



# SecurityCore Family

*Confidential*

**SD-SecurityCore-V2.0**

## Spec. Draft of SecurityCore

### System Copy Protection

V2.0

2011. 1

- ◆ CORERIVER Semiconductor reserves the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time.
- ◆ CORERIVER shall give customers at least a three month advance notice of intended discontinuation of a product or a service through its homepage.
- ◆ Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete.
- ◆ The CORERIVER products listed in this document are intended for usage in general electronics applications. These CORERIVER products are neither intended nor warranted for usage in equipment that requires extraordinarily high quality and/or reliability or a malfunction or failure of which may cause loss of human life or bodily injury.

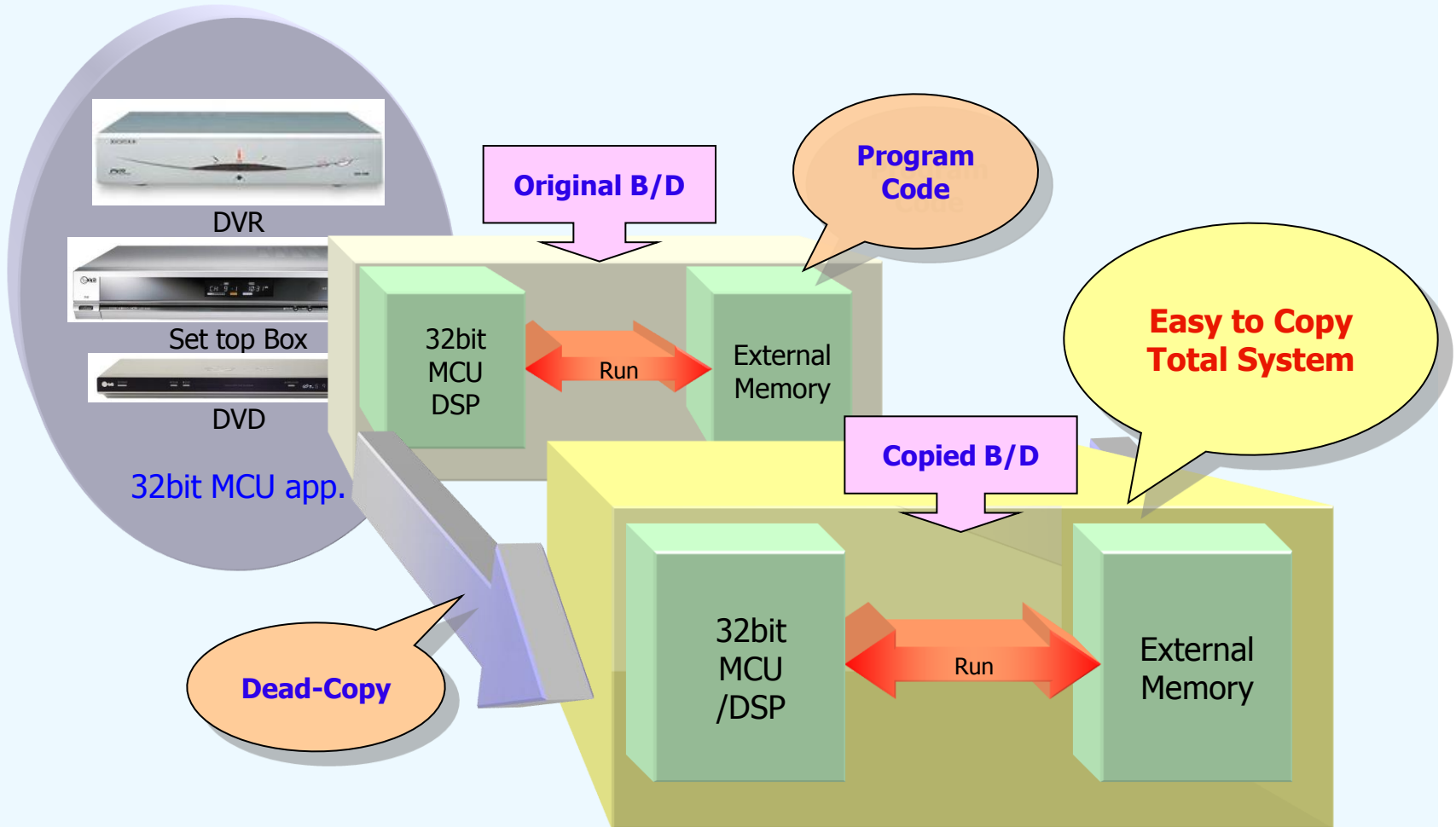
# Contents

1. What's Copy Protection?
  - ✓ Case 1 : without SecurityCore
  - ✓ Case 2 : with SecurityCore
2. Production Overview
3. Features
4. Block Diagram
5. Pin Configurations
  - ✓ SecurityCore1.0 / SecurityCore2.0
  - ✓ SecurityCore3.0
  - ✓ SecurityCore4.0 / SecurityCore4.1 / SecurityCore412
6. Pin Descriptions
7. Application Circuit
8. Strong Point of CORERIVER SECURITYCORE
9. Flow Chart
10. Single Wire Interface
11. I2C Interface
12. I2C Speed
13. How to Support Library
14. Absolute Maximum Ratings
15. Power Characteristics
16. DC Characteristics
17. AC Characteristics
18. Package Dimensions
19. Algorithm flow chart

# 1. What's Copy Protection?

*Confidential*

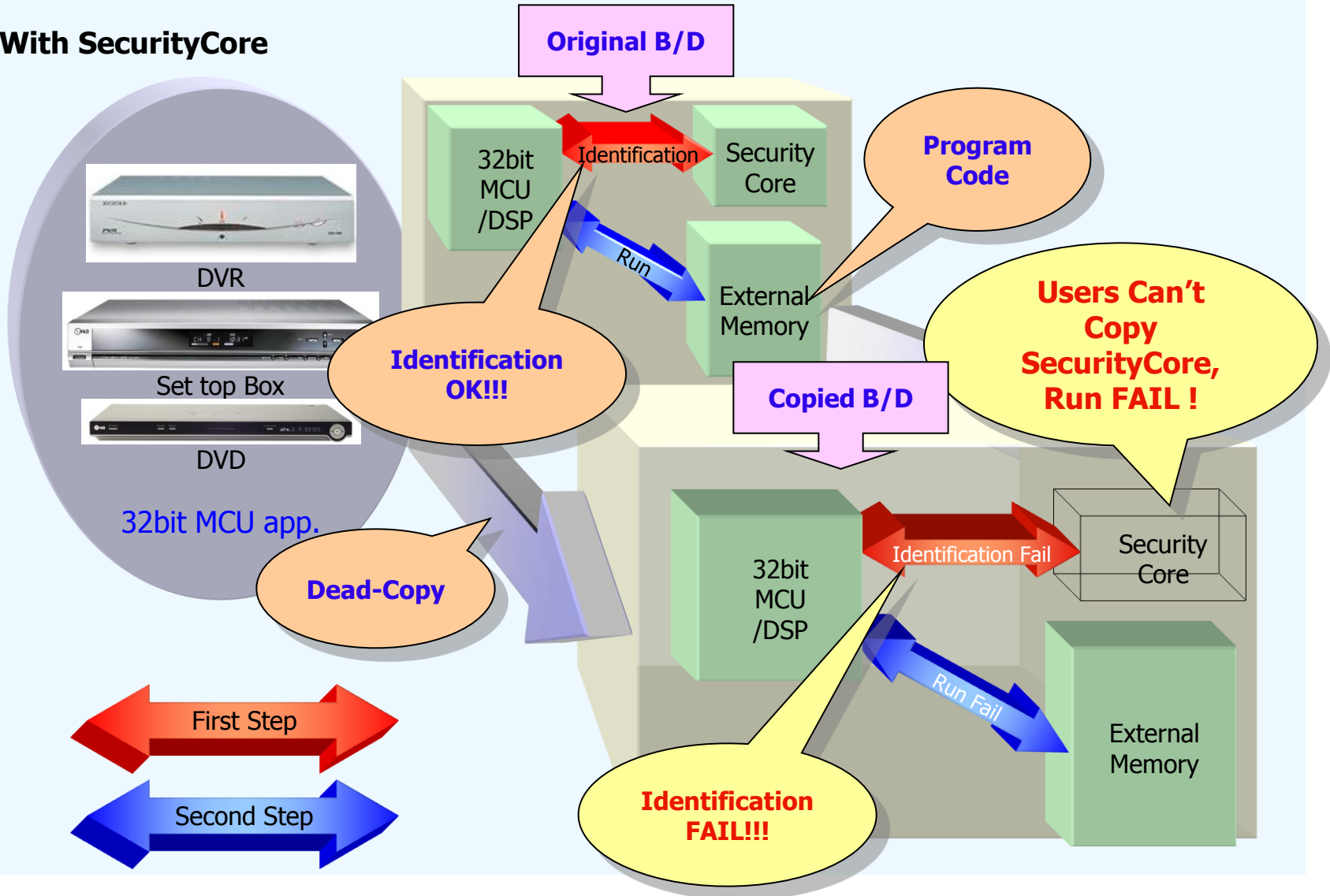
## ◆ Without SecurityCore



# 1. What's Copy Protection? (Cont'd)

*Confidential*

## ◆ With SecurityCore



## 2. Product Overview

- ◆ The solution of System Copy Protection.
- ◆ Support a unique identification number
- ◆ Inventory Tracking
- ◆ Customizing Unique Algorithm

## 3. Features

### ◆ Security

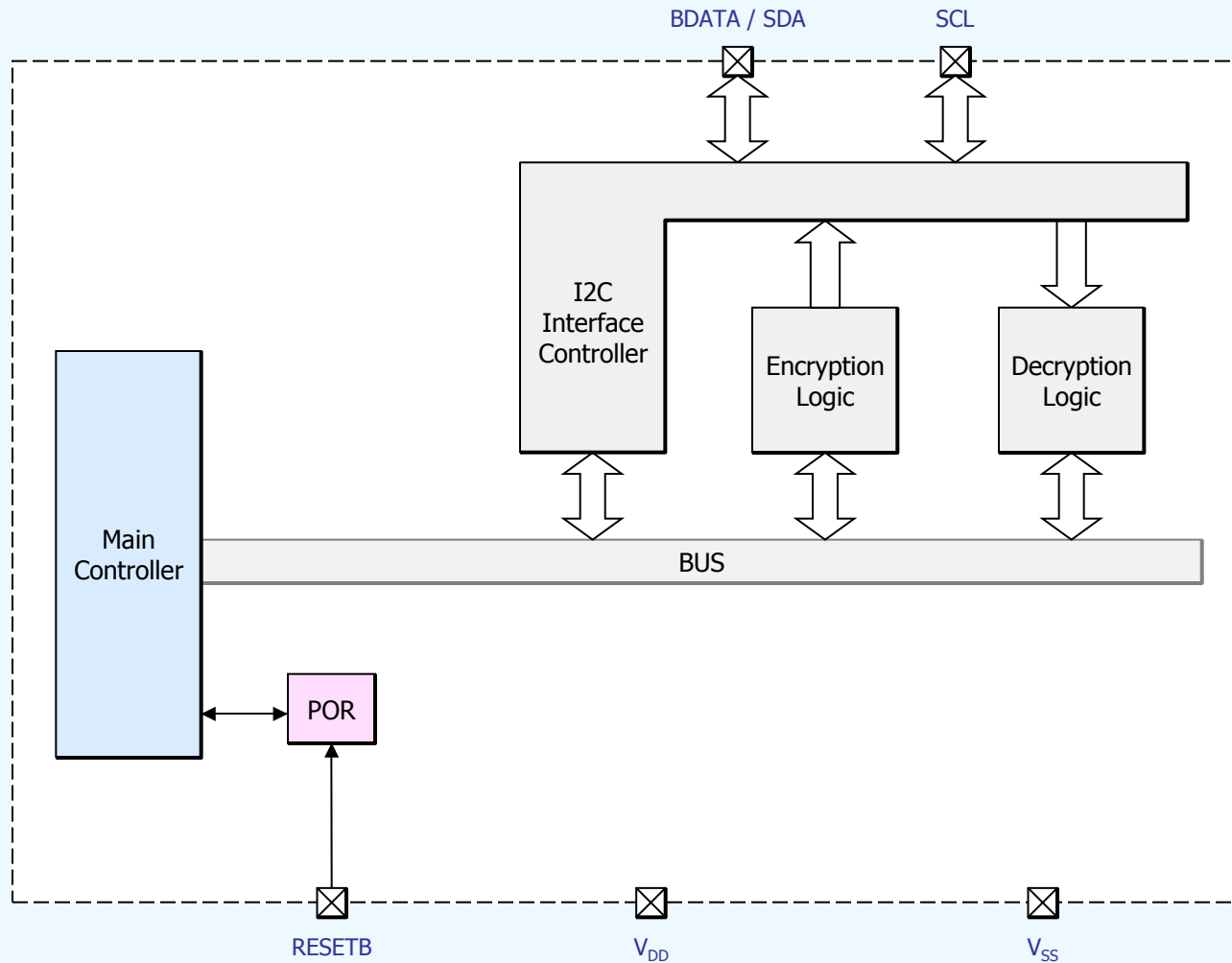
- ✓ Support Random Number Generation
- ✓ Encoder Read Protect
- ✓ Unique Algorithm : 32 bit Encryption
- ✓ Provide Unique SEED Key

### ◆ Operation

- ✓ 2.4 ~ 5.5 Volts Operation
- ✓ -20 °C to 85 °C operating temperature
- ✓ Active current : Max. 10mA @5V
- ✓ Stop current : Max. 1uA
- ✓ Program Interface : One-Wire Interface
- ✓ E.S.D. protection up to 2,000V
- ✓ Package : 8-SPDIP and 8-SOIC

# 4. Block Diagram

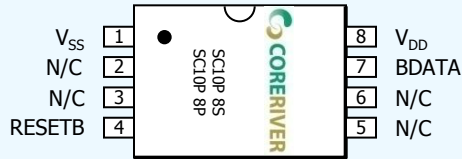
*Confidential*



# 5. Pin Configurations (1/3)

## ◆ SecurityCore1.0

### ✓ One-Wire interface



[ 8-SOIC / 8-SPDIP ]

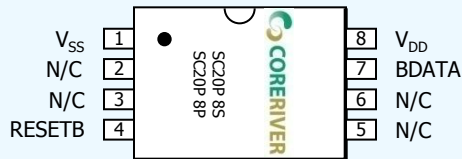
### ✓ I2C interface



[ 8-SOIC / 8-SPDIP ]

## ◆ SecurityCore2.0

### ✓ One-Wire interface



[ 8-SOIC / 8-SPDIP ]

### ✓ I2C interface



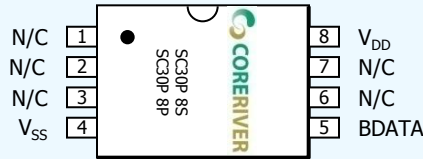
[ 8-SOIC / 8-SPDIP ]

# 5. Pin Configurations (2/3)

*Confidential*

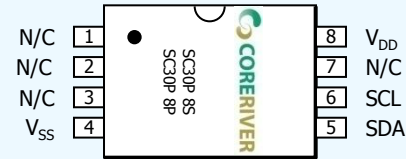
## ◆ SecurityCore3.0

✓ One-Wire interface



[ 8-SOIC / 8-SPDIP ]

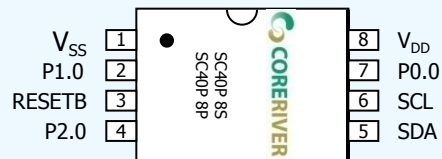
✓ I2C interface



[ 8-SOIC / 8-SPDIP ]

## ◆ SecurityCore4.0

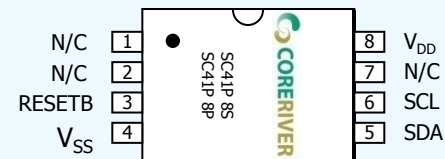
✓ I2C interface



[ 8-SOIC ]

## ◆ SecurityCore4.1

✓ I2C interface

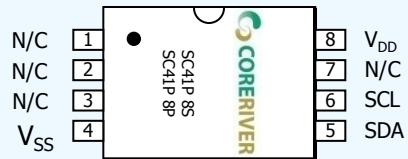


[ 8-SOIC ]

## 5. Pin Configurations (3/3)

### ◆ SecurityCore412

✓ I2C interface



[ 8-SOIC ]

## 6. Pin Descriptions (1/3)

### ◆ SecurityCore1.0

Symbol	Direction	Description	Share Pins
$V_{DD}$	Input	Voltage Power Source	-
$V_{SS}$	Input	Voltage Power Ground	-
RESETB / VPP	Input/Output	<ul style="list-style-type: none"> <li>▪ External Reset Input Signal (Default)</li> <li>▪ Bit Programmable</li> </ul>	VPP (11.5V)
BDATA / SDA	Input/Output	<ul style="list-style-type: none"> <li>▪ Data I/O</li> </ul>	-
SCL	Input/Output	<ul style="list-style-type: none"> <li>▪ Clock I/O</li> </ul>	-
OTHERS		<ul style="list-style-type: none"> <li>▪ N/C</li> </ul>	-

### ◆ SecurityCore2.0

Symbol	Direction	Description	Share Pins
$V_{DD}$	Input	Voltage Power Source	-
$V_{SS}$	Input	Voltage Power Ground	-
RESETB	Input/Output	<ul style="list-style-type: none"> <li>▪ External Reset Input Signal (Default)</li> <li>▪ Bit Programmable</li> </ul>	-
BDATA / SDA	Input/Output	<ul style="list-style-type: none"> <li>▪ Data I/O</li> </ul>	-
SCL	Input/Output	<ul style="list-style-type: none"> <li>▪ Data I/O</li> </ul>	-
OTHERS		<ul style="list-style-type: none"> <li>▪ N/C</li> </ul>	-

## 6. Pin Descriptions (2/3)

### ◆ SecurityCore3.0

Symbol	Direction	Description	Share Pins
$V_{DD}$	Input	Voltage Power Source	-
$V_{SS}$	Input	Voltage Power Ground	-
BDATA / SDA	Input/Output	▪ Data I/O	-
SCL	Input/Output	▪ Clock I/O	-
OTHERS		▪ N/C	-

### ◆ SecurityCore4.0

Symbol	Direction	Description	Share Pins
$V_{DD}$	Input	Voltage Power Source	-
$V_{SS}$	Input	Voltage Power Ground	-
BDATA / SDA	Input/Output	▪ Data I/O	-
SCL	Input/Output	▪ Clock I/O	-
RESETB	Input/Output	▪ External Reset Input Signal (Default) ▪ Bit Programmable	-
OTHERS		▪ Data I/O	-

## 6. Pin Descriptions (3/3)

### ◆ SecurityCore4.1

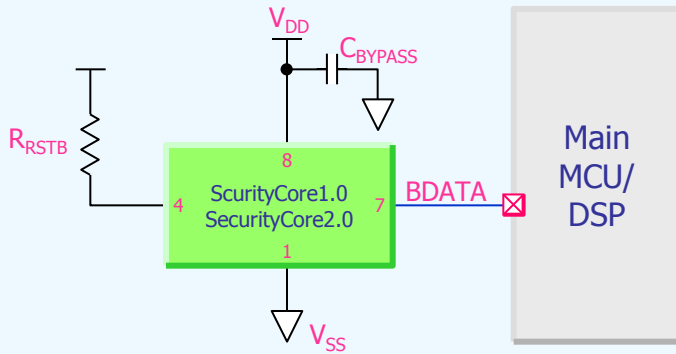
Symbol	Direction	Description	Share Pins
$V_{DD}$	Input	Voltage Power Source	-
$V_{SS}$	Input	Voltage Power Ground	-
SDA	Input/Output	▪ Data I/O	-
SCL	Input/Output	▪ Clock I/O	-
RESETB	Input/Output	▪ External Reset Input Signal (Default) ▪ Bit Programmable	-
OTHERS		▪ Data I/O	-

### ◆ SecurityCore412

Symbol	Direction	Description	Share Pins
$V_{DD}$	Input	Voltage Power Source	-
$V_{SS}$	Input	Voltage Power Ground	-
SDA	Input/Output	▪ Data I/O	-
SCL	Input/Output	▪ Clock I/O	-
OTHERS		▪ Data I/O	-

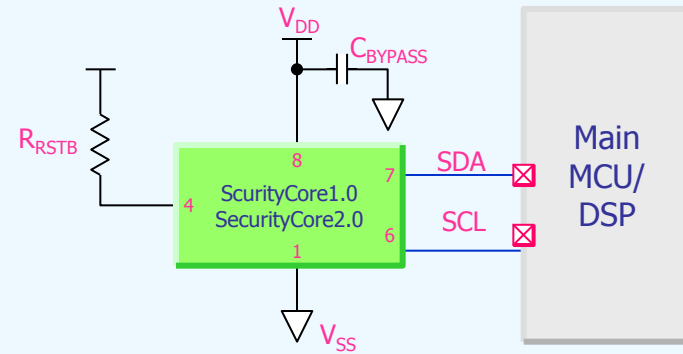
# 7. Application Circuit

## ◆ One-Wire Interface

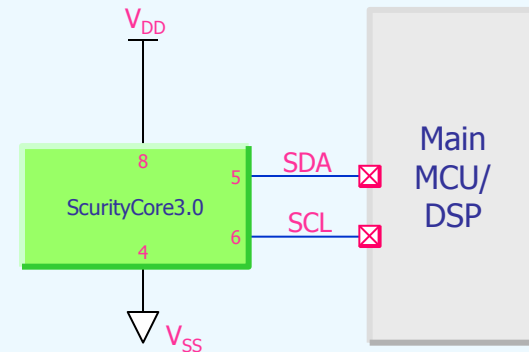
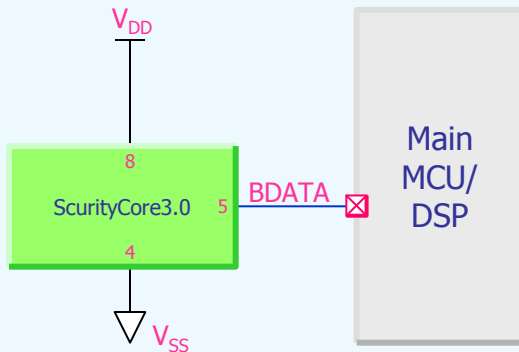


- $C_{BYPASS} = 1\mu F$  (Bypass Capacitor)
- $R_{RSTB} = 4.7k\Omega$  (Pull-up Resistor for RSTB Pin)

## ◆ I2C Interface

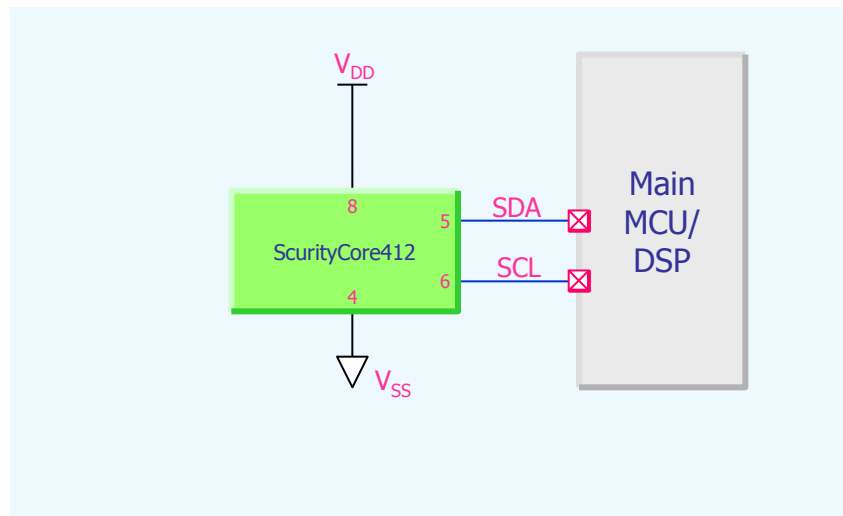
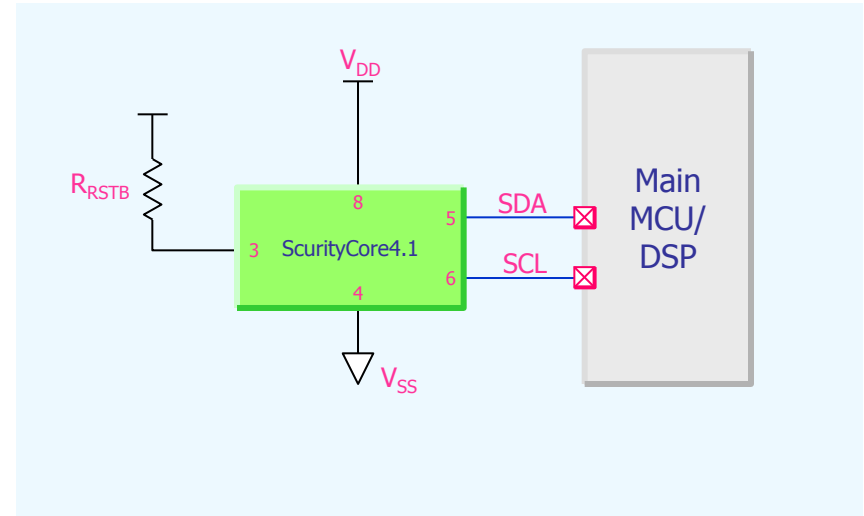
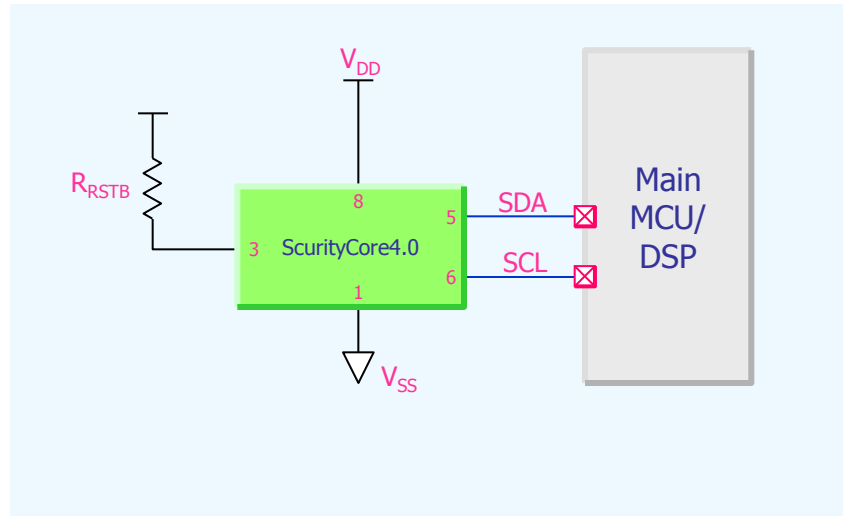


- $C_{BYPASS} = 1\mu F$  (Bypass Capacitor)
- $R_{RSTB} = 4.7k\Omega$  (Pull-up Resistor for RSTB Pin)



# 7. Application Circuit

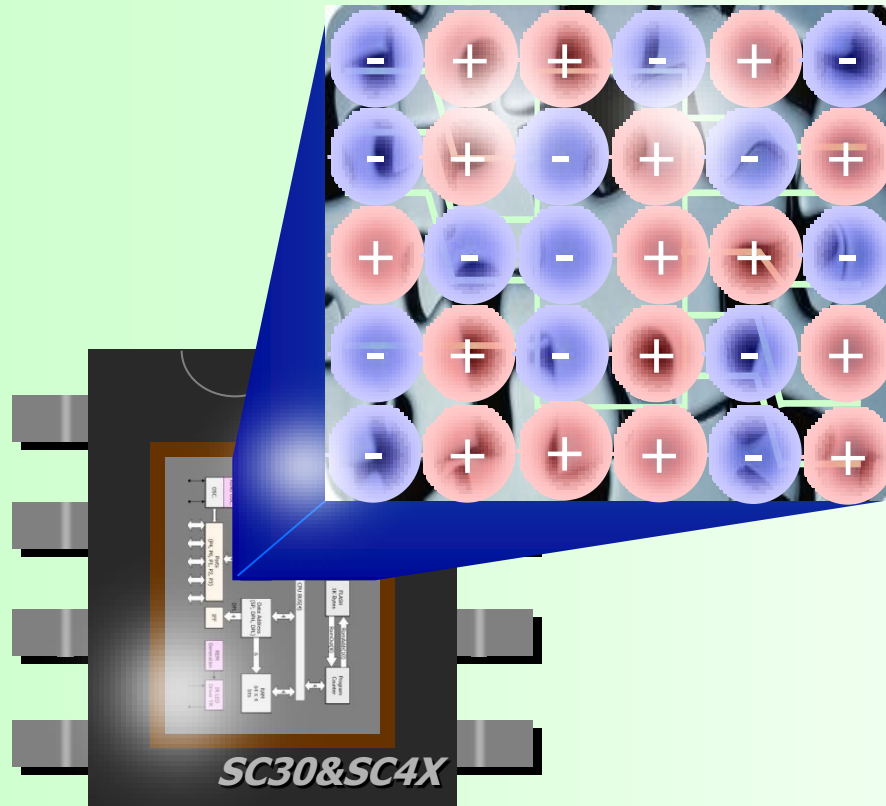
## ◆ I2C Interface



## 8. Strong Point of CORERIVER SC30&SC4X (1/2)

*Confidential*

- ◆ SC30&SC4X stores a security algorithm as extremely small electric charges.

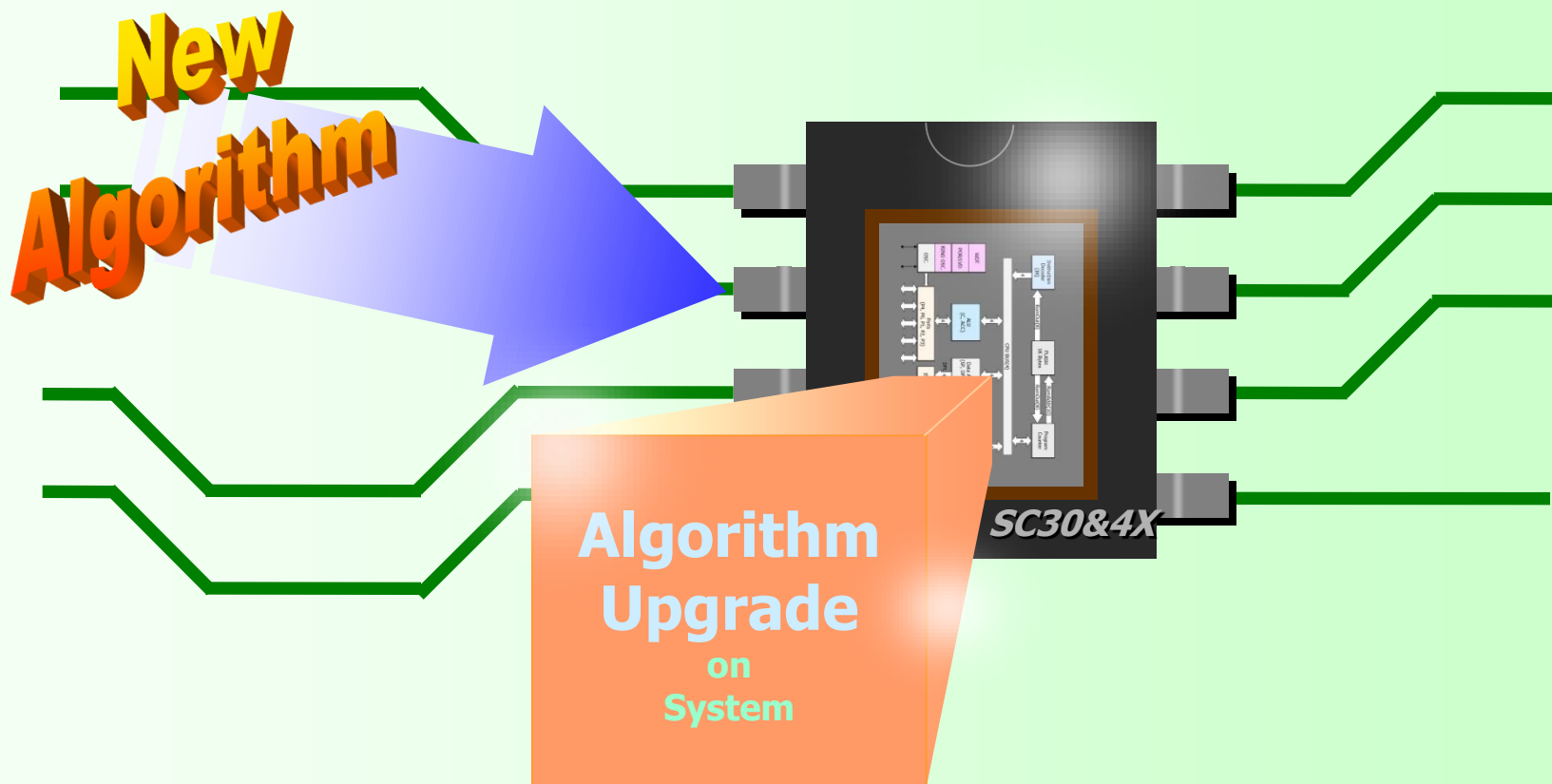


- ✓ The security algorithm is not hard-wired.
- ✓ It is really impossible to find it by de-cap.

## 8. Strong Point of CORERIVER SC30&SC4X (2/2)

*Confidential*

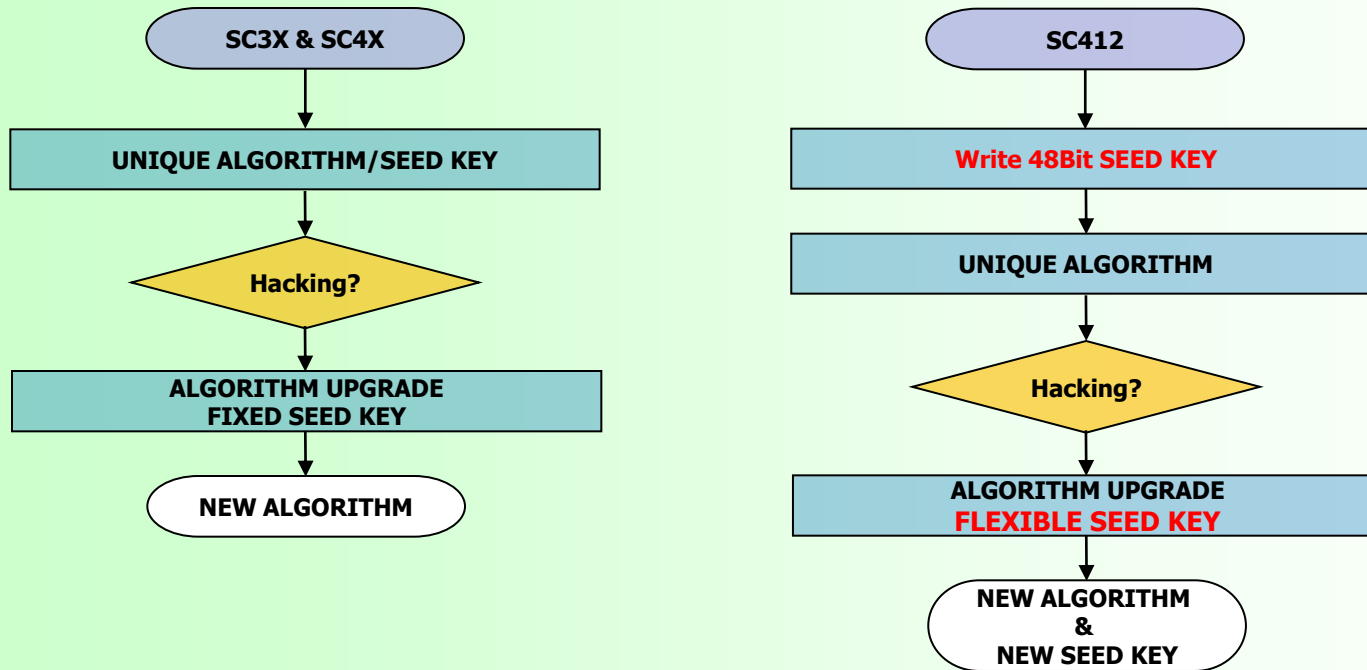
### ◆ Upgrade function in the field.



- ✓ CORERIVER SC30&SC4X can upgrade the security algorithm on a used system.
- ✓ To prevent the security algorithm from being cracked, you can replace it by a new one.

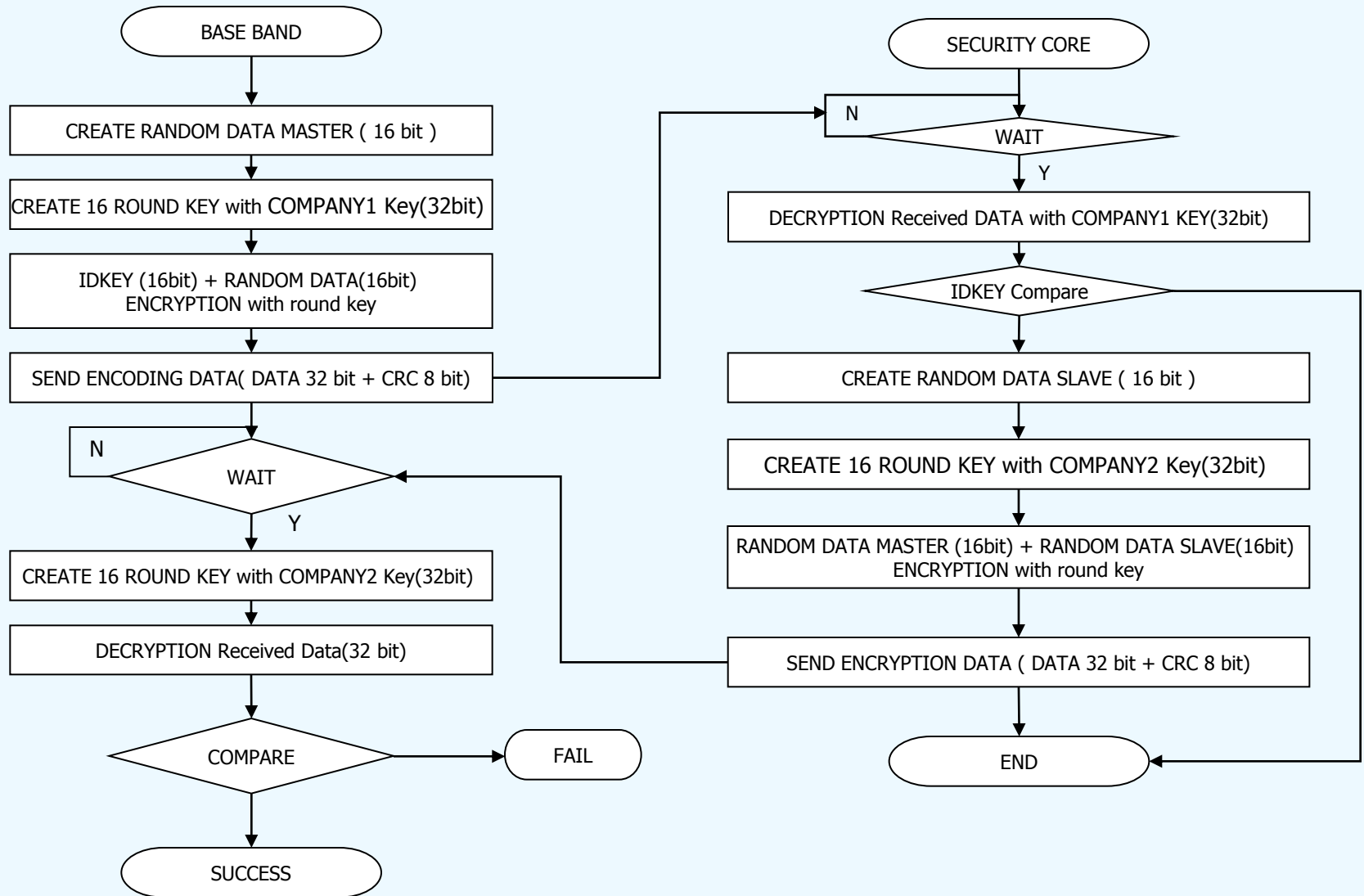
## 8. Strong Point of CORERIVER SC412(1/1)

*Confidential*

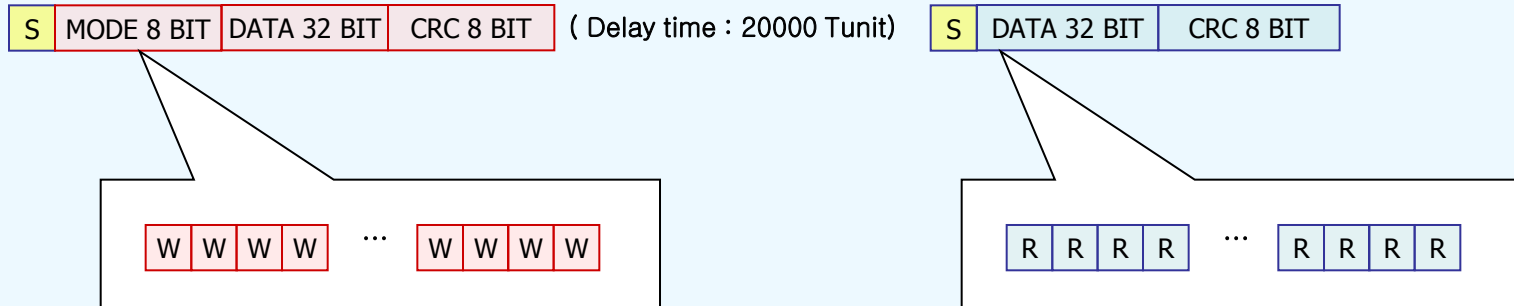


- ✓ CORERIVER SC412 can write the security SEED key on a used system.

# 8. Flow Chart



# 9. Single Wire Interface : Data Sequence (1)

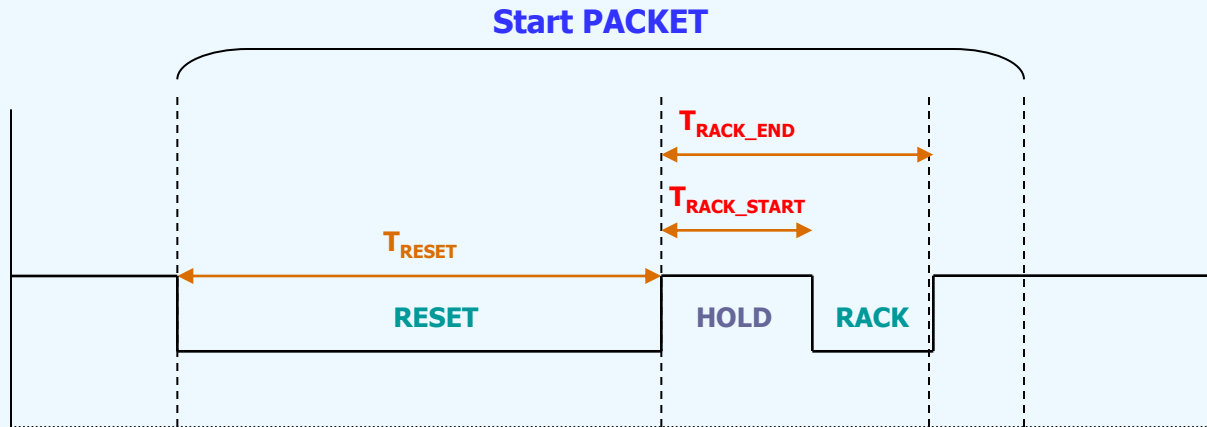


**IF (MODE == 0) then BYPASS MODE, BYPASS MODE will make Base Band testing easy.**

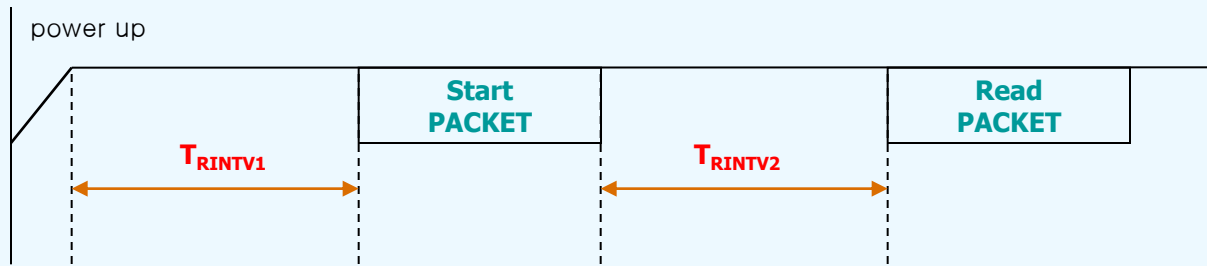
- |   |                        |  |                                       |
|---|------------------------|--|---------------------------------------|
| <span style="border: 1px solid black; background-color: yellow; padding: 2px;">S</span> | WAKE UP & START PACKET | <span style="background-color: yellow; border: 1px solid black; width: 20px; height: 15px; display: inline-block;"></span> | base band → security core → base band |
| <span style="border: 1px solid red; padding: 2px;">W</span>                             | WRITE 1 BIT PACKET     | <span style="background-color: #f8d7da; border: 1px solid red; width: 20px; height: 15px; display: inline-block;"></span>  | base band → security core             |
| <span style="border: 1px solid blue; padding: 2px;">R</span>                            | READ 1 BIT PACKET      | <span style="background-color: #d1ecf1; border: 1px solid blue; width: 20px; height: 15px; display: inline-block;"></span> | security core → base band             |

# 9. Single Wire Interface (2/4)

◆ Start Timing Diagram



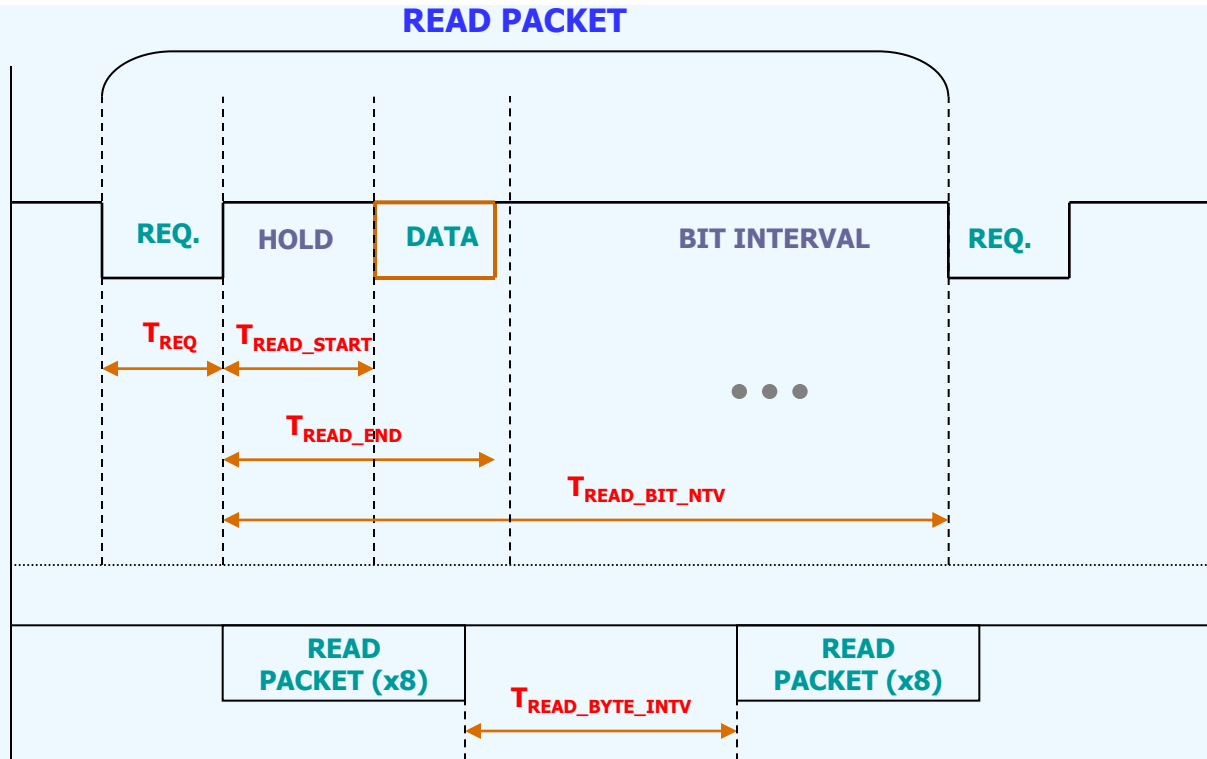
$T_{RESET}$  : 100us@3.3V, 80us@5V  
 $T_{RACK\_START}$  : 100us@3.3V, 80us@5V  
 $T_{RACK\_END}$  : 200us@3.3V, 160us@5V



$T_{RINTV1}$  :  $1200T_{UNIT} \leq T_{RINTV1}$        $T_{RINTV2}$  :  $20T_{UNIT} \leq T_{RINTV2}$

# 9. Single Wire Interface (3/4)

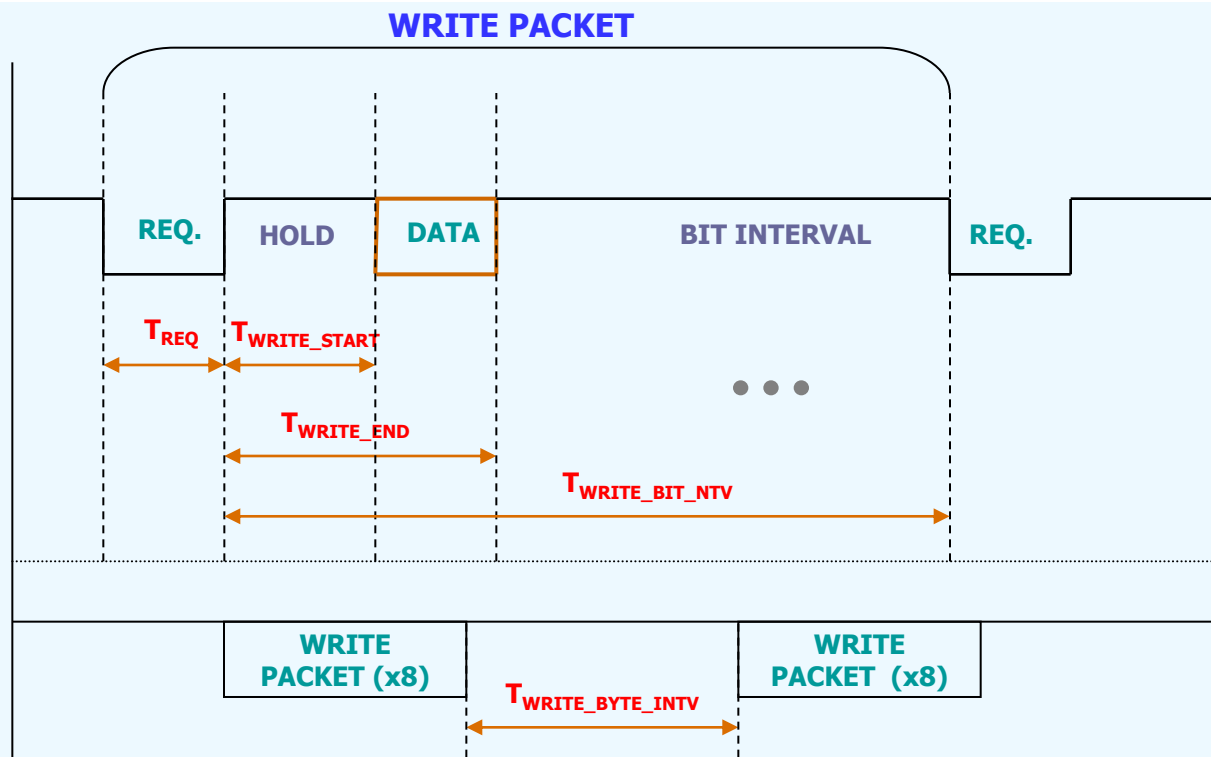
◆ READ Timing Diagram



- $T_{REQ}$  : 100us@3.3V, 80us@5V
- $T_{READ\_START}$  : 100us@3.3V, 80us@5V
- $T_{READ\_END}$  : 100us@3.3V, 160us@5V
- $T_{READ\_BIT\_INTV}$  : 300us@3.3V, 240us@5V
- $T_{READ\_BYTE\_INTV}$  : 100us@3.3V, 80us@5V

# 9. Single Wire Interface (4/4)

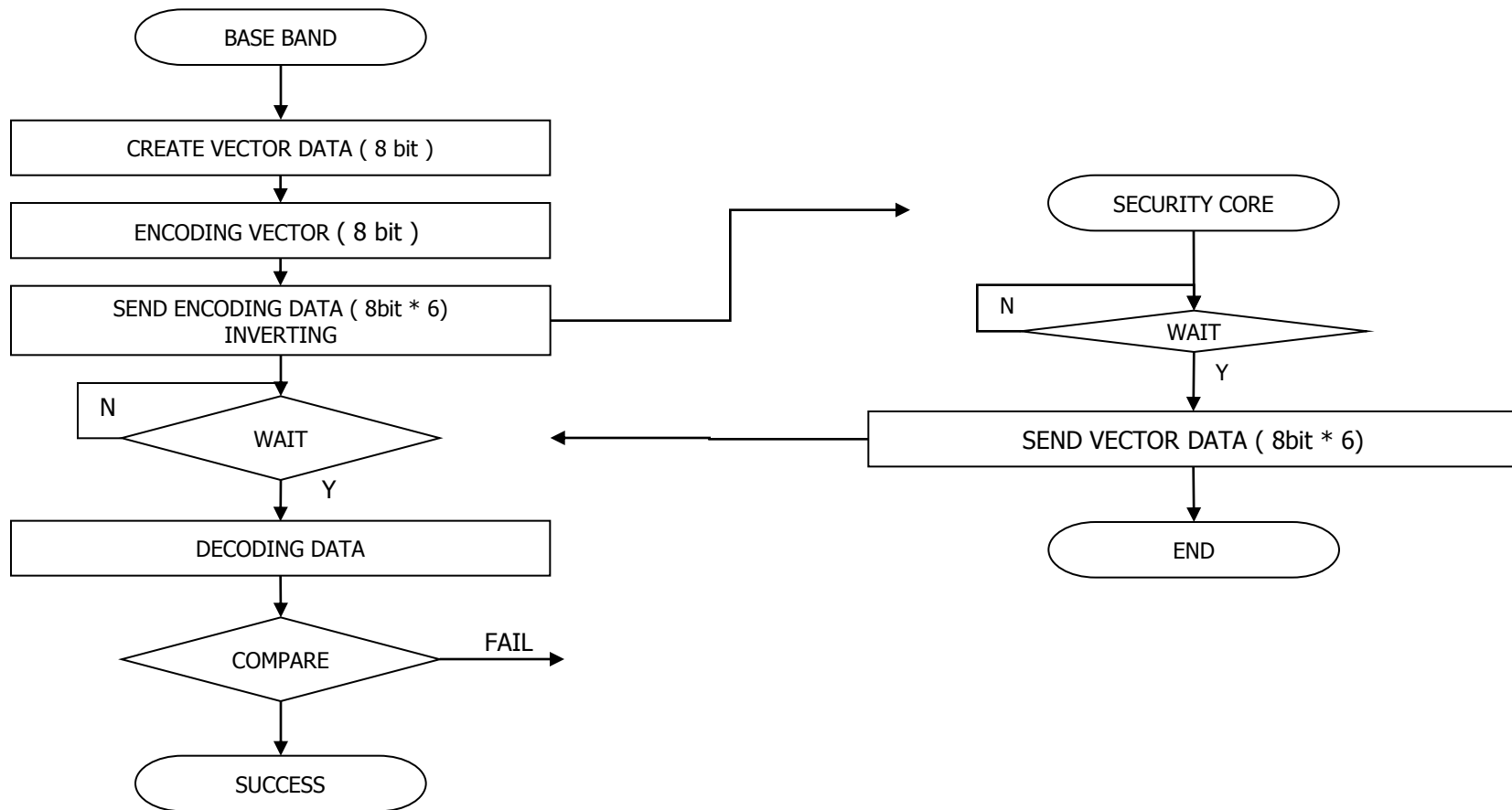
◆ WRITE Timing Diagram



- $T_{REQ}$**  : 100us@3.3V, 80us @5V
- $T_{WRITE\_START}$**  : 100us@3.3V, 80us @5V
- $T_{WRITE\_END}$**  : 200us@3.3V, 160us @5V
- $T_{WRITE\_BIT\_INTV}$**  : 100us@3.3V, 80us @5V
- $T_{WRITE\_BYTE\_INTV}$**  : 100us@3.3V, 80us @5V

# 10. I2C Interface : Bypass (1/7)

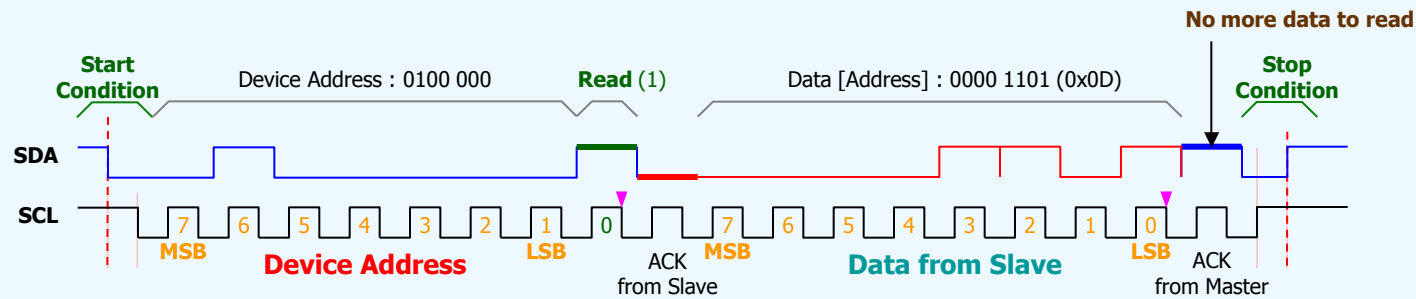
Confidential



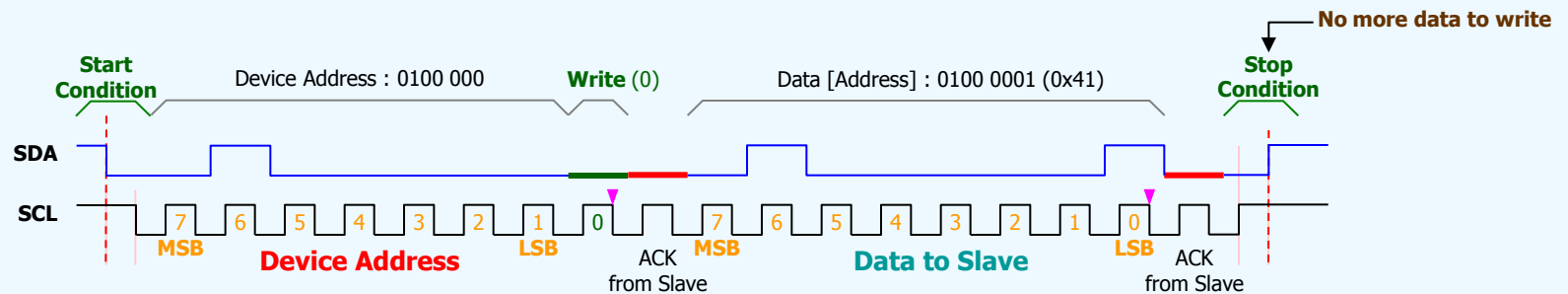
# 10. I2C Interface : Byte Read/Write (2/7)

*Confidential*

- ◆ 1 Byte Read Timing : Device Address default [0x20], Clock Frequency ( < 10 KHz)



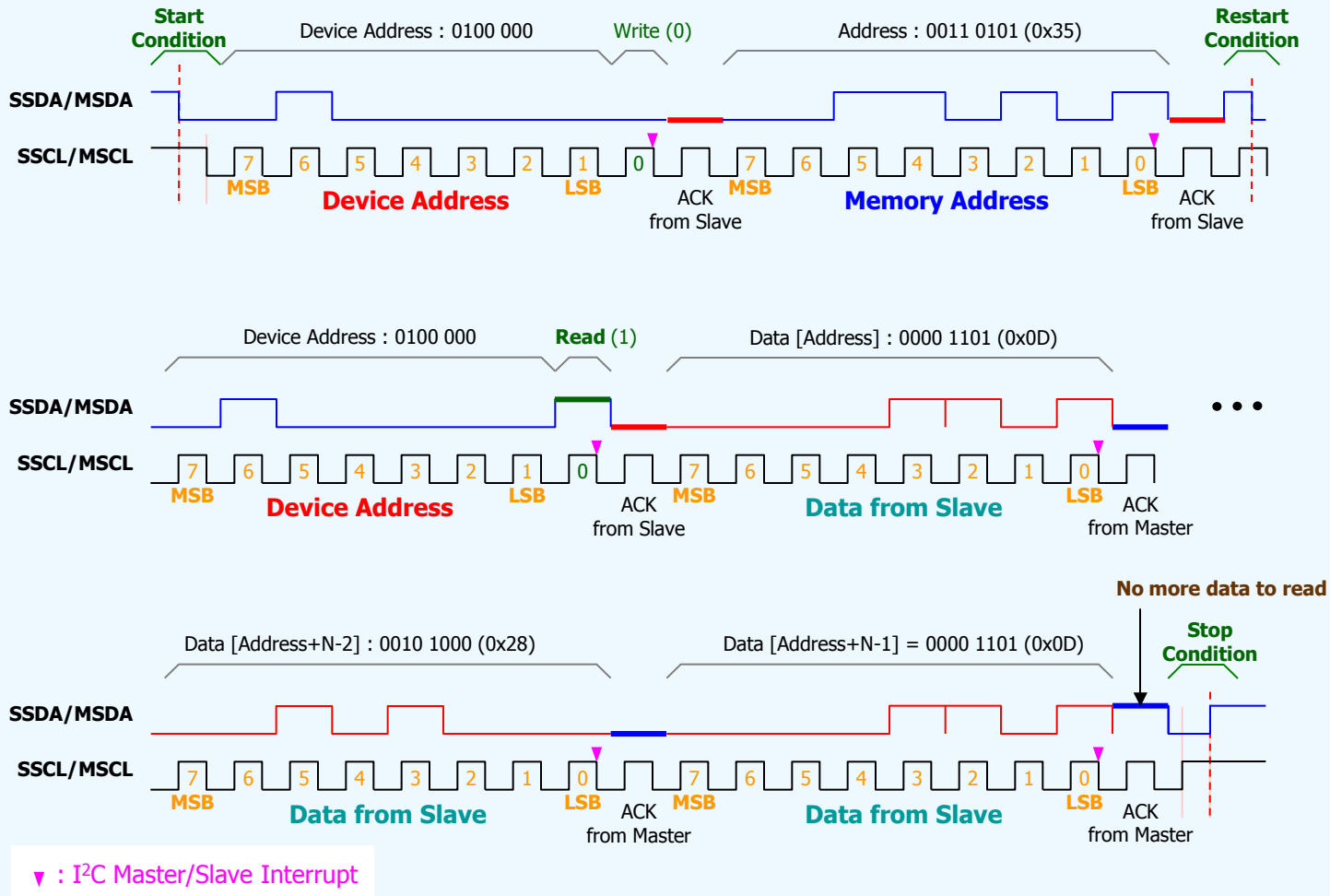
- ◆ 1 Byte Write Timing : Device Address default [0x20], Clock Frequency ( < 10 KHz)



# 10. I2C Interface : Slave & Master Timing (3/7)

Confidential

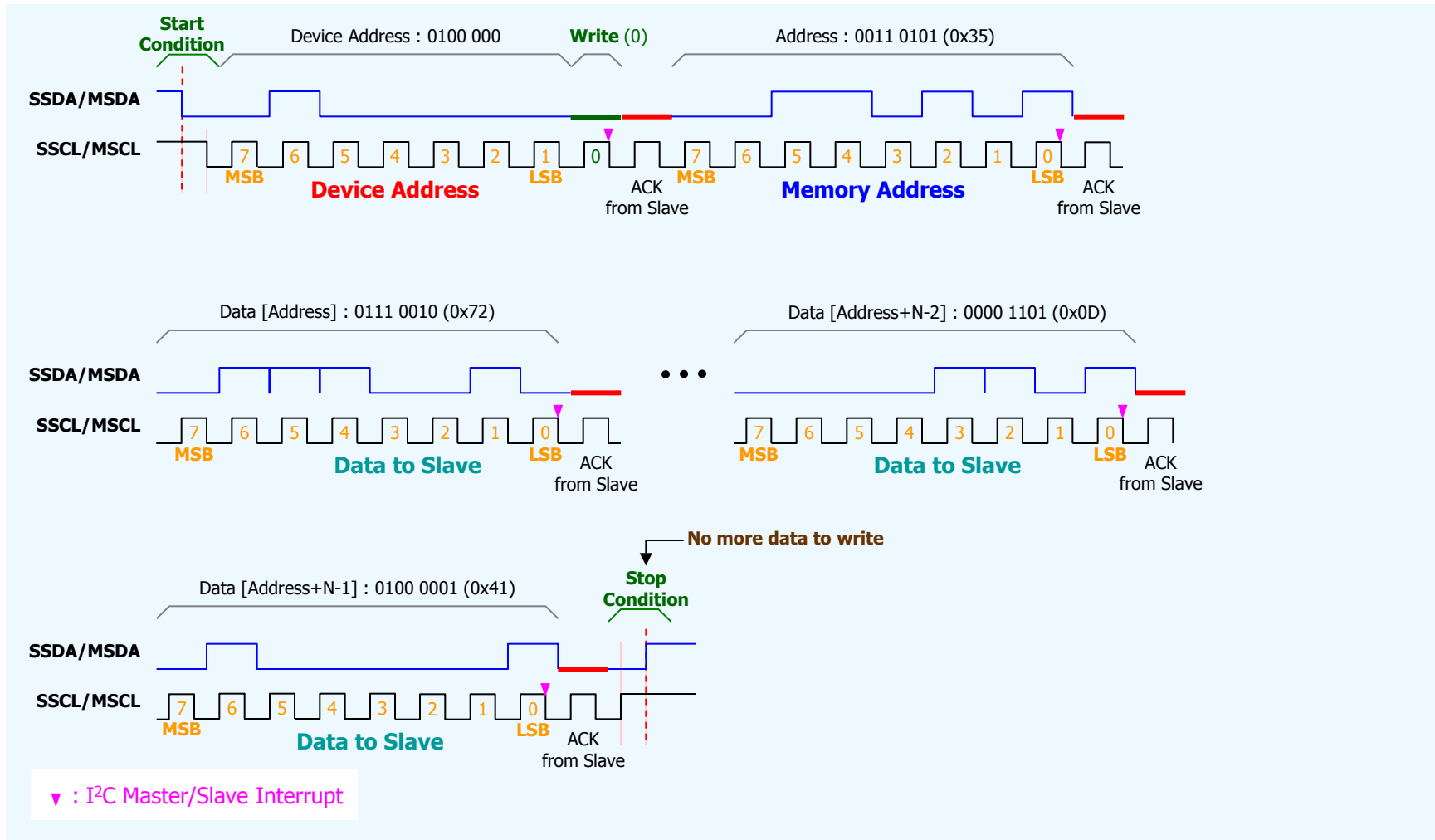
## ◆ Multi (N) Bytes Read Timing with Memory Address



# 10. I2C Interface : Slave & Master Timing (4/7)

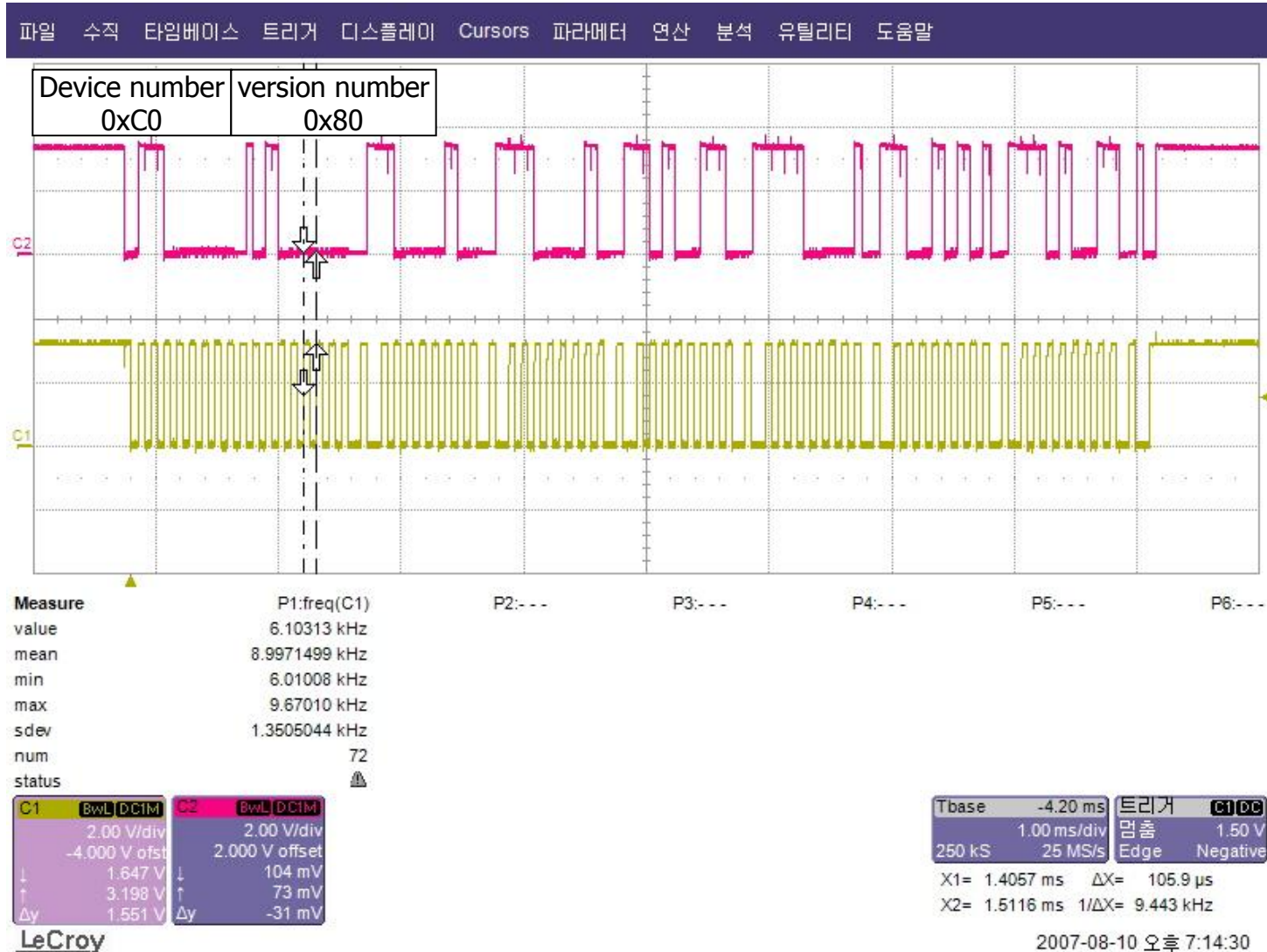
Confidential

## ◆ Multi (N) Bytes Write Timing with Memory Address



# 10. I2C Interface : Test signal - bypass (5/7)

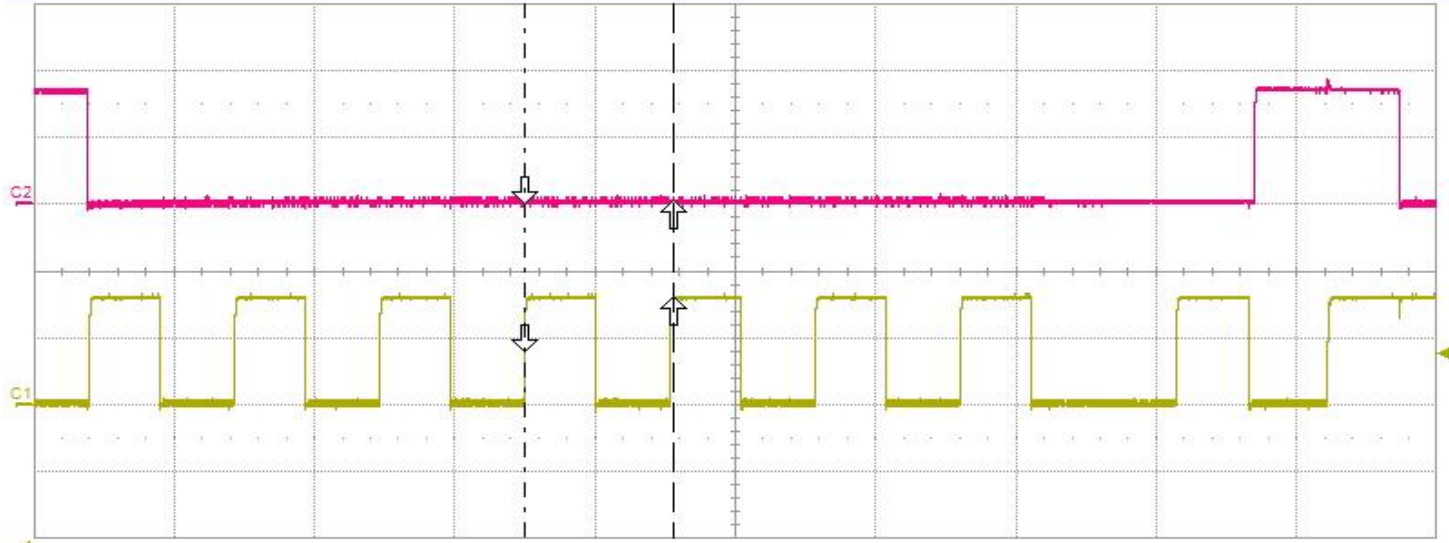
Confidential



# 10. I2C Interface : Test signal - delay (6/7)

Confidential

파일 수직 타임베이스 트리거 디스플레이 Cursors 파라미터 연산 분석 유틸리티 도움말



Measure	P1:freq(C1)	P2:---	P3:---	P4:---	P5:---	P6:---
value	9.24631 kHz					
mean	9.2174266 kHz					
min	6.49008 kHz					
max	9.66816 kHz					
sdev	1.0400040 kHz					
num	8					
status						

C1	BwL DClM	C2	BwL DClM
2.00 V/div		2.00 V/div	
-4.000 V ofst		2.000 V offset	
↓ 1.625 V		↓ 62 mV	
↑ 3.188 V		↑ 63 mV	
Δy 1.562 V		Δy 0 mV	

Tbase	-1.556 ms	트리거	C1 DC
	100 μs/div	멈춤	1.50 V
250 kS	250 MS/s	Edge	Negative
X1=	1.40568 ms	ΔX=	105.96 μs
X2=	1.51164 ms	1/Δf=	9.438 kHz

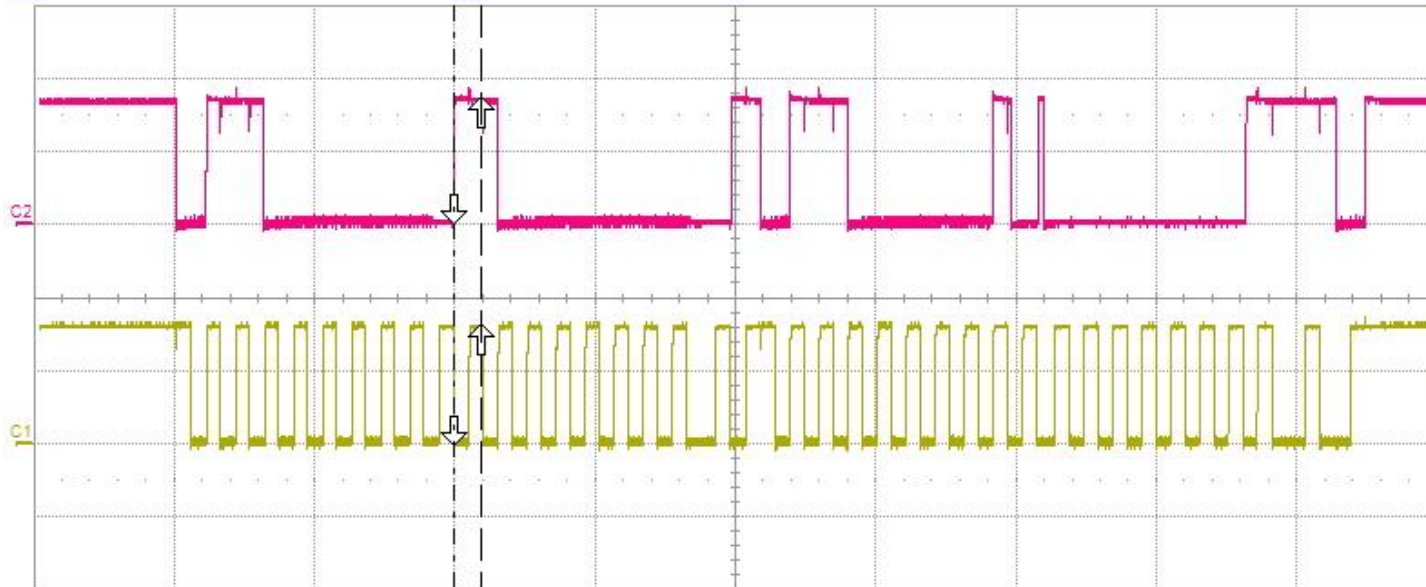
2007-08-10 오후 7:12:52

•SC30 의 경우 10 KHz 이하로 setting 하셔서 test 하시기 바랍니다.

# 10. I2C Interface : Test signal– Get\_version (7/7)

*Confidential*

파일 수직 타임베이스 트리거 디스플레이 Cursors 파라미터 연산 분석 유틸리티 도움말



Measure	P1:freq(C1)	P2:---	P3:---	P4:---	P5:---	P6:---
value	6.13022 kHz					
mean	9.2487896 kHz					
min	5.90756 kHz					
max	9.66813 kHz					
sdev	1.0692879 kHz					
num	37					
status						

C1	BwL	DCIM	C2	BwL	DCIM
2.00 V/div			2.00 V/div		
-4.000 V ofst			2.000 V offset		
↓ 0 mV			↓ 63 mV		
↑ 3.250 V			↑ 3.437 V		
Δy 3.250 V			Δy 3.375 V		

Tbase	-1.94 ms	트리거	C1 DC
	500 μs/div	멈춤	1.50 V
250 kS	50 MS/s	Edge	Negative
X1=	937.62 μs	ΔX=	97.50 μs
X2=	1.03512 ms	1/ΔX=	10.256 kHz

LeCroy

2007-08-10 오후 7:11:16

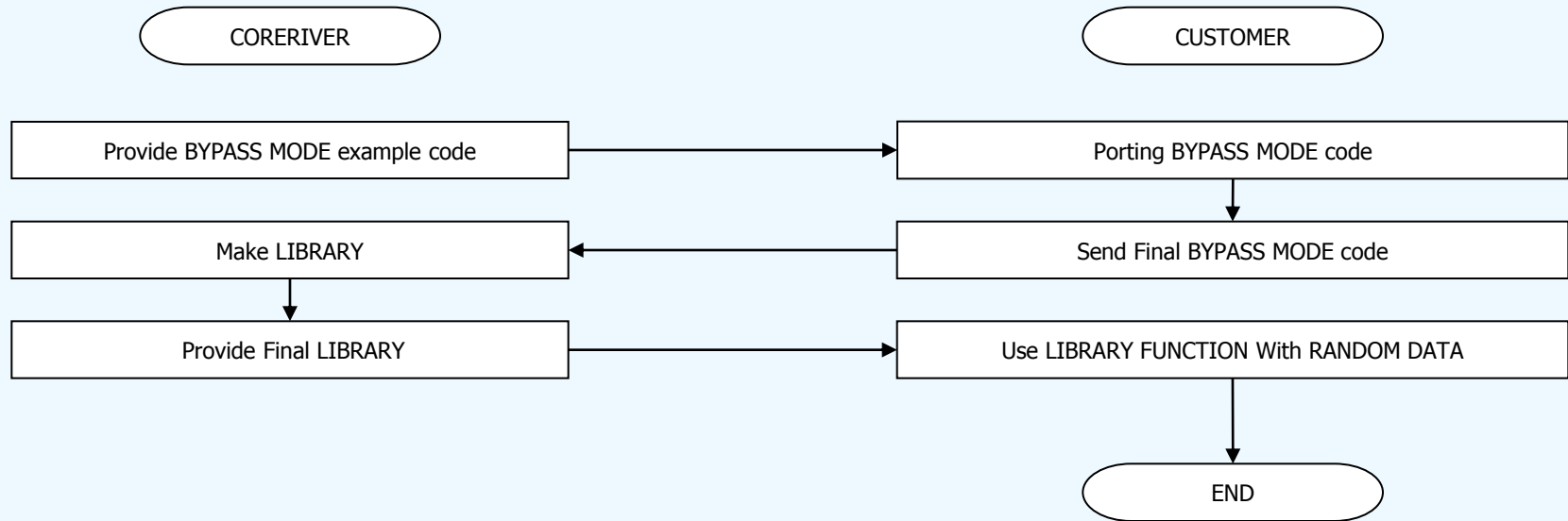
# 11. I2C Speed

*Confidential*

Device	I2C Min Speed	I2C Max Speed
SecurityCore 1.0~3.0	3KHz	10KHz
SecurityCore 4.0	3KHz	100KHz
SecurityCore 4.1	3KHz	800KHz
SecurityCore 412	3KHz	800KHz

## 12. How to support Library

*Confidential*



**NOTE : If CORERIVER don't have customer's development environment, we can borrow customer's IDE or visit customer's company to make library.**

## 13. Absolute Maximum Ratings

*Confidential*

Items	Conditions	Ranges
Voltage on any pin relative to Ground	-	-0.5V to ( $V_{DD}+0.5V$ )
Voltage in $V_{DD}$ relative to Ground	-	-0.5V to 6.5V
Output Voltage	-	-0.5V to ( $V_{DD}+0.5V$ )
Output Current High	One I/O pin active	-25mA
	All I/O pin active	-100mA
Output Current Low	One I/O pin active	+30mA
	All I/O pin active	+150mA
Operating Temperature	-	-40 °C to 85 °C
Storage Temperature	-	-65 °C to +150 °C
Soldering Temperature	-	160 °C for 10 seconds

# 14. DC Characteristics

*Confidential*

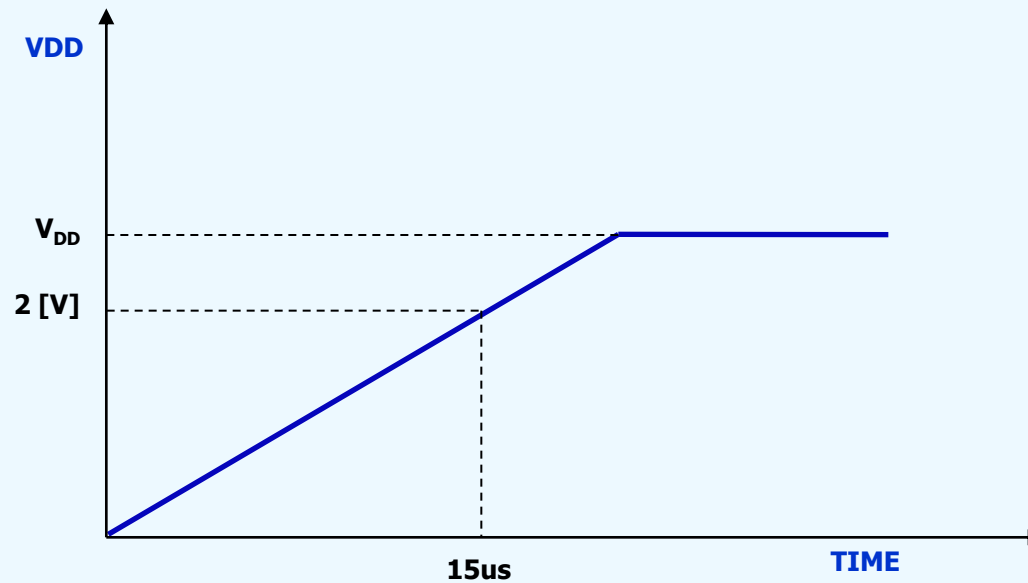
\* TA = -20 °C ~ +85 °C, V<sub>DD</sub> = 2.4V ~ 5.5V unless otherwise specified.

Parameter	Symbol	Pin	Conditions	Value			Unit
				Min.	Typ.	Max.	
Input Low Voltage	V <sub>IL1</sub>	BDATA	V <sub>DD</sub> = 2.4V~5.5V	-0.5	-	0.2V <sub>DD</sub> -0.1	V
				-0.5	-	0.3V <sub>DD</sub>	
Input high Voltage	V <sub>IH1</sub>	BDATA	V <sub>DD</sub> = 2.4V~5.5V	0.2V <sub>DD</sub> +1.0	-	V <sub>DD</sub> +0.5	V
				0.7V <sub>DD</sub>	-	V <sub>DD</sub> +0.5	
Output Low Voltage	V <sub>OL1</sub>	BDATA	I <sub>OL</sub> = 20mA @V <sub>DD</sub> =5V (I <sub>OL</sub> = 5mA @V <sub>DD</sub> =2.6V)	-	-	0.3V <sub>DD</sub>	V
	V <sub>OL2</sub>	RESETB	I <sub>OL</sub> = 10mA @V <sub>DD</sub> =5V (I <sub>OL</sub> = 2.5mA @V <sub>DD</sub> =2.6V)	-	-	0.3V <sub>DD</sub>	
Output High Voltage	V <sub>OH</sub>	BDATA	I <sub>OH</sub> = -15mA @V <sub>DD</sub> =5V (I <sub>OH</sub> = -2.5mA @V <sub>DD</sub> =2.6V)	0.7V <sub>DD</sub>	-	-	V
	V <sub>OHP1</sub>	BDATA (pull-up resistor only)	I <sub>OH</sub> = -140uA @V <sub>DD</sub> =5V (I <sub>OH</sub> = -20uA @V <sub>DD</sub> =2.6V)	0.7V <sub>DD</sub>	-	-	V
Input Leakage Current	I <sub>IL</sub>	All pins	V <sub>IN</sub> = V <sub>IH</sub> or V <sub>IL</sub>	-	-	±1	μA
Pin Capacitance	C <sub>I0</sub>	All	V <sub>DD</sub> = 5V	-	10	-	pF

# 15. Power Characteristics

*Confidential*

Parameter	Symbol	Pin	Conditions	Value [us]
Power Input Width	$t_{\text{power}}$	VDD	$V_{\text{DD}} = 5\text{V} \pm 10\%$ $V_{\text{DD}} = 3\text{V} \pm 10\%$	15

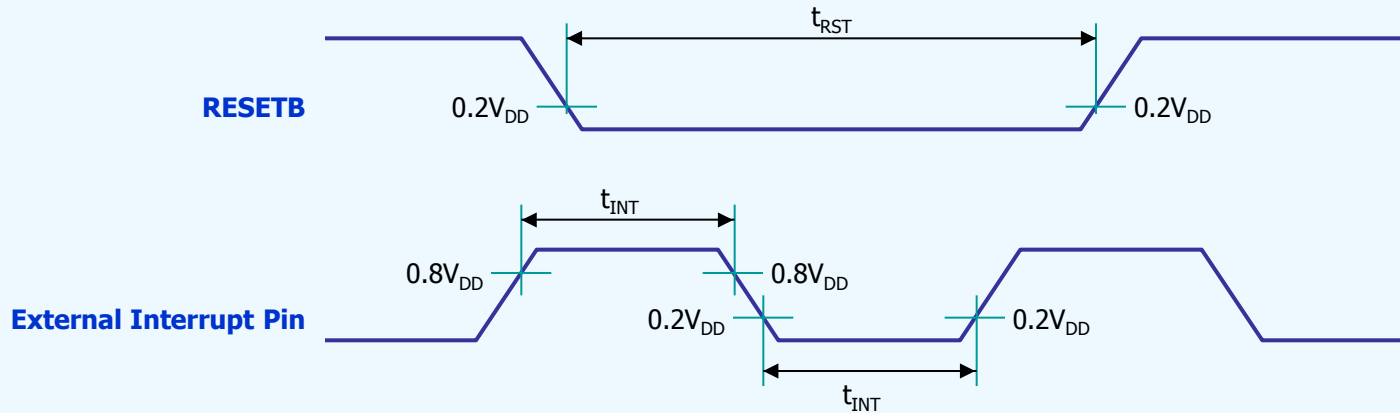


# 16. AC Characteristics

*Confidential*

\* TA = -20 °C ~ +85 °C unless otherwise specified.

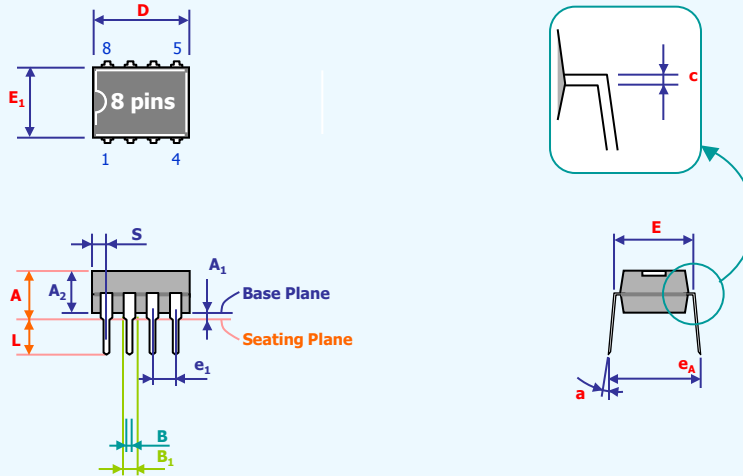
Parameter	Symbol	Pin	Conditions	Value [??]			Unit
				Min.	Typ.	Max.	
RESETB Input Width	$t_{RST}$	RESETB	$V_{DD} = 5V \pm 10\%$	24	-	-	$F_{OSC}$
			$V_{DD} = 3V \pm 10\%$	24	-	-	
External Interrupt Input Width	$t_{INT}$	External Interrupt	$V_{DD} = 5V \pm 10\%$	4	-	-	$F_{OSC}$
			$V_{DD} = 3V \pm 10\%$	4	-	-	



# 17. Package Dimensions : 8-SPDIP/8-SOIC

*Confidential*

## [8-SPDIP]

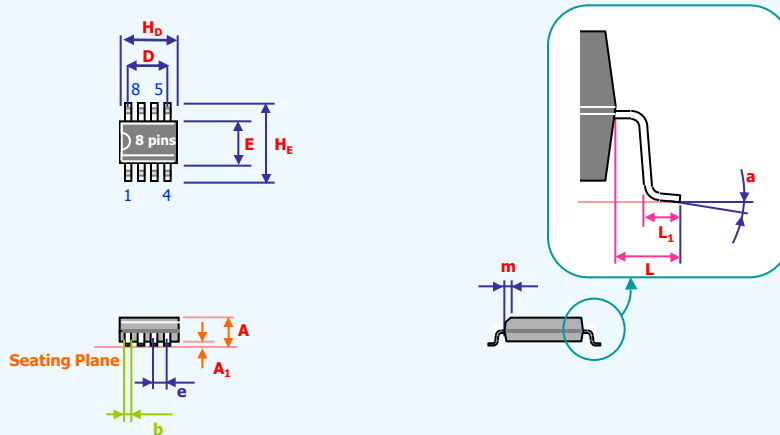


Symbol	Dimension in Inches			Dimension in mm		
	Min.	Nom.	Max.	Min.	Nom.	Max.
A	-	-	0.200	-	-	5.080
A <sub>1</sub>	0.015	-	-	0.381	-	-
A <sub>2</sub>	0.150	0.155	0.160	3.810	3.937	4.064
B	0.016	0.018	0.022	0.406	0.457	0.559
B <sub>1</sub>	0.045	0.055	0.065	1.143	1.397	1.651
c	0.008	0.010	0.012	0.203	0.254	0.356
D	0.445	0.455	0.475	11.303	11.557	12.065
E	0.290	0.300	0.310	7.366	7.62	7.874
E <sub>1</sub>	0.249	0.250	0.251	6.10	6.35	6.60
e <sub>1</sub>	0.090	0.100	0.110	2.286	2.540	2.794
L	0.120	0.130	0.140	3.048	3.302	3.556
a	0 <sup>ø</sup>	-	15 <sup>ø</sup>	0 <sup>ø</sup>	-	15 <sup>ø</sup>
e <sub>A</sub>	0.330	0.350	0.370	8.382	8.89	9.398
S	-	-	0.090	-	-	2.286

**Notes:**

1. Dimension D Max. & S include mold flash or tie bar Burns.
2. Dimension E<sub>1</sub> does not include interlead flash.
3. Dimension D & E<sub>1</sub> include mold mismatch and are determined at the mold parting line.
4. Dimension B<sub>1</sub> does not include dambar protrusion/intrusion.
5. General appearance spec. should be based on final visual inspection spec.

## [8-SOIC]



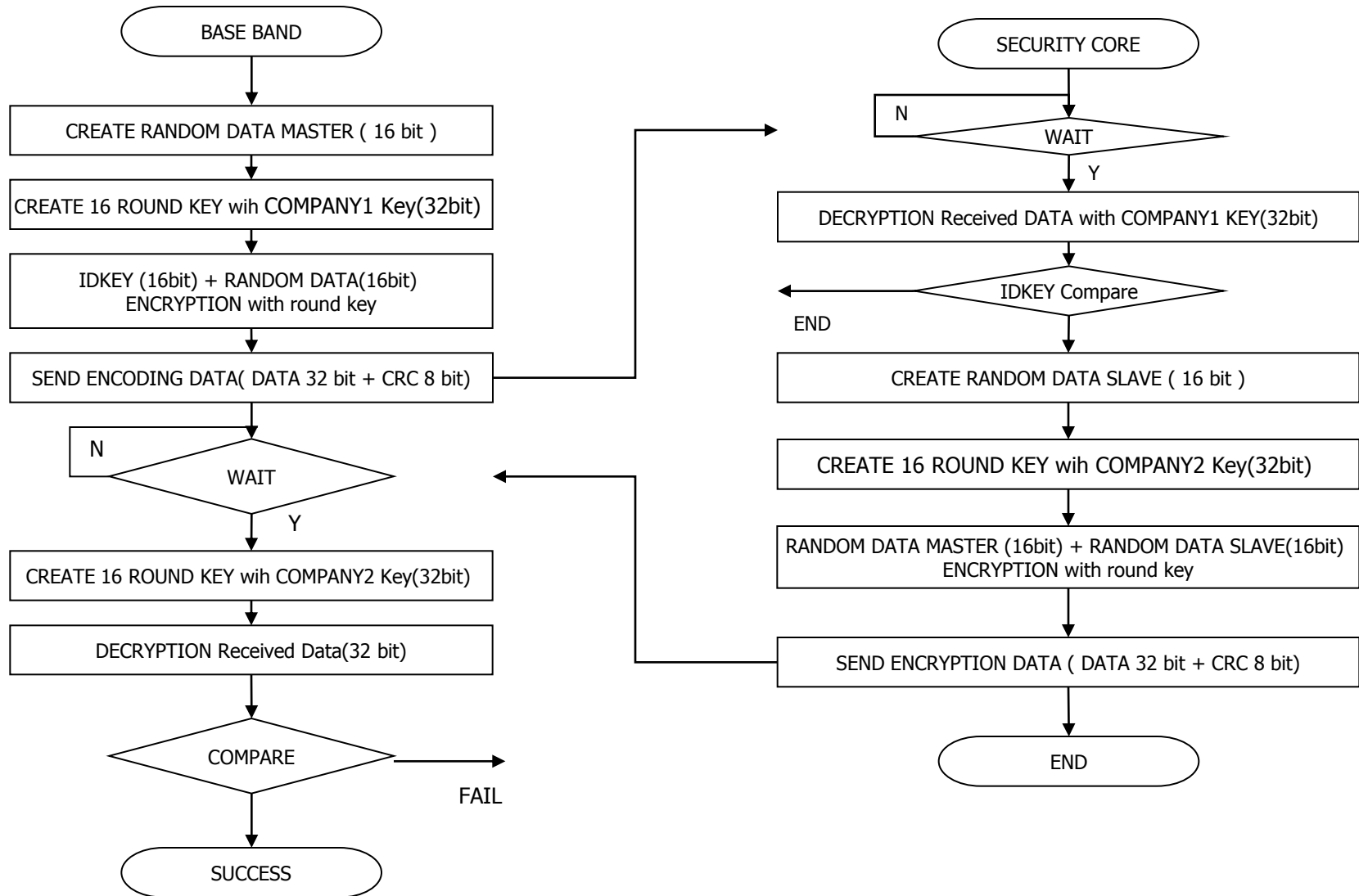
Symbol	Dimension in Inches			Dimension in mm		
	Min.	Nom.	Max.	Min.	Nom.	Max.
A	0.093	0.099	0.104	2.35	2.45	2.65
A <sub>1</sub>	0.004	0.008	0.012	0.10	0.20	0.30
b	0.014	0.016	0.019	0.35	0.42	0.49
D	-	0.150	-	-	3.81	-
E	0.150	0.153	0.157	3.80	3.90	4.00
H <sub>b</sub>	0.189	0.193	0.197	4.80	4.90	5.00
H <sub>c</sub>	0.234	0.239	0.244	5.95	6.07	6.20
L	0.038	0.043	0.048	0.97	1.08	1.2
L <sub>1</sub>	0.022	0.027	0.032	0.58	0.70	0.82
a	0 <sup>ø</sup>	-	8 <sup>ø</sup>	0 <sup>ø</sup>	-	8 <sup>ø</sup>
e	0.050 BSC			1.27 BSC		
m	0.010	0.015	0.020	0.25	0.37	0.50

**Notes:**

1. Dimension D & E include mold mismatch and are determined at the mold parting line.
2. General appearance spec. should be based on final visual inspection spec.

# 18. Algorithm flow chart

*Confidential*



## Appendix : Update History

- ◆ V1.0
  - ✓ spec draft
- ◆ V1.1
  - ✓ What's copy protection Image.
- ◆ V1.2
  - ✓ I2C Interface.
- ◆ V1.3
  - ✓ Package Dimensions.
- ◆ V1.4
  - ✓ SecurityCore3.0 Addition.
- ◆ V1.5
  - ✓ SecurityCore3.0 Strong Point Addition.
- ◆ V1.6
  - ✓ SecurityCore3.0 power slop Addition
- ◆ V1.7
  - ✓ SecurityCore4.0 Addition
- ◆ V1.8
  - ✓ SecurityCore4.1 Addition
- ◆ V1.9
  - ✓ SecurityCore412 Addition
- ◆ V2.0
  - ✓ SecurityCore412 strong point Addition