X-Wall MX+ Specification
Rev. 2.0

Product SKU (Stock Keeping Unit):

X-Wall MX+

Product Brief Description:

SATA-to-SATA real-time crypto module with selectable AES ECB, CBC, CBC with Tweak and XTS 256-bit encryption strength at SATA Gen 3 (6 Gb/s,) Gen 2 (3 Gb/s,) and Gen 1 (1.5 Gb/s) speed. The X-Wall MX+ also allows setting encrypted data key along with identity and role based authentication capabilities derived from the built-in RSA2048, HMAC, CMAC, SHA256, and DRBG RNG hardware crypto modules.

Revision History

Rev No.	Description	Author	Rev. Date
0.1	Draft release	Butz Huang Benson Liu Chung-Yen Chiu	03/05/2015
1.0	Formal Release	Robert Wann	03/10/2015
1.1	Correct PIN#13 ESCK and PIN#36 VDD12; General editing	Robert Wann	12/22/2015
1.11	Sync Pin definition & reference schematics to pre-MP	Butz Huang	12/28/2015
2.0	Revised and general editing of the followings: 1. pin definition 2. reference schematics 3. DC characteristics 4. power consumption 5. layout guideline 6. Add I2C Master/Slave protocols	Butz Huang Robert Wann Chung-Yen Chiu	01/26/2016

Asia Pacific
Enova Technology Corporation
1st Floor, #11, Research & Development 2nd Rd.
Science-based Industrial Park, Hsin-Chu City
Taiwan 30076, Republic of China
P +886 3 577 2767 F +886 3 577 2770
www.enovatech.net; info@enovatech.net;

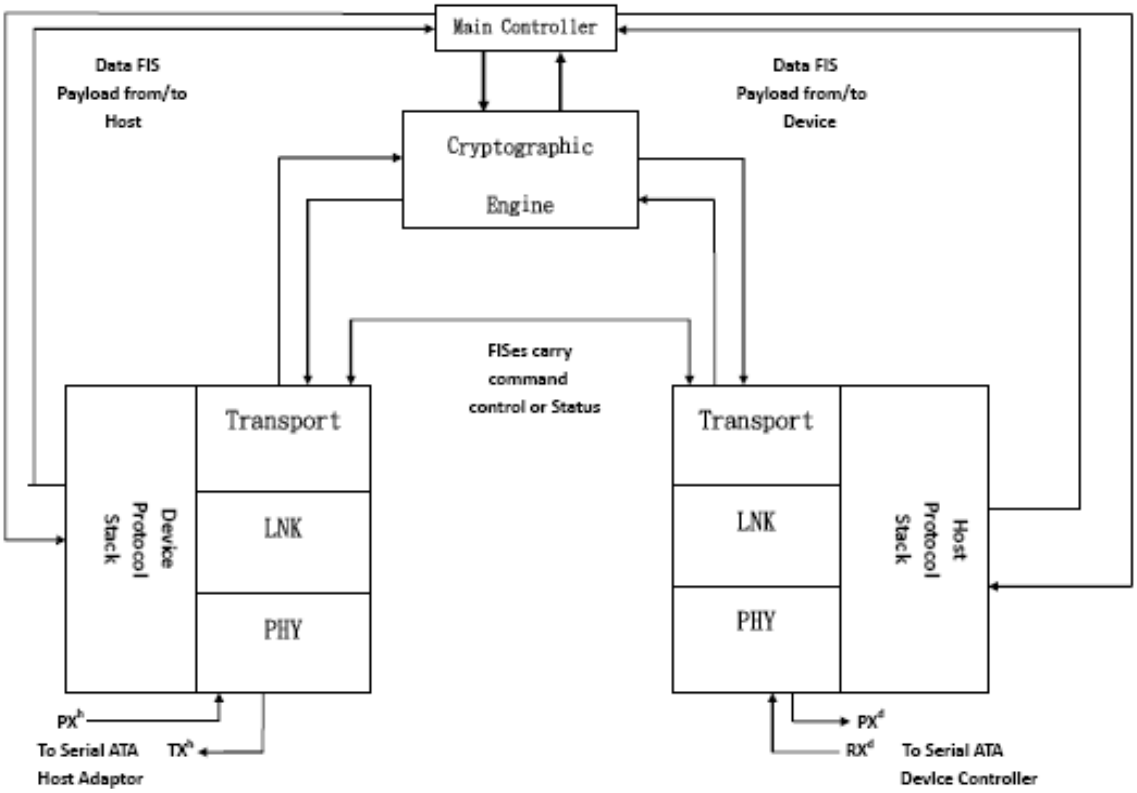
North America
Enova Technology
1918 Junction Avenue
San Jose, California 95131, USA
P +1 510 825 7900
http://www.enovatech.com
www.enovatech.com; info@enovatech.com

Table of Content

Introduction

The *X-Wall® MX+* family ASIC (Application Specific Integrated Circuit) is the 10th generation of patented[1] *X-Wall* ***real-time disk encryption*** technology. It is engineered specifically to encrypt/decrypt any standard SATA disk drive and SSD (Solid State Disk) including boot sector and operating system with a maximum 6Gbps **(6 gigabit per second at SATA Gen 3)** speed. Aside from the real-time disk encryption capability provided by the built-in AES ECB, XTS, CBC or CBC with Tweak block ciphers, users can also benefit from its internal RSA2048, HMAC, CMAC, SHA256 and DRBG RNG hardware crypto modules for setting encrypted data keys and most importantly, identity and role based authentication capabilities. The *X-Wall MX+* enhances both security and performance of its predecessor *X-Wall MX* and is progressing for FIPS 140-2 level 3 single chip crypto module certification.

How does it work



[1] US Patents 7,136995, 7,386,734, 7,900,057 and other countries. See http://www.enovatech.com/patents.php

The *X-Wall MX+*, an SATA-to-SATA real-time cryptographic ASIC, sits in-line between a host SATA adapter and a device SATA controller, acting as an invisible transparent cryptographic bridge connecting both the SATA host adapter and the SATA disk drive while encrypting all addressable sectors of the disk drive at SATA wire speed using AES CBC, CBC with Tweak, XTS and/or ECB 256-bit mode of operation.

As above figure illustrated, the *X-Wall MX+* equips with a SATA Device Protocol Stack acting as a SATA device controller connecting to a computer SATA host adapter and a SATA Host Protocol Stack acting as a SATA host adapter connecting to a physical disk drive (the SATA device controller). The System performance with *X-Wall MX+* engaged is unaffected as the encryption/decryption operation is totally transparent to the host computer and to the connected drive. *X-Wall MX+* can be operated with SATA Generation III, II and I compliant storage drives with a maximum cryptographic throughput at 6 Gbps. The performance-optimized AES hardware engine performs all encryption and decryption. There are no extra software driver to be loaded, eliminating entirely the memory and interrupt overheads thus freeing up the host CPU. The *X-Wall MX+* is independent from and invisible to all known Operating Systems including embedded OS. As long as the drive is SATA compliant, *X-Wall MX+* will encrypt it. Once authenticated (meaning the secret key to operate the crypto engine is set), its operation is completely transparent to all users. There is no complex GUI involved therefore your regular computing behavior is unchanged.

Features & Services

Overall Features

- Built-in Power-On-Self-Test (POST) ability to ensure product reliability;
- POST includes all cryptographic function tests;
- Versatile Key Management through either 2-wire serial interface or built-in SATA API (Application Programming Interface) libraries; The entire key setting and authentication process can be all encrypted, leaving no trace to clear text key data;
- 100% hardware AES (ECB,CBC, CBC with Tweak and XTS mode of operation) cryptographic engine producing SATA generation 3 line speed performance;
- Supports CBC IV scramble scheme with AES ECB algorithm, which may enhance the key strength up to 512 bits;
- Support XTS DUSN (Data Unit Sequence Number) key with AES ECB algorithm, which may enhance the key strength up to 512 bits;

- Built-in HMAC, CMAC, SHA256, RSA-2048 & DRBG RNG hardware crypto modules for enhanced security application; and
- Supports OTP EFUSE for storing critical security parameters.

SATA Features

- Supports Serial ATA Gen 3 at 6Gbit/s data transfer rate;
- Compliant with Serial ATA specification rev 3.1;
- Equips with both SATA Device Controller and SATA Host Adapter to transparently bridge a computer SATA host adapter and a SATA disk drive where the front-end port (SATA Device Protocol Stack, AKA SATA Device Controller) is connected to a computer SATA Host Adapter and the back-end port (SATA Host Protocol Stack, AKA SATA Host Adapter) is connected to a SATA Disk Drive;
- Support NCQ (Native Command Queue); and
- Supports FIS-based Switching for port multiplier (PM) function.

Enhanced Security Features & Services

- Built-in RSA 2048 bits PKI – hardware crypto module for Private/Public Key pair generation, sign (Signature) and verify;
- Built-in DRBG (Deterministic Random Bit Generator) RNG – hardware crypto module for seeding materials and TRNG (True Random Number Generator) for Entropy source;
- Built-in HMAC – hardware crypto module for Hashed Message Authentication Code;
- Built-in CMAC – hardware crypto module for Cryptographic Message Authentication Code;
- Built-in SHA256 – hardware crypto module for hash operation;
- Built-in OTP EFUSE for storing critical security parameters;
- AES CBC, CBC with Tweak, XTS and ECB block ciphers – hardware crypto module with selectable AES mode of operation for real-time block ciphering;
- Supports TCG OPAL 2.0 – software service for secure authentication through OPAL; and
- Supports IEEE1667 – software service for authentication in host attached transient storage device.

Miscellaneous

- Supports master/slave mode for 2-wire interface which is compliant with I^2C;
- Trusted and Secure *X-Wall MX+* SATA Cryptographic API;
- Trusted and Secure *X-Wall MX+* Master/Slave cryptographic protocols accessible through standard I^2C interface;

- 64-pin LQFP package (QFN package can be made available upon specific request);
- RoHS & Lead-free compliant;
- 5 (Five) years warranty for selective parts; and
- Optional industrial operating temperature from -45 to +90C.

X-Wall MX+ Pin Definitions

Pin Definition and Description

PHY INTERFACE				
NAME	**PIN**	**DIR**	**TYPE**	**DESCRIPTION**
SSRXPA SSRXMA	22 23	I		[redacted]
SSTXPA SSTXMA	26 25	O		[redacted]
RREFA	28	I/O		[redacted]
SSRXPB SSRXMB	58 57	I		[redacted]
SSTXPB SSTXMB	54 55	O		[redacted]
RREFB	52	I/O		[redacted]
				The SATA Channel A is the designated front-end port connecting to a SATA Host Adaptor of a computer whereas the SATA Channel B is the back-end port connecting to a SATA device controller of a disk drive.
Subtotal	10			
CLOCK AND PLL CONTROL PINS				
NAME	**PIN**	**DIR**	**TYPE**	**DESCRIPTION**
XSCI	39	I	PXOE1C	[redacted]
XSCO	38	O	DG	
CLKEN	33	I		
CLK25	10	I/O		
Subtotal	4			
GENERAL PURPOSE I/O AND INDICATOR SIGNALS				
NAME	**PIN**	**DIR**	**TYPE**	**DESCRIPTION**
RSTN	16	I		[redacted]
ERR	4	O		
DATA	3	O		

GPIO_0 GPIO_1 GPIO_2 GPIO_3 GPIO_4 GPIO_5	41 42 43 44 45 46	I/O		[redacted]
Subtotal	9			
TWO WIRES SERIAL INTERFACE				
NAME	**PIN**	**DIR**	**TYPE**	**DESCRIPTION**
SCL	49	I/O		[redacted]
SDA	50	I/O		[redacted]
Subtotal	2			
OTP EFUSE INTERFACE				
NAME	**PIN**	**DIR**	**TYPE**	**DESCRIPTION**
VDDQ	19	I		[redacted]
VEN	18	O		[redacted]
VGOOD	17	I		[redacted]
Subtotal	3			
DRBG INTERFACE				
NAME	**PIN**	**DIR**	**TYPE**	**DESCRIPTION**
ESIO	14	I/O		[redacted]
ESCK	13	O		[redacted]
Subtotal	2			
POWER GROUND				
NAME	**PIN**	**DIR**	**TYPE**	**DESCRIPTION**
AVCC12A	20 27			Analog 1.2V power
AGND12A	21 24			Analog ground of AVCC12A.
AVCC12B	53 60			Analog 1.2V power
AGND12B	56 59			Analog ground of AVCC12B.

VDDIO	2, 15, 35, 51			Digital 3.3V supply for I/O.
VSSIO	9, 40			Digital ground for I/O.
VDD12	12, 36, 47, 62			Digital 1.2V supply for core.
VSS12	11, 37, 48, 61			Digital ground for core.
Subtotal	22			
Total	64			

Electrical Characteristics

This section contains electrical specification for the *X-Wall MX+* crypto module. Please note, however, stressing conditions beyond the "Absolute Maximum Ratings" may cause permanent damage to the device. Operating beyond the "Maximum" condition is not allowed and extended exposure beyond the "Maximum" condition may adversely affect life and reliability of the *X-Wall MX+* crypto module, situation which voids the warranty.

Absolute Maximum Ratings

Symbol	Parameter	Value		Unit
		Min	Max	
Ts	Storage Temperature	-55	+125	°C
Ta	Operating Temperature (Normal)	0	+70	°C
Ta'	Industrial Operating Temperature (upon special request)	-45	+90	°C
VDDIO	I/O 3.3V Supply Voltage	-0.5	3.6	V
VDD12	1.2V Digital core Supply Voltage	-0.5	1.32	V
AVCC12	1.2V Analog Supply Voltage	-0.5	1.32	V
VIN_IO	Input I/O Signal Voltage	-0.5	VDDIO+10%	V
VO_IO	Output I/O Signal Voltage	-0.5	VDDIO+10%	V
Iout	I/O output current	4	16	mA

***The output current of pin CLK25 is 8mA.**

DC Characteristics

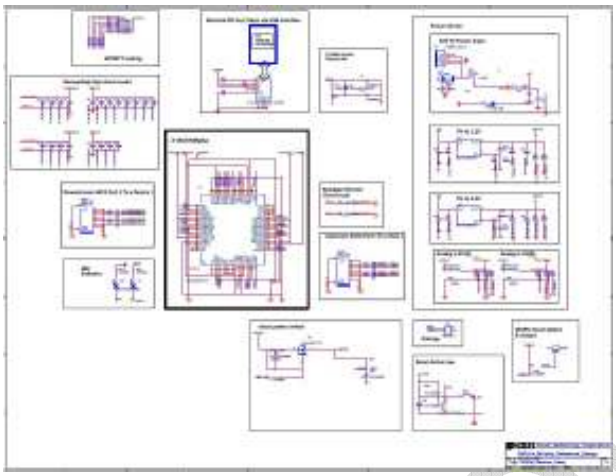
Symbol	Parameter	Value			Unit
		Min	Typ	Max	
VDDIO	I/O 3.3V Supply Voltage	2.97	3.3	3.6	V
VDD12	1.2V Digital core Supply Voltage	1.08	1.2	1.32	V
AVCC12	1.2V Analog Supply Voltage	1.08	1.2	1.32	V
VIH_{IO}	Input HIGH Voltage for general IO pins	2		3.6	V
VIL_{IO}	Input LOW Voltage for general IO pins	-0.5		0.8	V

Power Consumption

Symbol	Description	Test Conditions	SATA Gen 1	SATA Gen 2	SATA Gen 3	Units
I_{1v2}	Current consumption of 1.2V digital and analog power.	1.2V, OOB handshaking				mA
		1.2V, Active & continue burst	370	431	634	mA
		1.2V, Power down	14			mA
P_{1v2}	Power consumption of 1.2V digital and analog power.	Active, continue burst	0.444	0.517	0.760	W
I_{3v3}	Current consumption of 3.3V I/O power.	3.3V applied	9			mA
P_{3v3}	Power consumption of 3.3V I/O power.	3.3V applied	0.0297			W

Reference Design - Typical Application Schematics

A typical independent adapter design using the *X-Wall MX+* is shown below, where the *X-Wall MX+* provides two SATA connectors, a Mini-USB like key interface, an SPI flash, LED indicators and some control circuits. For detailed circuit layout files and Bill of Materials, please contact your sales representatives. For special implementation such as customized SDK and software source codes, send your inquiries to info@enovatech.com.



PCB Trace Routing

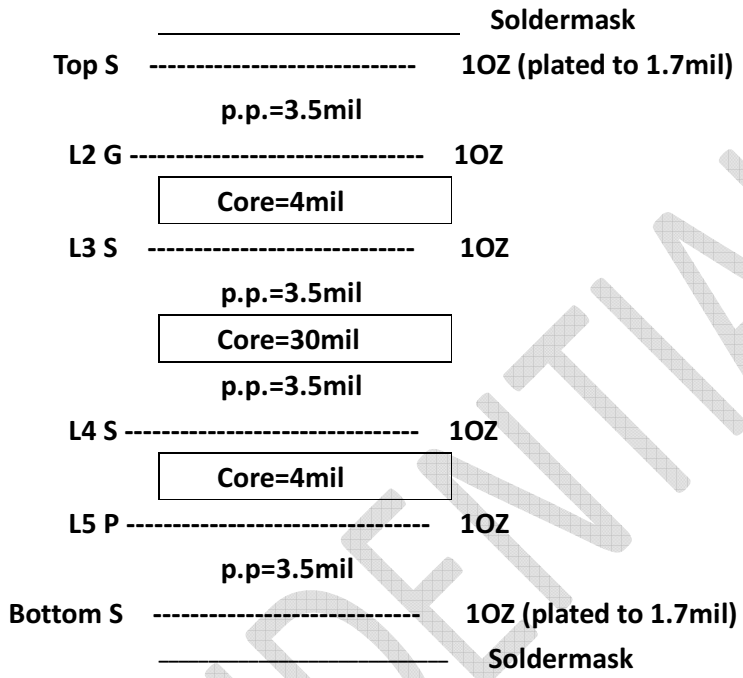
The routing of *X-Wall MX+* signals requires careful attention. The following bullets are general guidelines for signal routing. Note, however, this guideline does not cover the entire horizon of a complete design other than dealing with *X-Wall MX+* specifically.

6 Gbits SATA signal layout Guideline

- Impedance control: Differential impedance 100 ohm and single-end 50 ohm.
- Differential pair length matching criteria: +- 1 mils
- Each differential pair must go symmetrically and stay on the same layer as possible. Less via number is suggested and max via number is suggested to be 2 along every path of SATA traces.
- There must be a continuous reference plane under routing of all differential signals. The AGND12 is suggested to be the best ground plane under SATA signals.
- Do not Route SATA traces underneath or near components that employ high clocking.

PCB Stack-up

Example shown below is a 6-layers PCB stack-up implementation.



PCB total thickness is 1.60mm

Layer	Single ended 50 Ω	Differential 100 Ω		Ref.
	Trace width	Trace width	Spacing	
Top	5mil	4mil	8mil	Layer2
Layer3	5mil	4mil	8mil	Layer2/Layer5
Layer4	5mil	4mil	8mil	Layer2/Layer5
Bottom	5mil	4mil	8mil	Layer5

X-Wall MX+ 2-wire Serial Interface

The paragraphs described below address basics of the *X-Wall MX+* 2-wire serial interface and does not involve with any cryptographic function such as HMAC or CMAC. Consult with your sales representative to obtain protocol details on how the *X-Wall MX+* communicates with an external I2C component using HMAC or CMAC.

Master Mode

[redacted]

Slave Mode

[redacted]

Master Protocol

Page Write Protocol

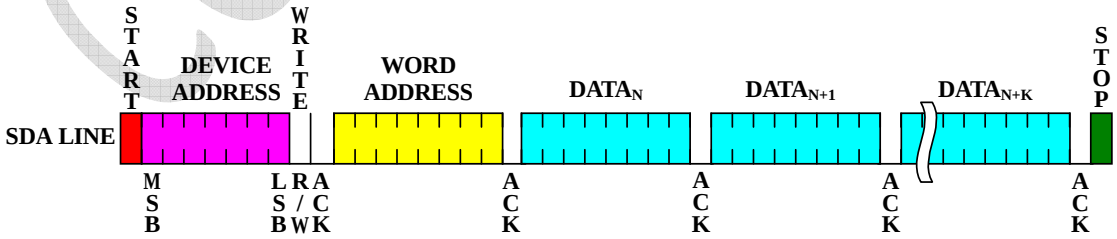


Figure 1. A page-write protocol: (page_write(device_address, start_address, data_byte#1, data_byte#2,…, data_byte#n);)

Byte Write Protocol

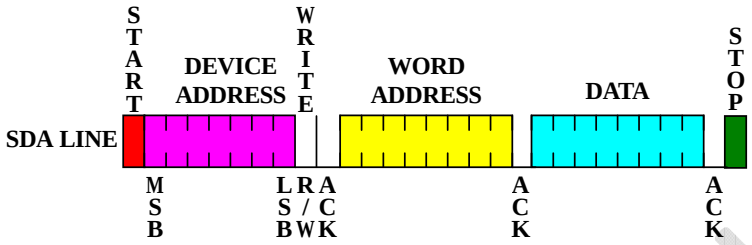


Figure 2. A byte-write protocol: (write_byte(device_address, word_address, data_byte);)

Byte Read Protocol

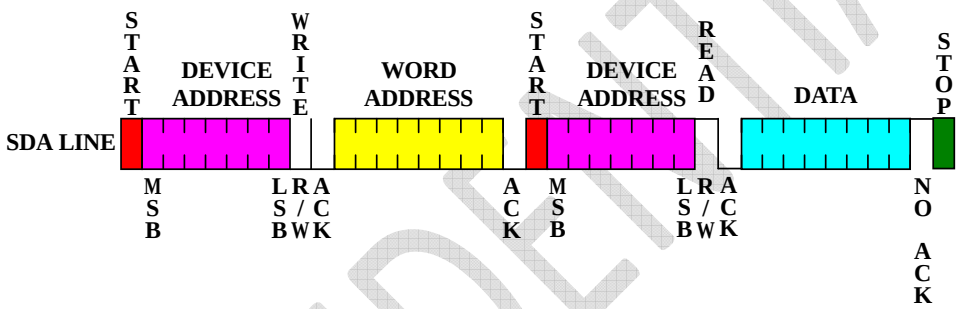


Figure 3. A byte-read protocol: (byte_read(device_address, word_address);)

Slave Protocol

Table 1 *X-Wall MX+* I²C Slave protocol for setting keys

STEP	INSTRUCTIONS	COMMENTS	MEANING
1			
2			
3			

Table 2 Definition of *X-Wall MX+* Key buffers

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00																

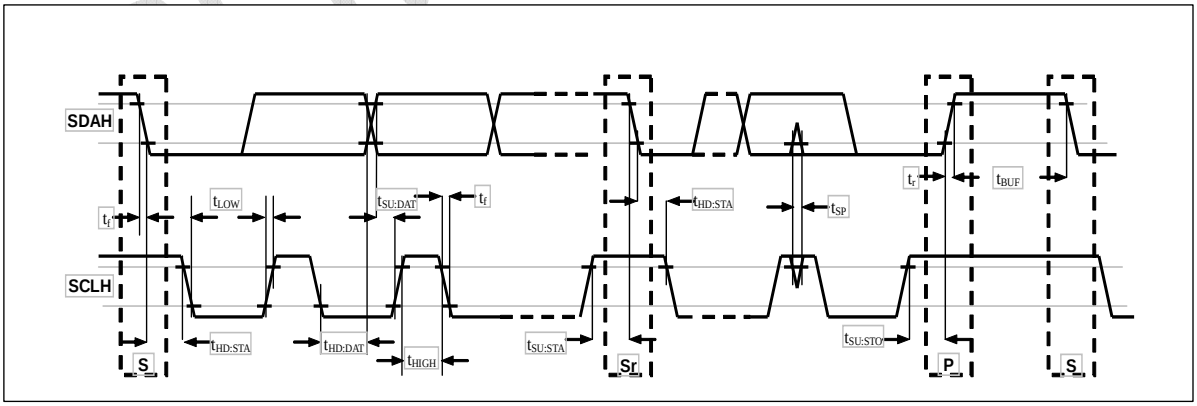
01	
02	[redacted]
03	
04	[redacted]
05	
06	[redacted]
07	

Special note with regard to using the key buffers:

- IV scrambled keys are used for AES-CBC (optional) and AES-XTS (mandatory);
- For AES-ECB mode, encryption IV scrambled key and decryption IV scrambled key are redundant. Leave them blank or fill all zeros into these registers when *X-Wall MX+* ASIC with AES-ECB mode is selected;
- Encryption data key equals to decryption data key by default. In some unique and more secure applications, one may choose different key value to fill up the respective key register.

X-Wall MX+ 2-wire Serial Interface Basic

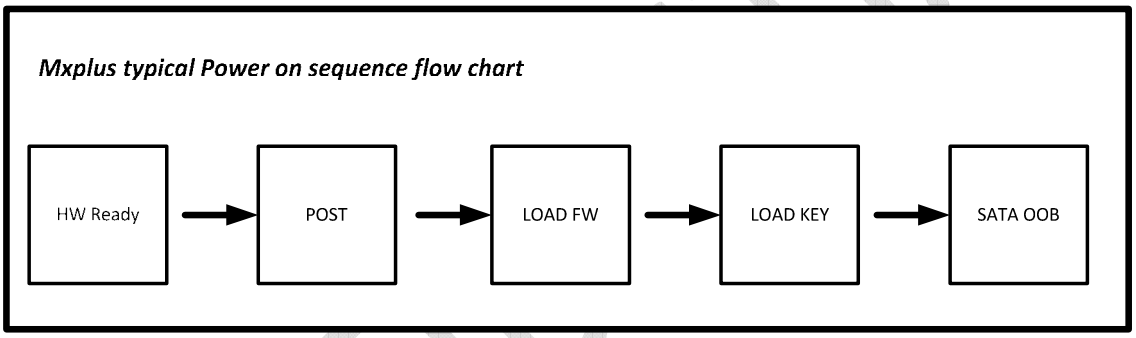
The interface has two bus wires. The first one, namely SDAH, is used for transmitting and receiving serial bit data. The second one, namely SCLH, is used for transmitting (under master mode) and receiving (under slave mode) clock pulses. By combining those two signals the START, repeated START and STOP conditions are created, which are then used for constructing entire bus protocol. Listed below is the signal-timing specification of SDAH and SCLH.



PARAMETER	SYMBOL	MIN.	MAX.	UNIT
SCL clock frequency	f_{SCL}	0	400	KHz
Hold time (repeated) START condition (**S**). After this period the first clock pulse is generated.	$t_{HD:STA}$	0.6	-	µs
LOW period of the SCL clock	t_{LOW}	1.3	-	µs
HIGH period of the SCL clock	t_{HIGH}	0.6	-	µs
Set-up time for a repeated START condition (**Sr**)	$t_{SU:STA}$	0.6	-	µs
Data hold time	$t_{HD:DAT}$	0	0.9	µs
Data set-up time	$t_{SU:DAT}$	100	-	ns
Rise time for both SDA and SCL signals	t_r	$20+0.1C_b$	300	ns
Fall time for both SDA and SCL signals	t_f	$20+0.1C_b$	300	ns
Setup time for STOP condition (**P**).	$t_{SU:STO}$	0.6	-	µs
Bus free time between a STOP and a START condition.	t_{BUF}	1.3	-	µs
Pulse width of spikes, which must be suppressed by the input filter.	t_{SP}	0	50	ns
C_b: total capacitance of one bus line if pf.				

Power On Sequence

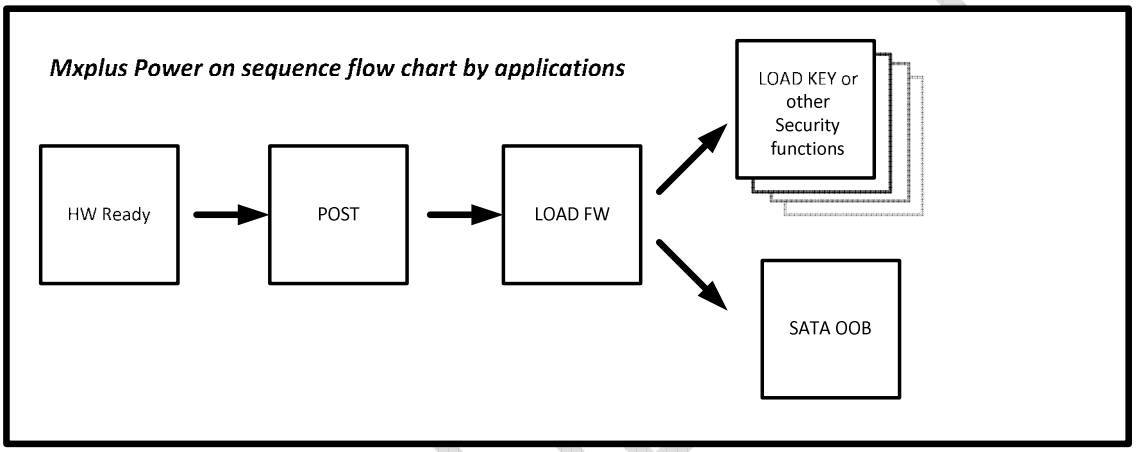
The *X-Wall MX+* features below power on sequence with special notion made to the steps "LOAD KEY" and "SATA OOB." On one possible implementation, the step "LOAD KEY" must be completed prior to any SATA link would establish, meaning the connected SATA disk drive would not be seen, as if the disk drive is absent, by the system unless the LOAD KEY process is completed. On another possible implementation, the SATA Link is established and the system simply waits for the LOAD KEY step being completed, meaning the connected SATA disk drive is seen as an unformatted disk drive waiting to be initialized. There are advantages to each of the above implementation and it's up to the designer's preference and security requirement. See below default flow chart diagram and explanations:



- **HW Ready or Hardware Ready**: Power stable, clock stable and valid reset signal asserted;
- **POST**: Power On Self Test; the POST initiates entire states which also involves with all Crypto Modules self testing.
  Caution! All security configurations and parameters are cleared after POST stage;
- **LOAD FW or Load Firmware**: *X-Wall MX+* starts loading the additional firmware code if available;
- **LOAD KEY or Load Key**: *X-Wall MX+* as a Master will start searching for a Slave device that may contain an *AES Secret Key* on the 2-wire Serial Interface (pin47 SDA and pin48 SCL respectively). If the *AES Secret Key* exists, *X-Wall MX+* loads the *AES Secret Key*. If the Slave device is not found, the *X-Wall MX+* by itself enters into Slave mode waiting for an external Master command. More, entire *X-Wall MX+* **I²C** Mater and Slave protocols can be made secured through the built-in HMAC, CMAC, SHA256, DRBG RNG, or RSA2048 capabilities. Alternatively, the step "LOAD KEY" can be accomplished through the specifically engineered *MX+* SATA API commands and library using advanced security features such as HMAC, CMAC, SHA256, DRBG RNG, or RSA2048. Please contact your Enova sales representative for the correct implementation.

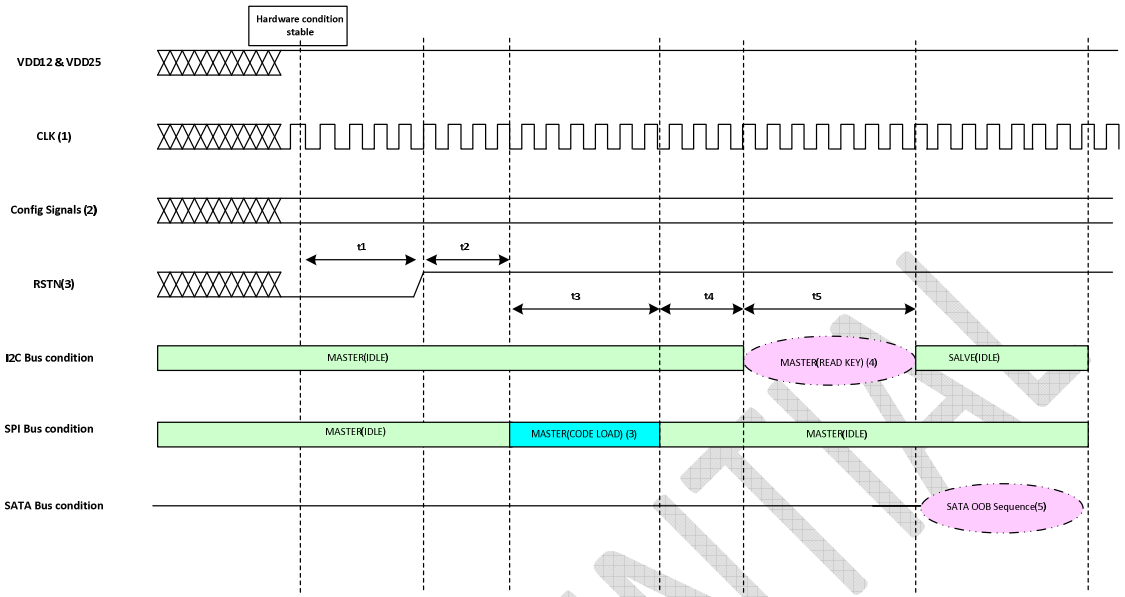
- **SATA OOB**: In OOB stage the *X-Wall MX+* waits for the active SATA OOB sequences. Once SATA OOB sequence occurs, *X-Wall MX+* will complete the process of OOB handshaking including speed negotiation and SATA link establishment.

Various security applications may require different power on sequence for which the *X-Wall MX+* may be able to support via additional firmware update. Consult Enova Technology engineering for additional requirements. Similarly, the timing of the SATA OOB link could be adjusted according to the desirable conditions being met. See below diagram for a brief explanation:



The diagram below shows detailed timing of typical *X-Wall MX+* Power-On Sequence.

X-Wall MXplus Power-On Sequence



(1) CLK : The external 25MHz clock generated by Crystal or oscillator.
(2) All configuration and hardware strapping signals must be ready and stable before valid reset operation.
(3) RSTN : A valid reset signal must be asserted low for t**1 period.**
(4) Mxplus SPI activity to load external firmware code
(5) Mxplus I2C activity to load AES KEY if needed (option by application)
(6) MXplus Starts to handle SATA OOB sequence at both SATA ports.

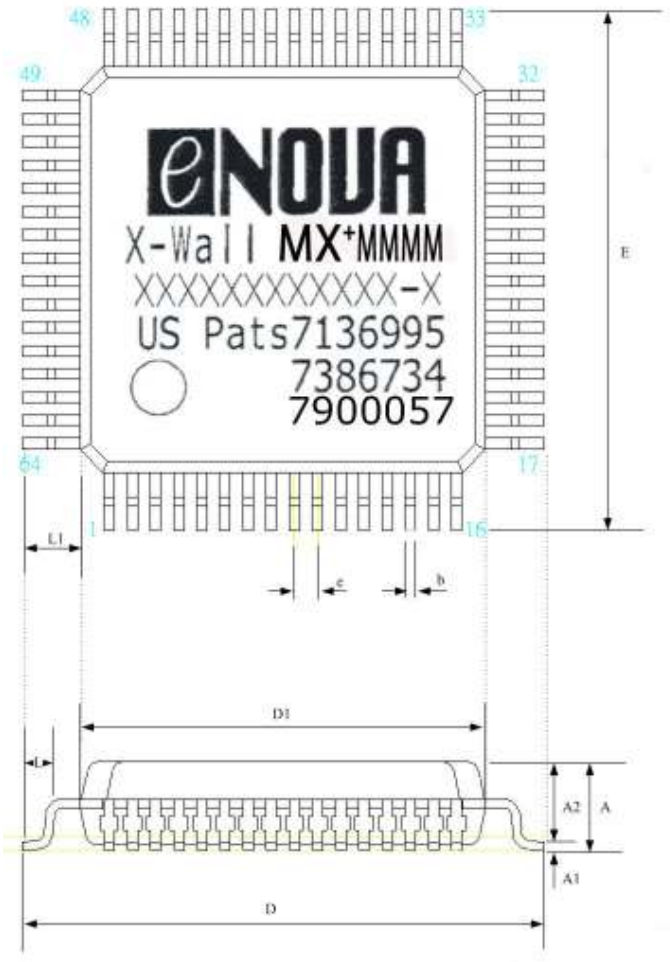
Name	Description	Value	Comment
t1	Reset time	>100ns	Minimum reset time
t2	Self test time	~26ms	
t3	Bus activity	~17ms	*X-Wall MX+* Loads the firmware code if available
t4	Internal firmware runtime	~17ms	
t5	I2C bus activity	~1.3ms	Load Secret Key

Package Information

We offer standard 64 pins LQFP package. The QFN package is optional.
LQFP (Low-profile Quad Flat Package) provides low profile with 1.4mm body thickness, suitable for space concerned applications. Package size 7x7mm and lead-counts 64 are offered for portable, lightweight and low profile applications. **ALL Enova X-Wall ASIC comply with RoHS and Leaf-free specification with the following features.**

- 7mm x 7mm body size with 64 lead counts
- Copper lead frame
- Low profile 1.4mm body thinness
- Refer to JEDEC MA026(ISSUE D)/BBD

Outline and Dimension



Symbol	Dimension [mm]
e	0.4
b	0.18
D1	7.00
D , E	9.00
A	1.60(max)
A1	1.45(max)
A2	0.15(max)
L	1.00(REF)
L1	0.75(max)

X-Wall MX+ top Marking
MMMM:
To be specified.
XXXXXXXXXXXX-X
Total is 14 code: Lot Serial Number (8 digital code) + Date Code (4 digits code) +2 module run code (-M: mass run, -S:test sample run, -Q: quality run.)