

# CS5310/11/12

Standard Hash Algorithm (SHA-1 & SHA-2)  
Cores



The CS5310/11/12 Hashing Cores are designed to achieve data authentication in digital broadband, wireless, and multimedia systems. These high performance application specific silicon cores support the Secure Hash Algorithm as described in the NIST Draft Federal Information Processing Standard 180-2 (DFIPS 180-2 "Secure Hash Standard"). The CS5310 core offers SHA-1 algorithm that is required for use with the Digital Signature Algorithm (DSA), as specified in the Digital Signature Standard (DSS) and provides authentication between users during data transmission. The CS5311 core provides SHA-256 algorithm and offers a security equivalent to 128-bit AES. The CS5312 offers the entire SHA-2 algorithms including SHA-256, SHA-384, and SHA-512. These cores are available for both ASIC and programmable logic versions that have been hand crafted by Amphion to deliver high performance while minimizing power consumption and silicon area.

## CORE FEATURES

**Table 1: CS5210/11/12Secure Hash Algorithm Cores at a Glance**

FEATURES	SHA-1	SHA-2	
	CS5310	CS5311	CS5312
Fully implements <b>SHA-1</b> secure hash algorithms to NIST FIPS 180-2 specifications	•		
Fully implements <b>SHA-256</b> secure hash algorithms to NIST FIPS 180-2 specifications		•	
Fully implements <b>SHA-256, SHA-384, SHA-512</b> secure hash algorithms to NIST FIPS 180-2 specifications			•
High Speed operation	•	•	•
Each 512-bit block requires 81 master clock cycles (1 clock per algorithm step + 1 clock load)	•		
Each 512-bit block for SHA-256 requires 65 master clock cycles (1 clock per algorithm step + 1 clock load)		•	•
Each 1024-bit block for SHA-384 and SHA-512 requires 81 master clock cycles (1 clock per algorithm step + 1 clock load)			•
32-bit I/O interface	•	•	
64-bit I/O interface			•
Supports user input initialization vectors	•	•	•
Supports message padding	•	•	•
HMACs (Hashing Message Authentication Codes) efficiently supported	•	•	•
Simple external interface	•	•	•

## APPLICATIONS

### ◆ Electronic financial transactions

- E-Commerce
- Banking
- Securities exchange
- Point-of-Sale

### ◆ Secure corporate communications

- Storage Area Networks (SAN)
- Virtual Private Networks (VPN)
- Video conferencing
- Voice services

### ◆ Personal mobile communications

- Video phones
- PDA
- Point-to-Point Wireless
- Wearable computers

### ◆ Secure environments

- Satellite communications
- Surveillance systems
- Network appliances

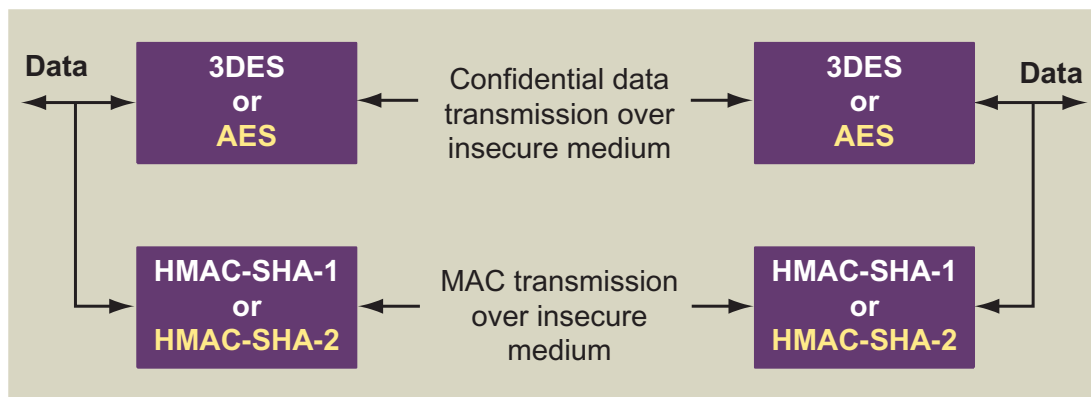


Figure 1: Example of an Authenticated Encryption System Using 3DES or AES with Matching SHA Algorithm

## CS5310 SHA-1 CORE

### SYMBOL AND PIN DESCRIPTION

Table 2 describes the input and output ports (shown graphically in Figure 2) of the SHA-1 core. Unless otherwise stated, all signals are active high and bit (0) is the least significant bit.

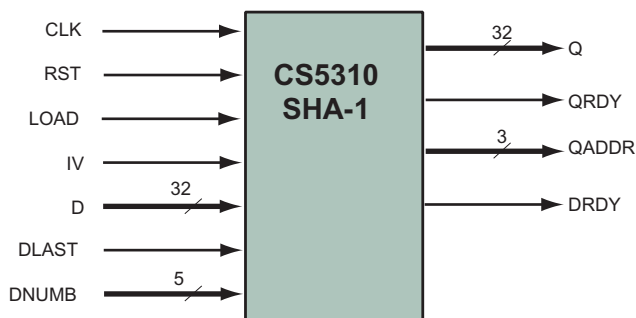


Figure 2: CS5310 Symbol

Table 2: CS5310 Signal Interface Signal Definitions

Signal	I/O	Width (Bits)	Description
CLK	Input	1	System clock signal, all flip-flops within the core are triggered on the rising edge
RST	Input	1	Asynchronous global reset signal, active HIGH.
LOAD	Input	1	Input data port D is sampled on the rising edge of CLK when LOAD is asserted. Otherwise the port is ignored
IV	Input	1	Initialization vector flag. Asserting this flag denotes that the data presently sampled is the core initialization vector, otherwise the sample is considered as message data. This port is ignored when Load is deasserted.
D	Input	32	32-bit data input port sampled on the rising edge of CLK when Load is asserted. When IV is deasserted this is processed as message data beginning with the most significant word of a 512 bit block, when IV is asserted the data is processed as an initialization vector
DLAST	Input	1	When asserted, the data present at port D, sampled at the rising edge of CLK is flagged as being the last in the current input block.
DNUMB	Input	5	The value present at DNUMB denotes how many bits of the data at D are to be sampled as message data when DLAST is simultaneously asserted to denote the last word in a block. Ignored when DLAST is deasserted.
Q	Output	32	Message digest output port driven on the rising edge of signal CLK, most significant 32 bits of 512 bit block presented first
QRDY	Output	1	Message digest ready signal, driven on the rising edge of CLK, when asserted signifies the message digest for the current block is present at output port Q
QADDR	Output	3	Denotes the significance or address of the 32 bits of the message digest present simultaneously a output port Q
DRDY	Output	1	Data input ready signal, when asserted denotes that the core is ready to accept data (or initialization vectors) placed on port D, when deasserted denotes the core is busy and the input data stream must be stalled.

## FUNCTIONAL DESCRIPTION

SHA-1 algorithm is used by both the transmitter and the intended receiver of a message in computing and verifying a digital signature. SHA-1 produces a 160-bit condensed representation of the message called a message digest. The message digest is used to generate a signature for the message. SHA-1 is also used to verify any received signature. Any change to the message in transit will result in a different message digest, and the signature will fail to verify. Figure 3 represents the functional block diagram of CS5310 core.

The SHA-1 algorithm processes an input message, of length  $n \times 512$  bits, in successive 512-bit blocks to produce a 160-bit message digest. The message digest is transmitted to the receiver along with the message and verified, thus providing authentication and ensuring the message has not been altered or interfered with. It consists of four rounds of processing

each of 20 steps. Once all 80 processing steps are complete, five 32-bit intermediate variables are updated and the next message block is processed. Once processing of the last message block is complete the final variable values represent the 160-bit message digest.

Optionally, prior to loading the first message word the external logic may load customized initial values into the core. This allows pre-computed initial values to be used for efficient implementation of a Hash-based Message Authentication Code (HMAC).

The Amphion CS5310 core is an excellent complement to the Amphion CS5210-40 suite of DES/Triple DES cores.

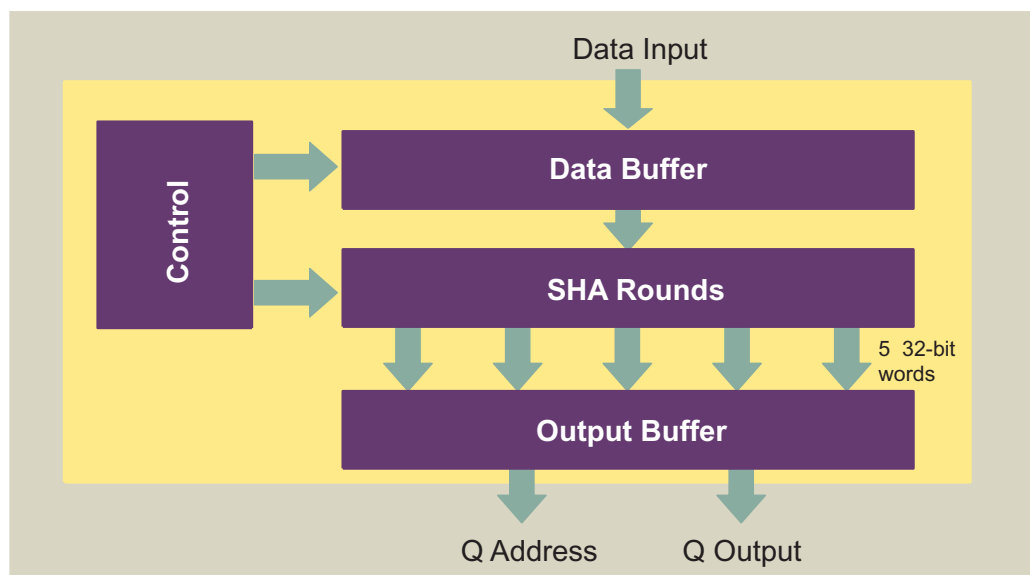


Figure 3: Block Diagram of the CS5310 SHA-1 Core

## CS5311 SHA-256 CORE

### SYMBOL AND PIN DESCRIPTION

Table 3 describes the input and output ports (shown graphically in Figure 4) of the SHA-256 core. Unless otherwise stated, all signals are active high and bit (0) is the least significant bit.

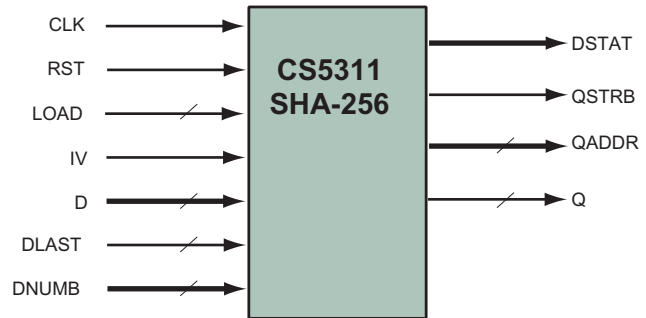


Figure 4: CS5311 Symbol

Table 3: CS5311 SHA-256 Core Interface Signal Definitions

Signal	I/O	Width (Bits)	Description
CLK	Input	2	System clock, rising edge active
RST	Input	1	Asynchronous reset
LOAD	Input	1	Load input message data
IV	Input	1	Load input initialization vector.  IV should be asserted with LOAD when an initialization vector is to be loaded prior to hashing a message.
D	Input	32	Input message vector
DLAST	Input	1	Input last message data word  Should be asserted when loading last word of message to enable SHA padding operations
DNUMB	Input	5	Input data word validity  This signal is ignored unless DLAST is asserted. DNUMB indicates the number of valid bits contained in the last message word.
Q	Output	32	Output data port
DSTAT	Output	1	Input port status  Indicates the readiness of the input interface to accept new message data. When asserted, initialization vectors and data words may be loaded.
QSTRB	Output	1	Output data strobe. Asserted to indicate valid data on the output data port.
QADDR	Output	3	Output data address. Indicates the relative address of the output data words, 0: most significant word of hash data.

## FUNCTIONAL DESCRIPTION

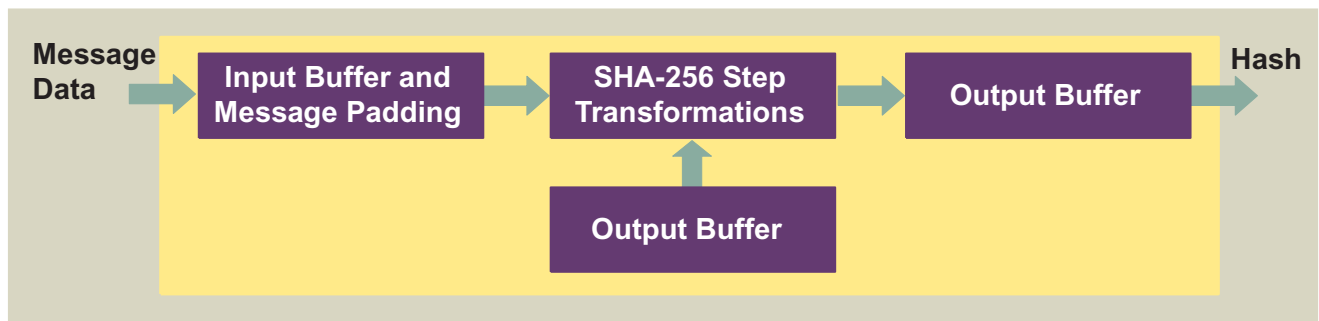
Since the 128 bit and 160 bit hash lengths of MD5 and SHA-1 respectively do not offer security equivalent to AES, the NIST has announced SHA-256 hash to provide a similar level of security in an authentication scheme employed alongside an encryption scheme utilizing a 128-bit AES. The increased hash length of the SHA-256 offers increased levels of security in authentication and data integrity, and should be used in applications utilizing encryption with key length 128-bit.

This algorithm can be implemented in IPSec, SSL/TLS etc. as an accompanying HMAC offering authentication services alongside encryption, in particular AES. Figure 5, represents the block diagram of CS5311 SHA-256 core.

The SHA-256 algorithm consists of 64 processing steps. Once all 64 processing steps are complete, eight 32-bit intermediate variables are updated and the next message block is processed. The final variable values represent the 256-bit message digest when the processing of the last message block

is complete. This algorithm processes an input message, of length  $n * 512$  bits in successive 512-bit blocks to produce a message digest. The message digest is transmitted to the receiver along with the message and verified, thus providing authentication and ensuring the message has not been altered or interfered with. The CS5311 SHA-256 core performs padding operations on incomplete data blocks as required and supports a maximum message length of 237 bits.

The Amphion CS5311 core is an excellent complement to the Amphion CS5200 suite of AES cores. For instance it can be combined with the CS5265 Compact AES Encryption/Decryption core to rapidly construct an IPSec hardware accelerator which will support the highest levels of security available today, and will offload the computationally intensive cryptographic processing required for security over the internet and VPNs while maintaining high data throughput rates.



**Figure 5: Block Diagram of the CS5311 SHA-256 Core**

## CS5312 SHA-256/384/512 CORE

### SYMBOL AND PIN DESCRIPTION

Table 4 describes the input and output ports (shown graphically in Figure 6) of the SHA-256 core. Unless otherwise stated, all signals are active high and bit (0) is the least significant bit.

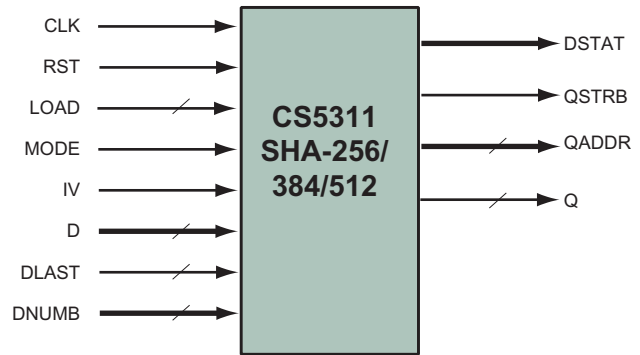


Figure 6: CS5312 Symbol

Table 4: CS5312 SHA-256/384/512 Core Interface Signal Definitions

Signal	I/O	Width (Bits)	Description
CLK	Input	2	System clock, rising edge active
RST	Input	1	Asynchronous reset
LOAD	Input	1	Load input message data
IV	Input	1	Load input initialization vector.  IV should be asserted with LOAD when an initialization vector is to be loaded prior to hashing a message.
D	Input	32	Input message vector
DLAST	Input	1	Input last message data word  Should be asserted when loading last word of message to enable SHA padding operations
DNUMB	Input	6	Input data word validity  This signal is ignored unless DLAST is asserted. DNUMB indicates the number of valid bits contained in the last message word.
MODE	Input	1	SHA-2 processing mode.  0: SHA-256; 1: SHA-384 and SHA-512
Q	Output	64	Output data port
DSTAT	Output	1	Input port status  Indicates the readiness of the input interface to accept new message data. When asserted, initialization vectors and data words may be loaded.
QSTRB	Output	3	Output data strobe. Asserted to indicate valid data on the output data port.
QADDR	Output	3	Output data address. Indicates the relative address of the output data words, 0: most significant word of hash data.

## FUNCTIONAL DESCRIPTION

The CS5312 core implements the SHA-256, SHA-384 and SHA-512 algorithms. This core offers the ability to change hashing algorithm on-line, and offers a scalable level of security to accompany all variable key sizes of AES.

The SHA-256/384/512 algorithms (commonly known as SHA-2) process an input message, of length  $n \cdot B$ -bits ( $B$  is the block size, 512 or 1024 bits respectively for SHA-256 and SHA-384/512), in successive  $B$ -bit blocks to produce a message digest. The message digest is transmitted to the receiver along with the message and verified, thus providing authentication and ensuring the message has not been altered or interfered with. Figure 7 represents the block diagram of CS5312 SHA-2 core.

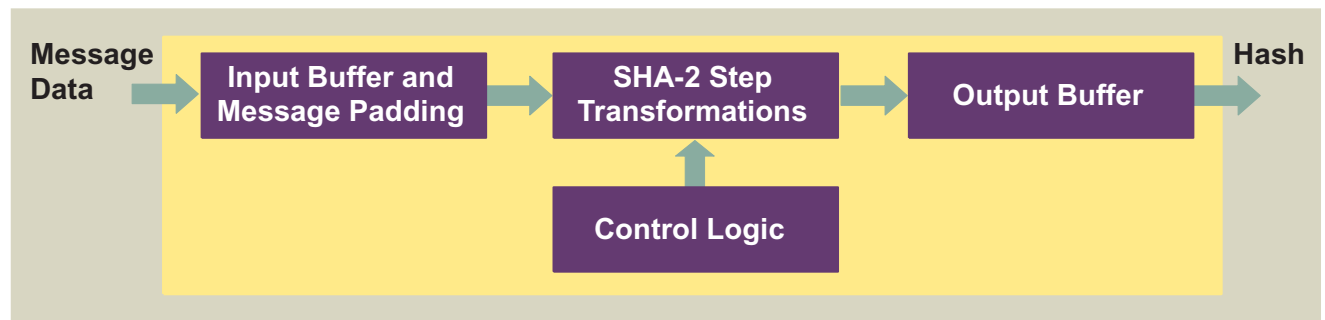
The SHA-256 algorithm consists of 64 processing steps. Once all 64 processing steps are complete, eight 32-bit intermediate variables are updated and the next message block is processed. Once processing of the last message block is

complete the final variable values represent the 256-bit message digest.

The SHA-512 and SHA-384 algorithms consist of 80 processing steps. Once all 80 processing steps are complete, eight 64-bit intermediate variables are updated and the next message block is processed. Once processing of the last message block is complete the final variable values represent the 512-bit SHA-512 hash. To obtain the 384-bit SHA-384 hash the output data should simply be truncated.

CS5312 cores perform padding operations on incomplete data blocks as required. The CS5312 core supports a maximum message length of 238 bits.

The Amphion CS5312 SHA-2 core is an excellent choice for security ICs incorporated into broadband switches, routers, firewalls and remote access concentrators.



**Figure 7: Block Diagram of the CS5312 SHA-256/384/512 Core**



## AVAILABILITY AND IMPLEMENTATION INFORMATION

### ASIC CORES

For applications that require the high performance, low cost and high integration of an ASIC, Amphion delivers application specific silicon cores that are pre-optimized to a targeted ASIC technology by Amphion experts.

Consult your local Amphion representative for product specific performance information, current availability of individual products, and lead times on ASIC core porting.

**Table 5: CS5310/11/12 ASIC Implementation using TSMC 130 nm Standard Cell Libraries**

PRODUCT ID	LOGIC GATES	CYCLES PER OPERATION	TIMING CONSTRAINT (MHz)	SUSTAINED DATA THROUGHPUT (Gbps)
CS5310TK	17K	81	300	1.896
CS5311	24K	65	250	1.069
CS5312	49K	81 (SHA-384/512)	200	2.528
		65 (SHA-256)	200	1.575

**Table 6: CS5310/11/12 ASIC Implementation using TSMC 180 nm Standard Cell Libraries**

PRODUCT ID	LOGIC GATES	CYCLES PER OPERATION	TIMING CONSTRAINT (MHz)	SUSTAINED DATA THROUGHPUT (Gbps)
CS5310TK	17K	81	300	1.264
CS5311	26K	65	250	1.575
CS5312	52K	81 (SHA-384/512)	166	2.098
		65 (SHA-256)	166	1.307

## PROGRAMMABLE LOGIC CORES

For ASIC prototyping or for projects requiring fast time-to-market of a programmable logic solution, Amphion programmable logic cores offer the silicon-aware performance tuning found in all Amphion products, combined with the rapid design times offered by today's leading programmable logic solutions.

**Table 7: CS5311 Programmable Logic Core Using Altera APEX20KE-1**

PRODUCT ID	LOGIC USED (LEs)	MEMORY USED (ESB)	CYCLES PER OPERATION	TIMING CONSTRAINT (MHz)	SUSTAINED DATA THROUGHPUT (Gbps)
CS5310AA	1878	0	81	60.81	380
CS5311AA	2749	0	65	49.34	388
CS5312AA	5201	4	81 (SHA-384/512)	32.62	412
			65 (SHA-256)	32.62	256

**Table 8: CS5311 Programmable Logic Core Using Xilinx VirtexII-5**

PRODUCT ID	LOGIC USED (Slices)	MEMORY USED (BRAM)	CYCLES PER OPERATION	TIMING CONSTRAINT (MHz)	SUSTAINED DATA THROUGHPUT (Gbps)
CS5310X2	854	0	81	99	626
CS5311X2	1122	1	62	53.370	420
CS5312X2	2403	1	81(SHA-384/512)	49.556	626
			65 (SHA-256)	49.556	390

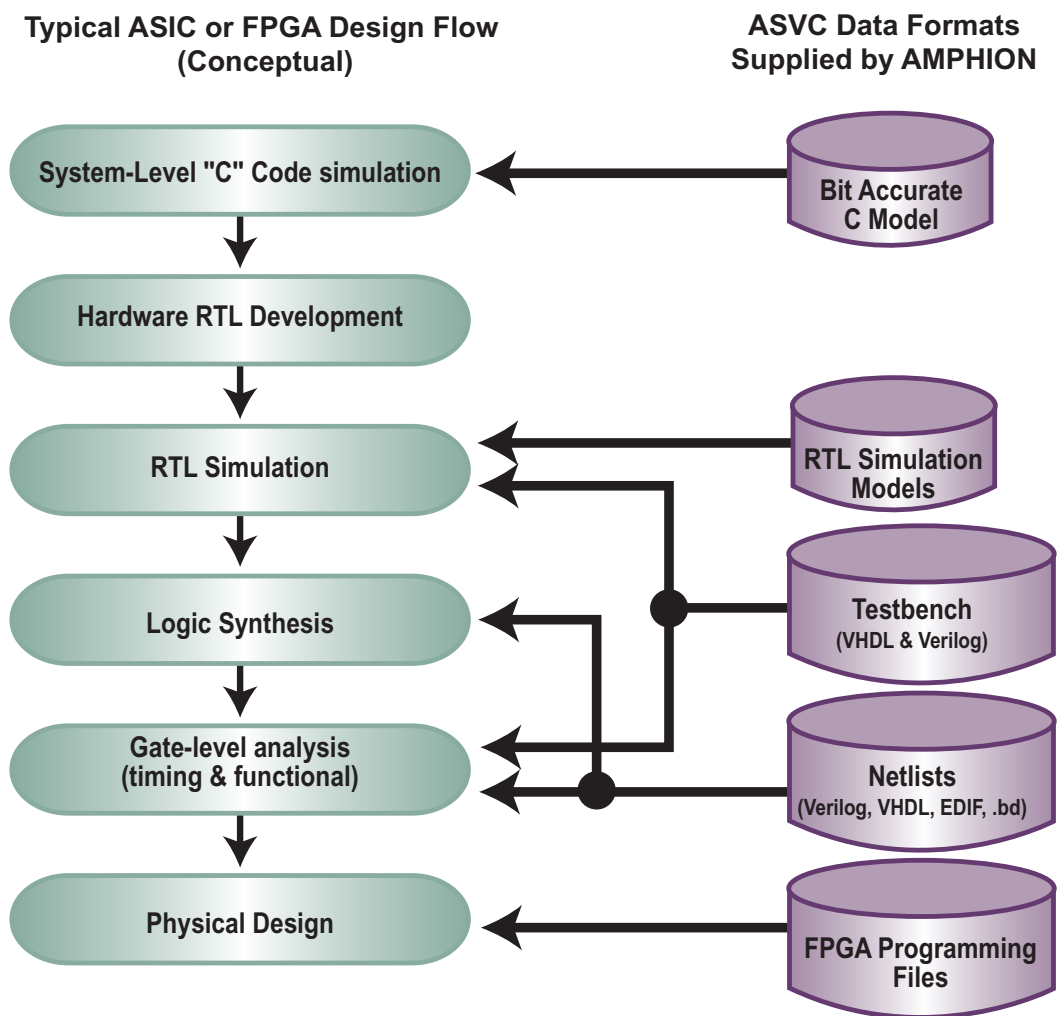


Figure 8: Design Data Formats Supplied by Amphion

## ABOUT AMPHION

Amphion (formerly Integrated Silicon Systems) is the leading supplier of speech coding, video/image processing and channel coding application specific silicon cores for system-on-a-chip (SoC) solutions in the broadband, wireless, and multimedia markets

**Web:** [www.amphion.com](http://www.amphion.com)

**Email:** [info@amphion.com](mailto:info@amphion.com)

## CORPORATE HEADQUARTERS

Amphion Semiconductor Ltd  
50 Malone Road  
Belfast BT9 5BS  
Northern Ireland, UK

Tel: +44.28.9050.4000

Fax: +44.28.9050.4001

## EUROPEAN SALES

Amphion Semiconductor Ltd  
CBXII, West Wing  
382-390 Midsummer Boulevard  
Central Milton Keynes  
MK9 2RG England, UK

Tel: +44 1908 847109

Fax: +44 1908 847580

## WORLDWIDE SALES & MARKETING

Amphion Semiconductor, Inc  
2001 Gateway Place, Suite 130W  
San Jose, CA 95110

Tel: (408) 441 1248

Fax: (408) 441 1239

## CANADA & EAST COAST US SALES

Amphion Semiconductor, Inc  
Montreal  
Quebec  
Canada

Tel: (450) 455 5544

Fax: (450) 455 5543

---

## SALES AGENTS

### Voyageur Technical Sales Inc

1 Rue Holiday  
Tour Est, Suite 501  
Point Claire, Quebec  
Canada H9R 5N3

Tel: (905) 672 0361

Fax: (905) 677 4986

### Phoenix Technologies Ltd

3 Gavish Street  
Kfar-Saba, 44424  
Israel

Tel: +972 9 7644 800

Fax: +972 9 7644 801

### SPINNAKER SYSTEMS INC

Hatchobori SF Bldg. 5F 3-12-8  
Hatchobori, Chuo-ku  
Tokyo 104-0033 Japan

Tel: +81 3 3551 2275

Fax: +81 3 3351 2614

### JASONTECH, INC

Hansang Building, Suite 300  
Bangyidong 181-3, Songpaku  
Seoul Korea 138-050

Tel: +82 2 420 6700

Fax: +82 2 420 8600

### SPS-DA PTE LTD

21 Science Park Rd  
#03-19 The Aquarius  
Singapore Science Park II  
Singapore 117628

Tel: +65 774 9070

Fax: +65 774 9071