{EINT}}$	49	VDD	91	MPLX_BUS[13]	133	ADDR[4]	175	GND
8	$\overline{\text{EBR}}$	50	GND	92	MPLX_BUS[12]	134	ADDR[5]	176	DATA[4]
9	$\overline{\text{EBG}}$	51	MPLX_BUS[26]	93	VDD	135	ADDR[6]	177	DATA[5]
10	MMAP	52	MPLX_BUS[25]	94	GND	136	ADDR[7]	178	DATA[6]
11	BMODE	53	MPLX_BUS[24]	95	MPLX_BUS[11]	137	ADDR[8]	179	DATA[7]
12	BUS_MODE	54	MPLX1	96	MPLX_BUS[10]	138	ADDR[9]	180	DATA[8]
13	BUS_SEL	55	MPLX_BUS[23]	97	MPLX_BUS[9]	139	ADDR[10]	181	DATA[9]
14	EE_SK	56	MPLX_BUS[22]	98	MPLX_BUS[8]	140	ADDR[11]	182	DATA[10]
15	EE_CS	57	VDD	99	VDD	141	ADDR[12]	183	DATA[11]
16	EE_DI	58	GND	100	GND	142	ADDR[13]	184	DATA[12]
17	EE_DO	59	MPLX_BUS[21]	101	MPLX4	143	GND	185	DATA[13]
18	VDD	60	MPLX_BUS[20]	102	MPLX_BUS[7]	144	ADDR[14]	186	DATA[14]
19	GND	61	MPLX_BUS[19]	103	MPLX_BUS[6]	145	ADDR[15]	187	DATA[15]
20	PF[7]/$\overline{\text{INT\_H}}$	62	MPLX_BUS[18]	104	MPLX_BUS[5]	146	ADDR[16]	188	VDD
21	PF[6]	63	GND	105	MPLX_BUS[4]	147	ADDR[17]	189	GND
22	PF[5]	64	VDD	106	VDD	148	ADDR[18]	190	DATA[16]
23	PF[4]	65	VDD	107	GND	149	ADDR[19]	191	DATA[17]
24	PF[3]	66	GND	108	MPLX_BUS[3]	150	VDD	192	DATA[18]
25	PF[2]	67	MPLX_BUS[17]	109	MPLX_BUS[2]	151	ADDR[20]	193	DATA[19]
26	PF[1]	68	MPLX_BUS[16]	110	MPLX_BUS[1]	152	ADDR[21]	194	DATA[20]
27	PF[0]	69	MPLX2	111	MPLX_BUS[0]	153	ADDR[22]	195	DATA[21]
28	$\overline{\text{PWD}}$	70	PCI_$\overline{\text{IRDY}}$	112	GND	154	ADDR[23]	196	VDD
29	PWDACK	71	VDD	113	CLKOUT	155	ADDR[24]	197	GND
30	$\overline{\text{BR}}$	72	GND	114	VDD	156	ADDR[25]	198	DATA[22]
31	$\overline{\text{BG}}$	73	PCI_$\overline{\text{STOP}}$	115	GND	157	DT0	199	DATA[23]
32	$\overline{\text{BGH}}$	74	MPLX10	116	$\overline{\text{WR}}$	158	TFS0	200	DATA[24]
33	$\overline{\text{IRQE}}$	75	MPLX11	117	$\overline{\text{RD}}$	159	RFS0	201	DATA[25]
34	$\overline{\text{IRQL0}}$	76	PCI_PAR	118	$\overline{\text{DMSH}}$	160	DR0	202	DATA[26]
35	$\overline{\text{IRQL1}}$	77	VDD	119	$\overline{\text{DMSL}}$	161	SCLK0	203	DATA[27]
36	$\overline{\text{IRQ2}}$	78	GND	120	$\overline{\text{PMS}}$	162	DT1	204	DATA[28]
37	VDD	79	MPLX3	121	$\overline{\text{BMS}}$	163	TFS1	205	DATA[29]
38	GND	80	MPLX7	122	$\overline{\text{CMS}}$	164	RFS1	206	DATA[30]
39	MPLX_$\overline{\text{RESET}}$	81	MPLX9	123	$\overline{\text{IOMS}}$	164	DR1	207	DATA[31]
40	MPLX12	82	MPLX8	124	VDD	166	SCLK1	208	$\overline{\text{ERESET}}$
41	MPLX_BUS[31]	83	GND	125	CLKIN	167	GND		
42	VDD	84	VDD	126	XTAL	168	VDD		

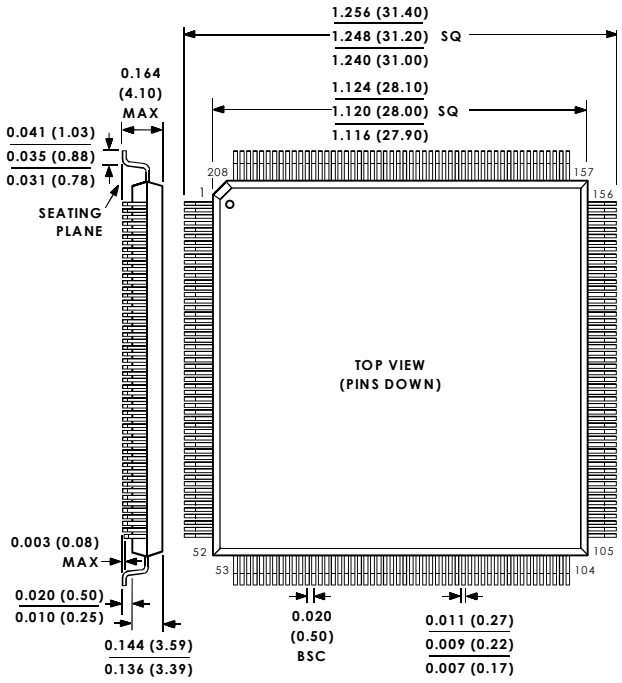




PACKAGE DESCRIPTION

Package Details

The package shown below is a 208 lead Metric Quad Flatpack. Measurements are listed in English and (metric). Because this package is designed as a metric package Analog Devices recommends that you use these measurements for any PCB layout.



208-Lead Metric Plastic Quad Flatpack (MQFP)
(non-hermetic)

ORDERING GUIDE

Part Number	Ambient Temperature Range	Instruction Rate	Package Description	Package Option
ADSP-2141LKS-160x	0°C to +70°C	40 MHz	208-Lead MQFP	S-208