Features

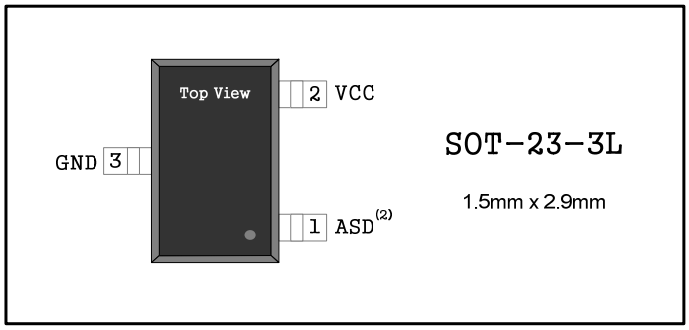
- High performance illegal copy protection IC
- 128bits encryption applied with AES-128
- ART(1) Interface, Supporting up to 25 Kbps
- 3.3V/1.8V Operation Voltage
- Built- in Power on Reset / 16MHz OSC
- Two Power Mode (Active, Sleep)

(1) Adaptive Reference Time (ART-1-Line Interface)

Applications

- DMB, Navigation
- Mobile Phone, PMP, MP3
- DVR(PVR), DVDP
- Set-Top Boxes (STBs)
- Etc.(Most of electronic system using u-Processor)

Pin Configuration



(2) ART Serial Data Pin

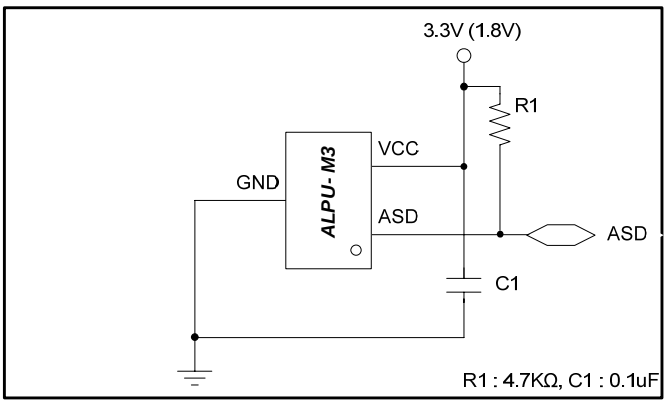
Ordering Information

Part	Operation Voltage	Package Type
ALPU-M3	3.3V	3L-SOT-23
ALPU-M3L	1.8V	3L-SOT-23

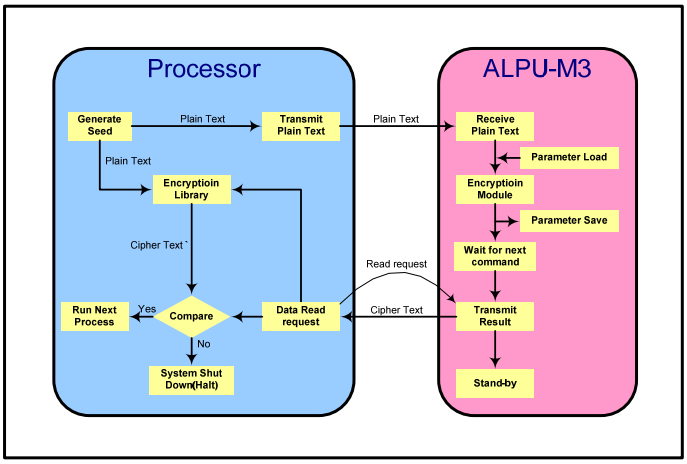
General Description

The ALPU-M3 is the high-end IC among the ALPU series. Its encryption core is based on Rijndeal AES-128 with 192-bits programmable parameters. It is a slave device that always operates with MCU through the serial bus.

Typical Operation Circuit



Encryption Flow



Contents

1. Overview ---------- 3
2. I/O Port ---------- 5
3. Clock Management ---------- 6
4. Power Mode ---------- 7
5. Initialization ---------- 8
6. Encryption ---------- 9
7. Communication Interface ---------- 13
8. Electrical Characteristic ---------- 17
9. Typical Operation Circuit ---------- 19
10. Package Information ---------- 20
11. Datasheet Revision History ---------- 21

1. Overview

ALPU-M3 is the high-end IC among the ALPU series. Its encryption core is based on Rijndael AES-128 with 192-bit programmable parameters. It is a slave device that always operates with MCU through the serial bus.

1.1. Features

1.1.1 Security

- High performance illegal copy protection IC
- 128 bit encryption applied with AES-128

1.1.2 Peripheral Features

- ART(1) Interface, Supporting up to 25 Kbps

(1) Adaptive Reference Time (1-Line Interface)

1.1.3 Special Features

- Built in Power-on-Reset
- Built in 16MHz OSC
- Two Power Modes : Active, Sleep

1.1.4 Operating Voltages

- 3.3V / 1.8V Operation Voltage

1.1.5 Package

- 3L-SOT23

1.2. Block Diagram

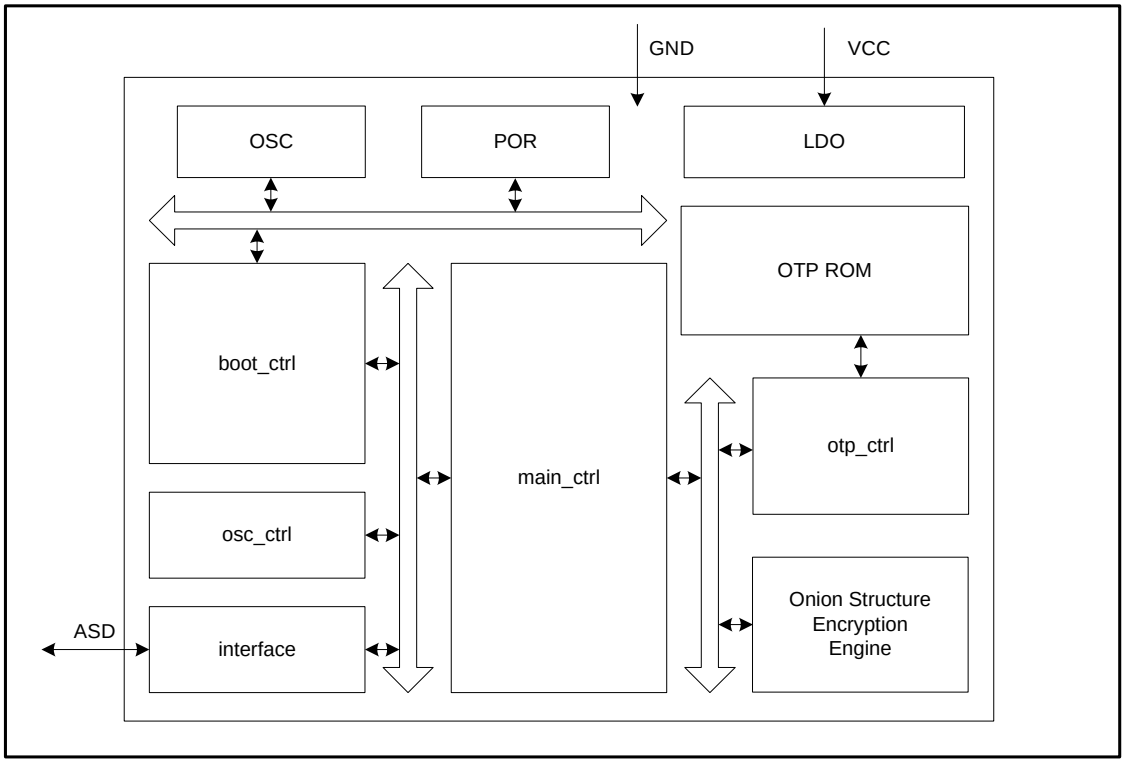


Figure 1-1. Block Diagram

ALPU-M3 consists of analog blocks (OSC, POR and LDO) and a memory block and digital logic ones. The boot control block manages the signals of analog blocks. And the main control block manages the communications between the digital blocks through two buses.

1.3. Pin Configurations

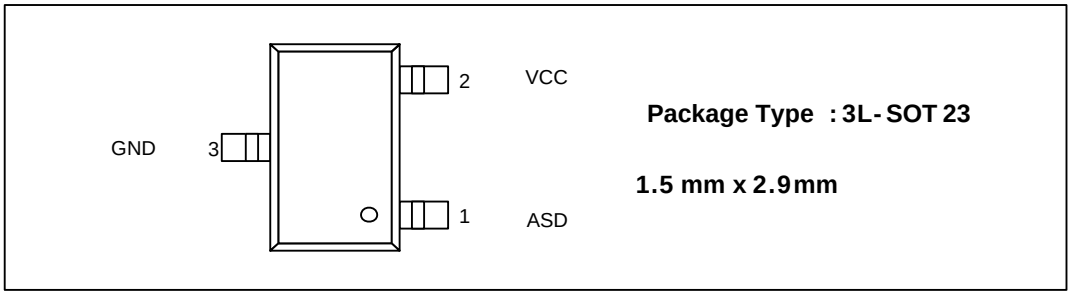


Figure 1-2. ALPU-M3 Pin Configuration

1.4. Pin Descriptions

Table 1-1. ALPU-M3 Pin Description

Pin Num	Pin Name	Description	Remark
1	ASD	ART Serial Data, CMOS Input / Open-Drain Output bi-directional I/O	
2	VCC [(1)]	Digital supply voltage	
3	GND	Ground	

Note [(1)] The ALPU-M3 operation voltage is supported by the two types, 1.8V or 3.3V

2. I/O Port

2.1 ESD protection circuit

ESD protection circuit for the whole chip is achieved as shown in Figure2-1. It can be protected the chip against two widely used industry standard ESD test models: Human Body Model (HBM) and Machine Model (MM). Both of these models test each pin against every other pin and/or a power/ground supply using a positive and a negative pulse.

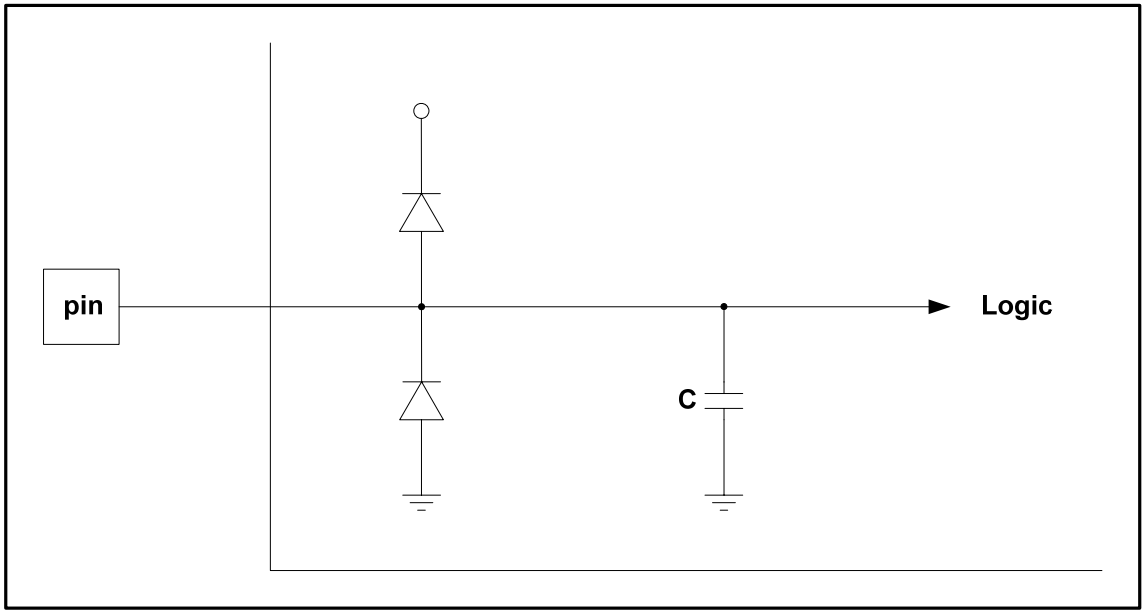


Figure 2-1. ESD protection circuit

2.2 I/O type

ALPU-M3 has I/O types as shown in Table2-1.

Table 2-1. I/O Types

Direction	Name	Description
Power	VCC	Digital supply voltage
	GND	Ground
Bi-direction Port	ASD	ART Serial Data bi-direction pin

2.2.1 Bi-direction Port (ASD)

This cell is a bidirectional buffer with CMOS input and 2mA n-channel open drain output.

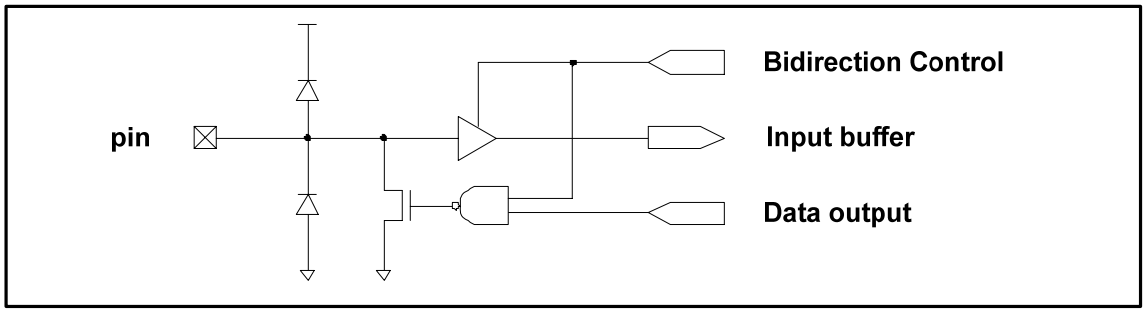


Figure 2-2. Bi-direction port Schematic

3. Clock Management

3.1 Internal clock

All Inner blocks use internal OSC clock. Internal OSC clock is approximately 16MHz shown in Table3-1.

Table 3-1. Internal OSC parameters (Ta = 25°C)

PARAMETER	SYMBOL	CONDITION	Min	Typ	Max	Unit
Frequency	f16m		14	16	18	MHz
Frequency Variation	Δf16m	-40≤Ta≤80°C	-	-	±10	%
Duty Cycle	Dmax		48	50	52	%

3.1.1 Clock on/off

Internal OSC clock can be turned on or off. If ALPU-M3 is in the condition of Sleep-mode, then internal OSC clock is turned off to save the power.

Here is the condition to enter the Sleep-mode. ASD pin stay high and all functions are

disabled for more than 2 seconds. When the conditions above are not met it wakes up to active-mode. (Refer to chapter 4. Power Mode)

4. Power Mode

ALPU-M3 supports the power saving mode called Sleep-mode in which internal oscillator is off.

4.1 Condition of entering Sleep-mode

Here is the condition to enter the Sleep-mode. ASD pin stay high and all functions are disabled for more than 2 seconds. (Refer to Figure 4-1)

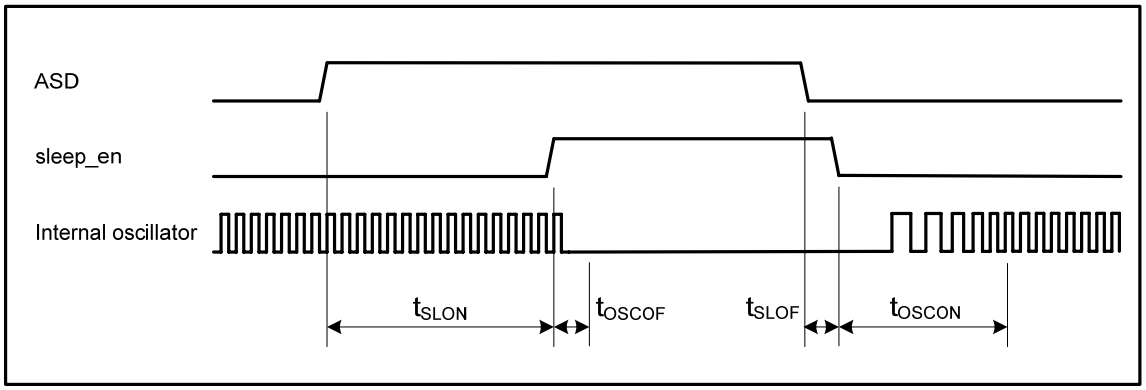


Figure 4-1. Sleep-mode Waveform

ASD : ART Data signal

sleep_en : internal sleep-enable signal

internal oscillator : 16MHz oscillator for internal logic

Table 4-1. Sleep-mode Waveform Parameters

Parameter	Symbol	MIN	TYP	MAX	Unit
Sleep-mode On Time	t_{SLON}	2000			ms
Sleep-mode Off Time	t_{SLOF}			10	ns
OSC On Time	t_{OSCON}			5	us
OSC Off Time	t_{OSCOF}			10	ns

4.2 Condition of exiting Sleep-mode

When the conditions are not met it wakes up to active-mode; ASD line goes down to low.

5. Initialization

ALPU-M3 has an internal POR (Power-on-Reset) circuit. When system power turns on ALPU-M3's POR resets its own system. During reset time, all internal registers of ALPU-M3 are configured as their initial values. After that, internal registers are set to the values in OTP memory. (Refer to chapter 9. Electrical Characteristic)

5.1 Start-up Waveform

After RESET, internal registers in ALPU-M3 need $t_{INITIAL}$ time period to initialize all registers. After $t_{INITIAL}$ time period ALPU-M3 enters the sleep mode.

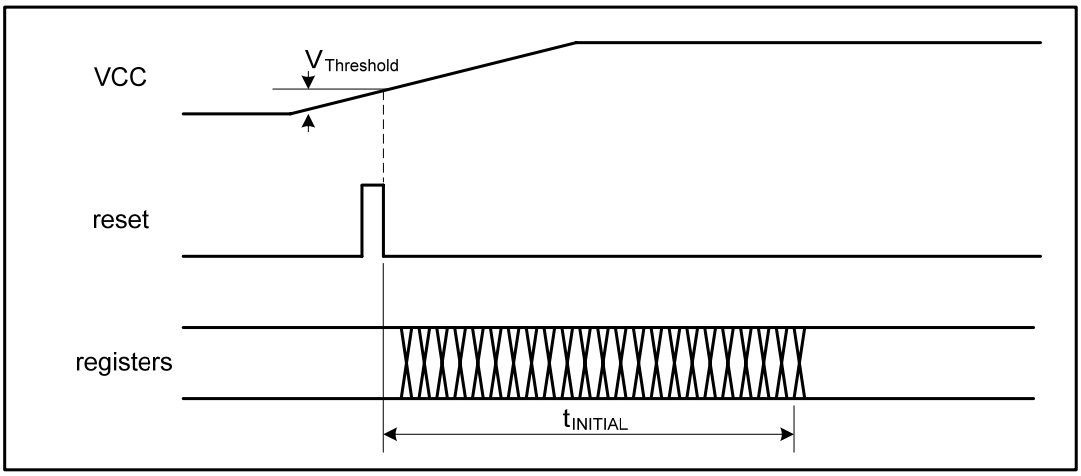


Figure 5-1. Start-up Waveform

VCC : 3.3V Supplied Power

reset : internal Power-on-Reset signal

registers : internal registers for initialization

Table 5-1. Start-up Timing Parameters

Parameter	Symbol	MIN	TYP	MAX	Unit
Threshold Voltage	$V_{Threshold}$	1.1	1.2	1.3	V
Initial Time	$t_{INITIAL}$			160	us

VCC information (Refer to chapter 10. Electrical Characteristic)

5.2 Internal Power-on-Reset

A Power-on-Reset (POR) pulse is generated by an On-chip detection circuit. The detection level is defined in Table5-1.The POR is activated whenever VCC is below the detection level (threshold voltage). The POR circuit ensures that the device is reset from Power-on. Reaching the POR threshold voltage invokes the delay counter, which determines how long the device is kept in RESET after VCC rise.

6. Encryption

6.1 Encryption Core Block Diagram

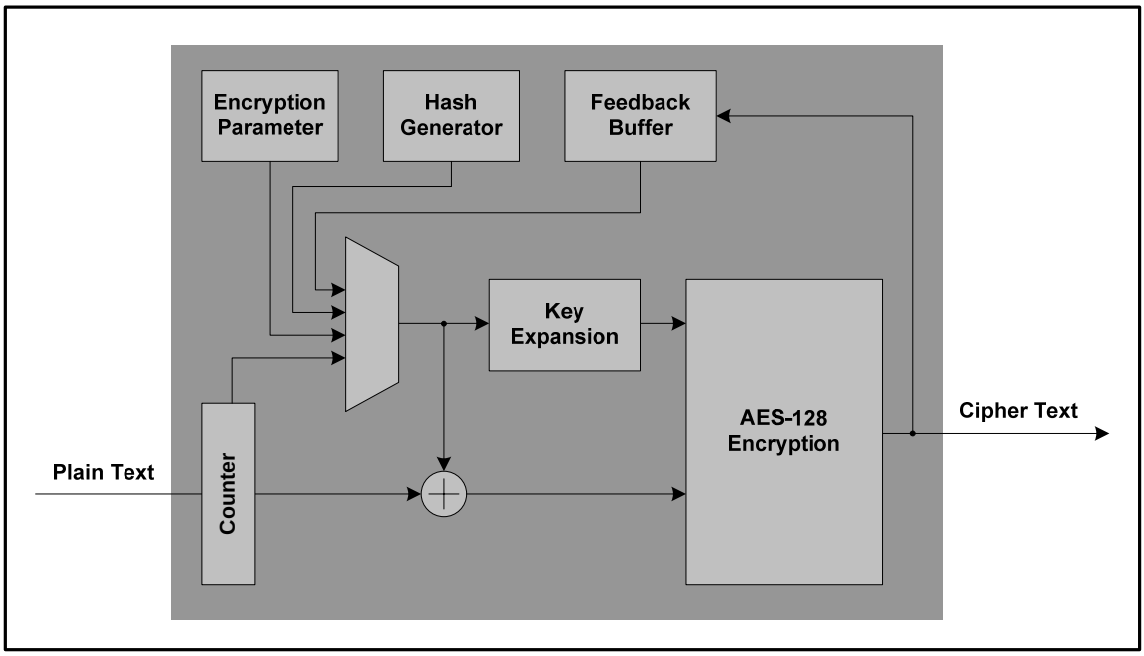


Figure 6-1. Encryption Core Block Diagram

ALPU-M3 has 128-bit encryption core applied with AES-128. The core consists of several blocks. They are AES-128 Core, Random Generator, Feedback buffers and Encryption parameter.

6.2 Encryption configured with IIC sub address

Encryption Core is configured with sub addresses as shown in Figure 6-2. Each encryption bit can be overlapped.

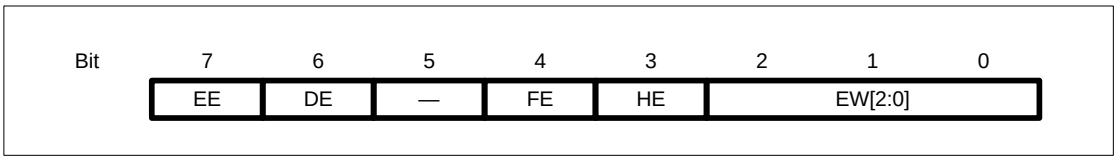


Figure 6-2. Sub Address Configuration

Bit 7: EE (Encryption Enable)

When EE bit is set 1, it is in Encryption Mode

Bit 6: DE (Double Enable)

When both EE and DE bits are set to 1, it is in Double Mode

Bit 5: Reserve

Bit 4: FE (Feedback Enable)

When both EE and FE bits are set to 1, it is in Feedback Mode.

Bit 3: HE (Hash Enable)

When both EE and HE bits are set to 1, it is in Hash Generation Mode

Bit 2~0: EW (Encryption Width)

The EW bits are loop count numbers of the encryption algorithm. It is recommended that the bits are set with random numbers.

6.3 Encryption Mode

6.3.1 Bypass Mode

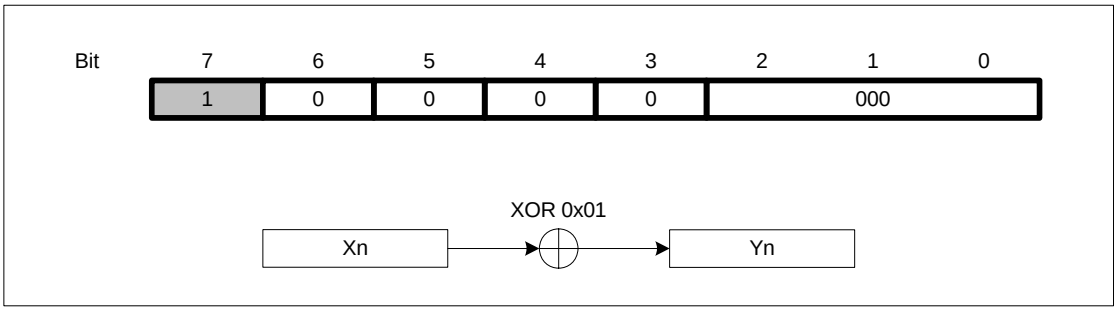


Figure 6-3. Bypass Mode Sub Address Construction

Bypass Mode is a mode to test the communication interface between CPU and ALPU-M3. The data(Xn) from CPU will do Exclusive OR operation with 0x01 in ALPU-M3

6.3.2 Double Encryption Mode

It is not able to open this information

6.3.3 Feedback Encryption Mode

It is not able to open this information

6.3.4 Hash Generator Mode

It is not able to open this information

6.4 Encryption Flow

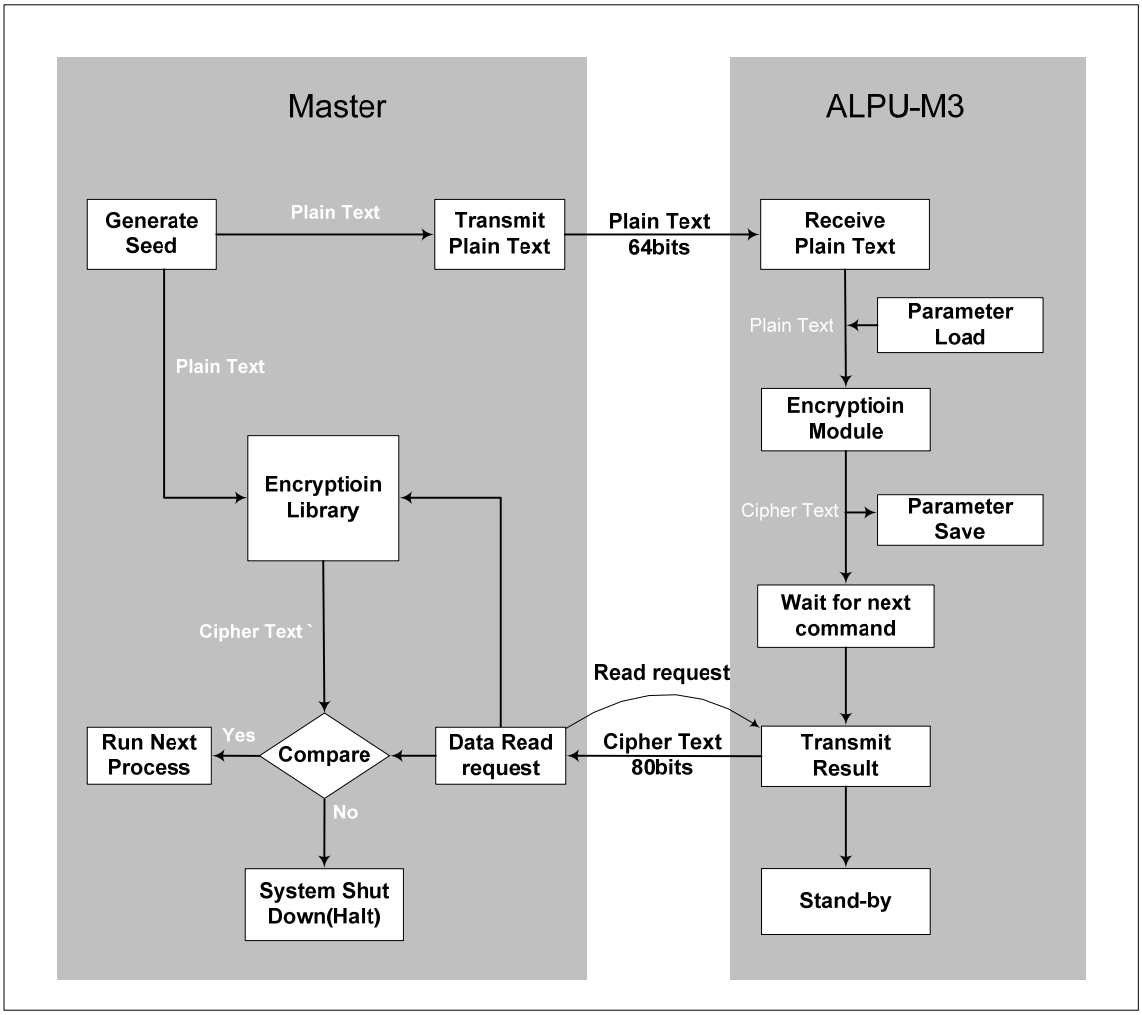


Figure 6-4. Encryption Flow

6.5 Communication Packet Structure

6.5.1 Write Packet Structure

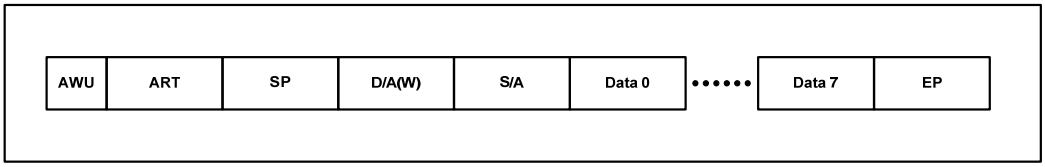


Figure 6-5. Write Packet Structure

AMU: Art Wake Up

ART: ART Preamble

SP: Start Preamble

D/A(W): Device Address (Write)

S/A: Sub Address

Data 0~7: 8byte Write Data (Seed data)

EP: End Preamble

6.5.2 Read Packet Structure

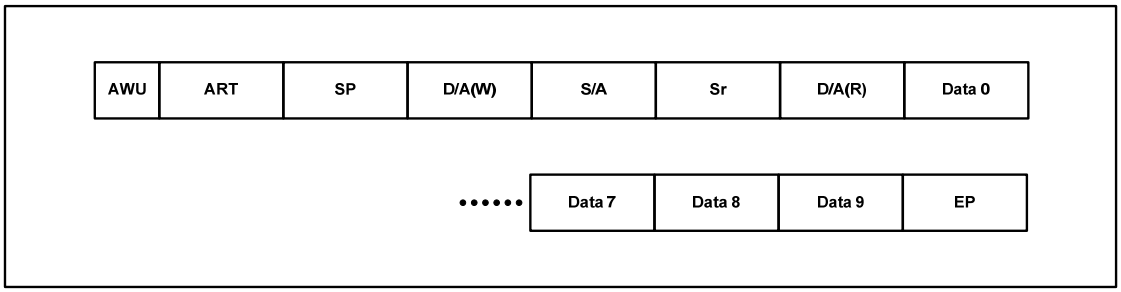


Figure 6-6. Read Packet Structure

AMU: ART Wake Up

ART: ART Preamble

SP: Start Preamble

D/A(W): Device Address (Write)

S/A: Sub Address

Sr: Repeated Start

D/A(R): Device Address (Read)

Data 0~9: 10bytes Read Data (Result data)

EP: End Preamble

6.6 Implementation

6.6.1 Bypass Mode

```
// Bypass Mode Set
sub_address = 0x80;

// Seed Generate
for ( i=0; i<8; i++) alpum1_tx_data[i] = rand();

// Write Seed Data to ALPU-M1
_art_write(device_address, sub_address, alpum1_tx_data, 8);

// Read Result Data from ALPU-M1
_art_read(device_address, sub_address, alpum1_rx_data, 10);

// XOR operation
for ( i=0; i<8; i++) alpum1_ex_data[i] = alpum1_tx_data[i] ^ 0x01;

// Compare the encoded data and received data
for (i=0; i<8; i++) {
        if (alpum1_rx_data[i] != alpum1_ex_data[i]) return 1; // Fail
}
return 0: // Pass
```

Figure 6-7. Bypass Mode example C code

1. Generate seed data(Plain Text) with the random data
2. Write seed data to ALPU-M3
3. Read Result data from ALPU-M3
4. Compare the encrypted data(Cipher Text) and received data

7. Communication Interface

7.1 ART interface (1-wire interface)

ART 1-Line communication is suitable to be applied in MCU. It operates as slave, and can be available 128 different device with just one MCU GPIO pin when ART protocol applied. 128 device must have different device address each other, and pull-up resistor is required on the data line. ART 1-Line interface is the format which NEOWINE is originative, and it is possible to support the speed form 8kbps to 25kbps.

7.1.1 Write Packet Structure

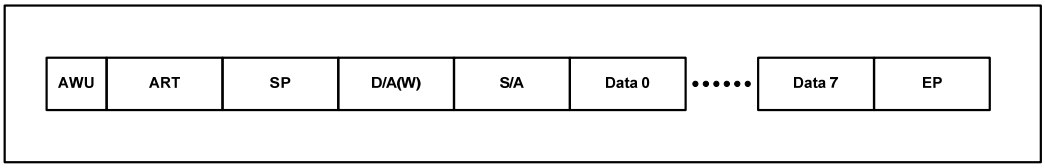


Figure 7-1. Write Packet Structure

AWU: Art Wake Up

ART: ART Preamble

SP: Start Preamble

D/A(W): Device Address (Write)

S/A: Sub Address

Data 0~7: 8byte Write Data (Seed data)

EP: End Preamble

7.1.2 Read Packet Structure

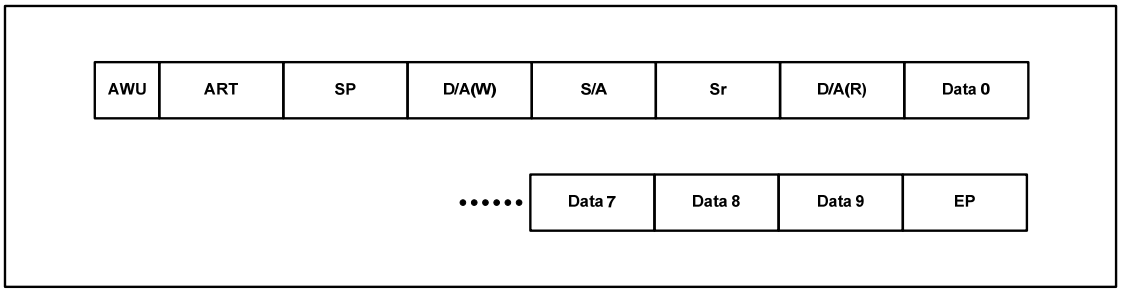


Figure 7-2. Read Packet Structure

AWU: ART Wake Up

ART: ART Preamble

SP: Start Preamble

D/A(W): Device Address (Write)

S/A: Sub Address

Sr: Repeated Start

D/A(R): Device Address (Read)

Data 0~9: 10bytes Read Data (Result data)

EP: End Preamble

7.1.3 ART Wakeup

ART Wakeup protocol is start signal prevent 1-wire communication. If the ALPU-M3 detect ART Wakeup signal, that is ready for 1-wire communication with ALPU-M3.

7.1.4 Start Preamble Structure (The same as ART Preamble)

Figure 9-3 shows the START PREAMBLE structure of ALPUM1. If the ALPU-M3 receive a correct START PREAMLE, ALPU-M3 transmit true('1') value for acknowledge.

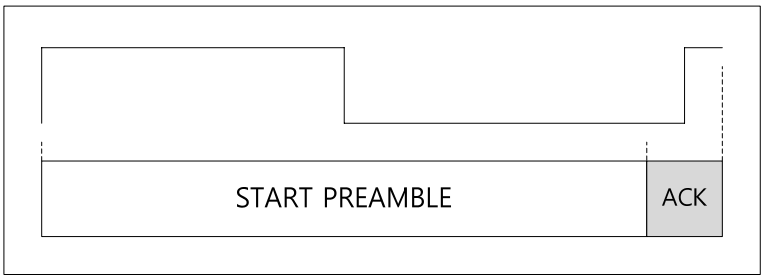


Figure 7-3. Start Preamble Structure

7.1.5 Byte Structure

Figure 7-4 shows the Byte structure of write data. ALPU-M3 transmit true('1') value every 4bits for acknowledge.

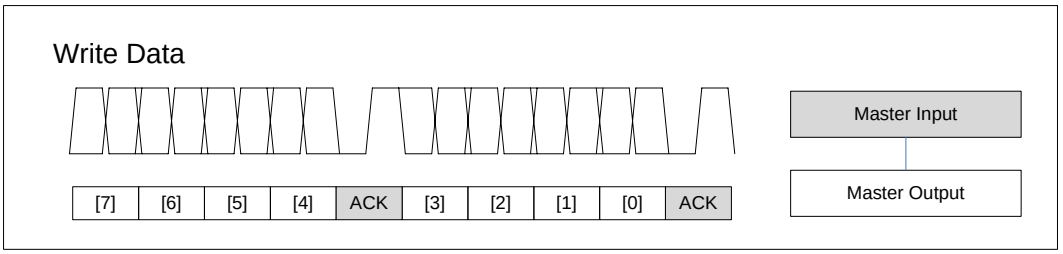


Figure 7-4. Write Byte Structure

Figure 7-5 shows the Byte structure of read data. MCU should transmit Sync signal High to ALPU-M3 after receiving 4bits data from ALPU-M3.

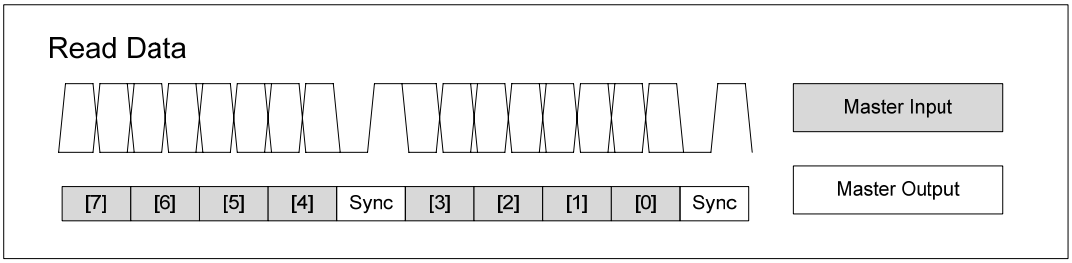


Figure 7-5. Read Byte Structure

7.1.6 Waveform & Definition of timing

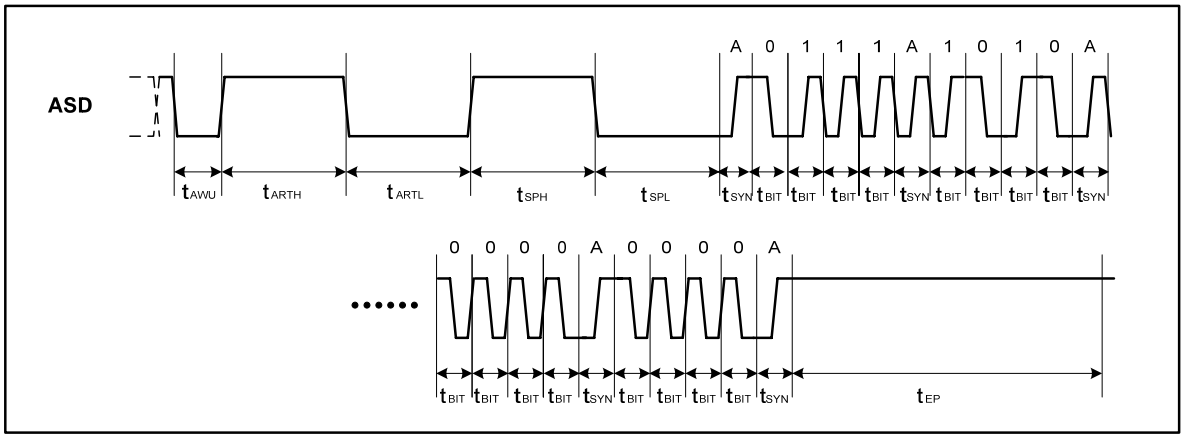


Figure 7-6. Definition of timing

Table 7-1. ART Timing Parameters

Parameter	Symbol	MIN	TYP	MAX	Unit
Communication Speed	-	8	15	25	Kbps
ART Wakeup Time	t_{AWU}	-	30	25	us
ART Preamble High Time	t_{ARTH}	500	264	160	us
ART Preamble Low Time	t_{ARTL}	500	264	160	us
Start Preamble High Time	t_{SPH}	500	264	160	us
Start Preamble Low Time	t_{SPL}	500	264	160	us
Sync bit time	t_{SYN}	125	66	40	us
Data bit time	t_{BIT}	125	66	40	us
Stop Preamble Time	t_{EP}	1000	528	320	us

8. Electrical Characteristic

8.1 Absolute Maximum Ratings

Table 8-1. Absolute Maximum Ratings

Parameter	Min	Max	Units
Supply Voltage (1)	2.7	6.0	V
Storage Temperature	-35	120	℃
ESD Susceptibility	2000		V
DC Current VCC and GND		3	mA

Note. Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or other conditions beyond those indicated in the operational sections of this specification is not implied.

Note (1) In case of low voltage operation type, have the range of 1.4 ~ 3.8V.

8.2 Recommended Operating Conditions

Table 8-2. Recommended Operation Conditions

Parameter	Min	Max	Units
Operating Temperature	-30	80	℃
Operating Voltage (1)	3.0	3.6	V

Note (1) In case of low voltage operation type, have the range of 1.6 ~ 2.2V.

8.3 DC Characteristics

Table 8-3. DC Specifications 3.3V I/O

Symbol	Parameter	Condition	Min	Typ	Max
V_{IL}	Input Low Voltage				0.8V
V_{IH}	Input High Voltage		2.0V		
I_I	Input Leakage Current	VCC = MIN V_{IN}=GND or 3.6V			1uA
V_{OL}	Output Low Voltage	I_{OL} = 2mA			0.4V
V_{OH}	Output High Voltage	I_{OH} = 2mA	2.4V		3.6V

Table 8-4. Supply Current

Symbol	Parameter	Condition	Min	Typ	Max
I_{VCC}	VCC Supply Current	Active 16MHz, VCC = 3.3V		200uA(1)	
		Sleep mode		55uA(2)	

Note (1) In case of 1.8V operation type, has under 130uA.

(2) In case of 1.8V operation type, has under 5uA.

8.4 Internal IP

Table 8-5. Internal Oscillator (Ta = 25°C)

Symbol	Parameter	Condition	Min	Typ	Max
fOSC	Switching Frequency		14MHz	16MHz	18MHz
Δf_{OSC}	Frequency Variation	-40≤Ta≤80°C	-		±10 %
Dmax	Duty Cycle		48%	50%	52%

Note (1) When the ring voltage is 3.3V (typical), CMOS voltage level and LVTTL voltage level are the same.

Table 8-6. Power-on-Reset

Symbol	Parameter	Condition	Min	Typ	Max
Vt	Threshold Voltage		1.1 V	1.2V	1.3V
t_{RINIT}	Register Initial time				160 us

Table 8-7. OTP cell

Symbol	Parameter	Condition	Min	Typ	Max
I_{VDD_R}	Read Current VDD				128uA (32bits)
I_{VDD_P}	Program Current VDD				<1uA
I_{VDD_SB}	Standby Current VDD				<1uA

Note. No active current at sleep mode thus I_{VDD_SB} is dependent on device leakage current.

Table 8-8. Regulator (1.8V for Logic, VCC=3.3V, Ta=25°)

Symbol	Parameter	Condition	Min	Typ	Max
VDD	Output Voltage	No load	1.7V	1.8V	1.9V
		0 < load < 3mA	1.6V	1.8V	2.0V
I_{max}	Peak Output Current			10mA	

9. Typical Operation Circuit

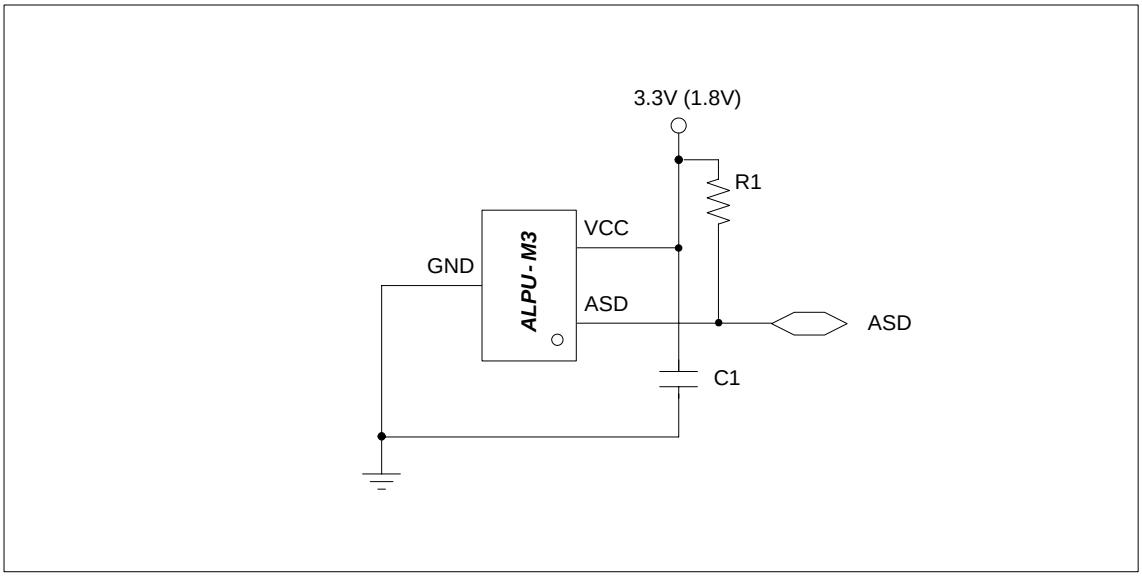


Figure 9-1. ALPU-M3 Operation Circuit

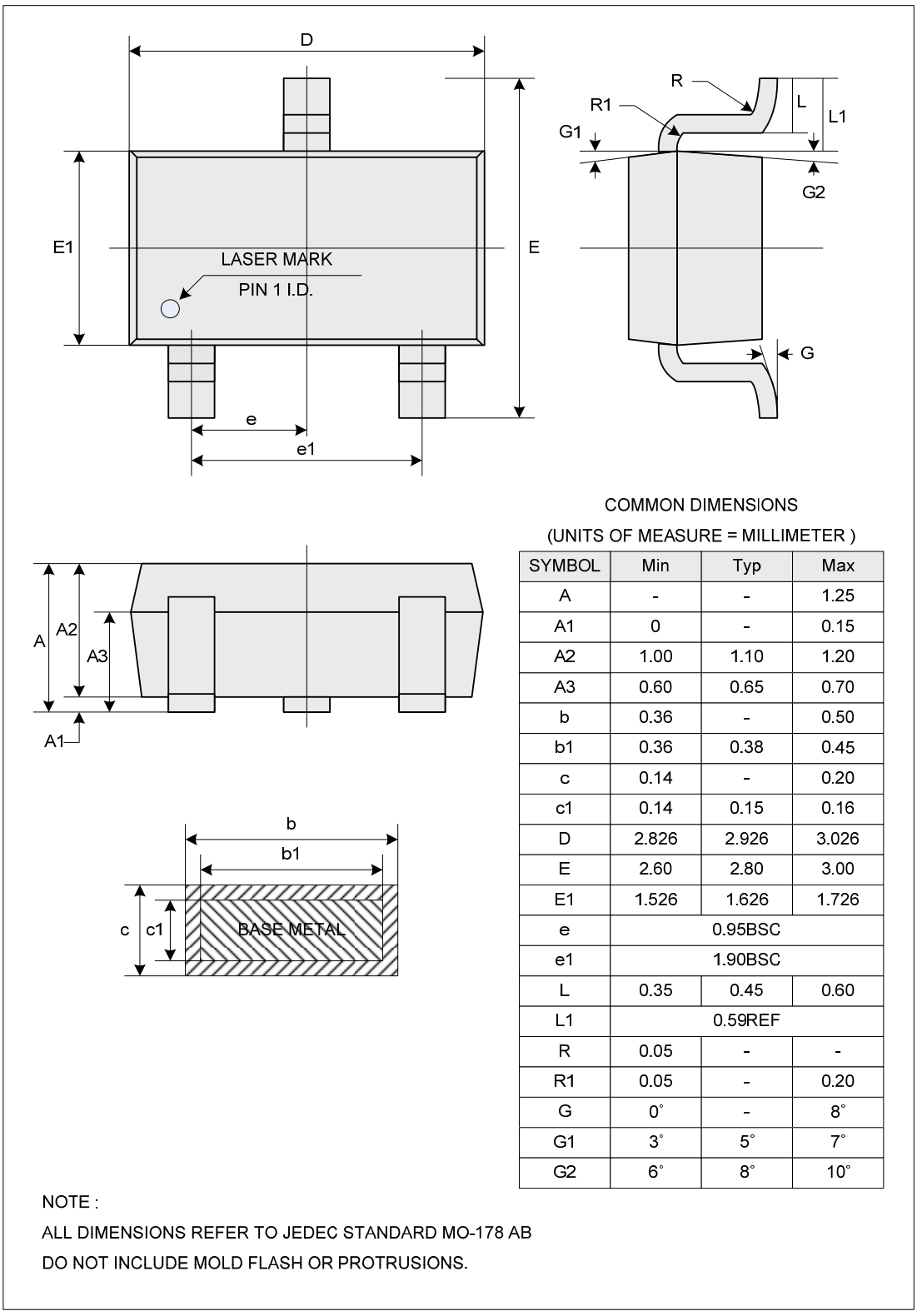
R1 : 2K ~ 10K ohm (Typ 4.7K ohm)

C1 : 0.1uF

Note (1) This can be changed to 1.8V Operation in case of low voltage type.

10. Package Information

10.1 POD - 3L-SOT23



COMMON DIMENSIONS

(UNITS OF MEASURE = MILLIMETER)

SYMBOL	Min	Typ	Max
A	-	-	1.25
A1	0	-	0.15
A2	1.00	1.10	1.20
A3	0.60	0.65	0.70
b	0.36	-	0.50
b1	0.36	0.38	0.45
c	0.14	-	0.20
c1	0.14	0.15	0.16
D	2.826	2.926	3.026
E	2.60	2.80	3.00
E1	1.526	1.626	1.726
e	0.95BSC		
e1	1.90BSC		
L	0.35	0.45	0.60
L1	0.59REF		
R	0.05	-	-
R1	0.05	-	0.20
G	0°	-	8°
G1	3°	5°	7°
G2	6°	8°	10°

NOTE :

ALL DIMENSIONS REFER TO JEDEC STANDARD MO-178 AB

DO NOT INCLUDE MOLD FLASH OR PROTRUSIONS.

Figure 12-1. 3L-SOT23 Package Outline Dimension

11. Datasheet Revision History

11.1 Ver 1.0 (2011/03/07)

- Initial version release.

11.2 Ver 1.01 (2011/03/08)

- Added ART Wakeup condition in chapter 8.
- Corrected typographical errors.

11.3 Ver 1.02 (2012/06/01)

- Change Figure 2-2

Neowine Co., Ltd

http://www.neowine.com

Headquarters

3FL GreenPlaza. 131-8 Imae-Dong, Bundang-Gu, Seongnam-City, Gyeonggi-Do, Korea 463-806

Tel: 82-31-706-8484 Fax: 82-31-706-8485

info@neowine.com

China Office (Shanghai)

A-2111 Oriental International Plaza, 85 LouShanGuan Rd, Changning District, Shanhai China 200336

Tel: 86-21-6278-2288(ext 221) Fax: 86-21-6278-3723

alpu-china@neowine.com