Notification about the transfer of the semiconductor business

The semiconductor business of Panasonic Corporation was transferred on September 1, 2020 to Nuvoton Technology Corporation (hereinafter referred to as "Nuvoton"). Accordingly, Panasonic Semiconductor Solutions Co., Ltd. became under the umbrella of the Nuvoton Group, with the new name of Nuvoton Technology Corporation Japan (hereinafter referred to as "NTCJ").

In accordance with this transfer, semiconductor products will be handled as NTCJ-made products after September 1, 2020. However, such products will be continuously sold through Panasonic Corporation.

Publisher of this Document is NTCJ.
If you would find description “Panasonic” or “Panasonic semiconductor solutions”, please replace it with NTCJ.

※ Except below description page
“Request for your special attention and precautions in using the technical information and semiconductors described in this book”

Nuvoton Technology Corporation Japan

Panasonic®

SYSTEM LSI Dual Interface RFID

MN63Y1208-E1
Administrator's Manual Ver. 1.1

＜ non NDA type ＞

About this manual

■ Organization

These specifications provide important information for users of the MN63Y1007E1, including an overview and descriptions of functions.

■ Manual Configuration

Each section of this manual consists of a title, main text, and notes. The layout and definition of each section are shown below.

1.1 UART

Middle title

This section describes the UART specification.

1.1.1 Communication Specifications

Small title

Table 1-1 shows the UART specification of this RFID.

Table 1-1 UART Communication Specification

Data transfer method	Asynchronous, half-duplex (Only IRQ notification allows full-duplex)
Data rate	1200 bps, 2400 bps, 4800 bps, 9600 bps, 19200 bps, 38400 bps
Character transmission	·LSB-first ·Data (8 bits) ·Start bit (1bit) ·Parity bit (1bit, even) ·Stop bit (1bit) See Note below.
Other	No flow control signal (RTS/CTS)

Text

Note: In order to ensure the timing margin, when sending consequtive data from the host, use a 2-bit stop bit or set the interval between stop bit and next start bit to 1 bit or more.

Note

This is the Note.
Please read.

■ Finding Desired Information

This manual provides two methods for finding desired information quickly and easily.

1. Consult the table of contents at the front of the manual to locate desired titles.
2. Chapter names are located at the top outer corner of each page, and section titles are located at the bottom outer corner of each page.

Contents

Chapter 1 Overview

1.1 Overview

This is a manual for the administrator of the dual interface RFID (Radio Frequency Identification) LSI MN63Y1208, and describes the following:

■ System area (Chapter 2)

Describes the information on security in the system area of FeRAM, which is omitted in the User's Manual.

■ Cipher functionality (Chapter 3)

Provides the cipher functionality (encryption, authentication) that uses AES.

■ Additional error codes (Chapter 4)

Provides the error codes related to the Administrator's Manual, which are not described in the User's Manual.

■ Annex (Chapter 5)

Describes examples of configuring the system area in the manufacturing process.

Chapter 2 System Area

2

2.1 Physical Memory Map

Figure 2-1 shows the physical memory map. The part indicated in bold italic is to be defined in this manual.

Blocks 25 and 26 are the user area and can be also used as the area storing secrec key for encryption by a family key to be described in Chapter 4. If family key is not used, the blocks can be used as the user area.

<table>
<tr><th>Block</th><th>Address</th><th>0x0</th><th>0x1</th><th>0x2</th><th>0x3</th><th>0x4</th><th>0x5</th><th>0x6</th><th>0x7</th><th>0x8</th><th>0x9</th><th>0xA</th><th>0xB</th><th>0xC</th><th>0xD</th><th>0xE</th><th>0xF</th></tr>
<tr><td>0</td><td>0x0000</td><td colspan="16">User Area</td></tr>
<tr><td>1</td><td>0x0010</td><td colspan="16">User Area</td></tr>
<tr><td>2</td><td>0x0020</td><td colspan="16">User Area</td></tr>
<tr><td>3</td><td>0x0030</td><td colspan="16">User Area</td></tr>
<tr><td>4</td><td>0x0040</td><td colspan="16">User Area</td></tr>
<tr><td>5</td><td>0x0050</td><td colspan="16">User Area</td></tr>
<tr><td>6</td><td>0x0060</td><td colspan="16">User Area</td></tr>
<tr><td>7</td><td>0x0070</td><td colspan="16">User Area</td></tr>
<tr><td>8</td><td>0x0080</td><td colspan="16">User Area</td></tr>
<tr><td>9</td><td>0x0090</td><td colspan="16">User Area</td></tr>
<tr><td>10</td><td>0x00A0</td><td colspan="16">User Area</td></tr>
<tr><td>11</td><td>0x00B0</td><td colspan="16">User Area</td></tr>
<tr><td>12</td><td>0x00C0</td><td colspan="16">User Area</td></tr>
<tr><td>13</td><td>0x00D0</td><td colspan="16">User Area</td></tr>
<tr><td>14</td><td>0x00E0</td><td colspan="16">User Area</td></tr>
<tr><td>15</td><td>0x00F0</td><td colspan="16">User Area</td></tr>
<tr><td>16</td><td>0x0100</td><td colspan="16">User Area</td></tr>
<tr><td>17</td><td>0x0110</td><td colspan="16">User Area</td></tr>
<tr><td>18</td><td>0x0120</td><td colspan="16">User Area</td></tr>
<tr><td>19</td><td>0x0130</td><td colspan="16">User Area</td></tr>
<tr><td>20</td><td>0x0140</td><td colspan="16">User Area</td></tr>
<tr><td>21</td><td>0x0150</td><td colspan="16">User Area</td></tr>
<tr><td>22</td><td>0x0160</td><td colspan="16">User Area</td></tr>
<tr><td>23</td><td>0x0170</td><td colspan="16">User Area</td></tr>
<tr><td>24</td><td>0x0180</td><td colspan="16">User Area</td></tr>
<tr><td>25</td><td>0x0190</td><td colspan="16">User Area (EEFK)</td></tr>
<tr><td>26</td><td>0x01A0</td><td colspan="16">User Area (EEMK)</td></tr>
<tr><td>27</td><td>0x01B0</td><td colspan="16">EEK</td></tr>
<tr><td>28</td><td>0x01C0</td><td colspan="16">EMK</td></tr>
<tr><td>29</td><td>0x01D0</td><td colspan="8">COUNTER</td><td colspan="4">CFEN</td><td colspan="4">MC</td></tr>
<tr><td>30</td><td>0x01E0</td><td colspan="2">SC</td><td colspan="8">IDM</td><td colspan="2">PMM</td><td>AFI</td><td>FWI</td><td colspan="2">HW1</td></tr>
<tr><td>31</td><td>0x01F0</td><td colspan="4">RORF</td><td colspan="4">ROSI</td><td colspan="4">SECURITY</td><td>TNPRM</td><td>HW2</td><td>SL</td><td>BCC</td></tr>
</table>

Figure 2-1 Physical Memory Map

2.2 System Area

This section describes the system area.

2.2.1 Parameter Specification

This section provides parameters for security in the system area. For information about other parameters, see the User's Manual.

All addresses and block numbers used in this section correspond to the physical address in Figure 2-1.

■ EEK (16 bytes)

EEK is a secret key used for data encryption or decryption in encrypted communication with private key, and is encrypted by master key and stored in this area.

Reading this area causes all-0 to be read. For more information, see Chapter 4.

When writing data to this parameter, use data for EEK only. For more information, see Table 4-7.

■ EMK (16 bytes)

EMK is a secret key used for MAC (Message Authentication Code) generation and authentication in encrypted communication with private key, and is encrypted by master key and stored in this area.

Reading this area causes all-0 to be read. For more information, see Chapter 4.

Note: When writing data to this parameter, use data for EMK only. For more information, see Table 4-7.

■ COUNTER (8 bytes)

COUNTER is a value used as a part of the initialization vector (16 bytes) in encrypted communication with READ command.

In manufacturing process, when writing the Block 29 data to this area, write all-0 data.

For more information, see Chapter 4.

Table 2-1 COUNTER Parameter

Address	0x01D0	0x01D1	0x01D2	0x01D3	0x01D4	0x1D5	0x1D6	0x01D7
COUNTER	D0	D1	D2	D3	D4	D5	D6	D7

Note: This RFID increases the COUNTER value every time it receives a READ command in encrypted communication.

■ CFEN (4 bytes)

As with BCC, CFEN is a flag data to validate the setting values in the system area of FeRAM. Table 2-2 shows the valid setting values for system area. Until valid values are written to CFEN and BCC, default values (implemented in hardware) are used for each parameter. For information about the default values, see Section 3.3 in the User's Manual and the descriptions for each parameter in this section.

Table 2-2 Valid CFEN Setting Values for System Area

Address	0x01D8	0x01D9	0x01DA	0x01DB
System area enable setting	0x01	0x23	0x45	0x67

Note: For EEK, EMK, and COUNTER, no default values are provided and the system area values of FeRAM are used regardless of CFEN settings.

Note: In order to enable the written flag data, the RFID's power supplies (both VDDEX and the supply from RF interface) must be turned off once after writes. The data will be enabled after next power-on.

Note: Before writing valid setting values to CFEN, write the given setting values to each parameter in the system area of FeRAM. (Default values for each parameter are implemented in hardware.)

■ MC (4 bytes)

MC is a data to control the internal modes of this RFID.

In manufacturing process, when writing the Block 29 data to this area, write the data shown in Table 2-3.

Table 2-3 MC Setting Values

Address	0x01DC	0x01DD	0x01DE	0x01DF
System area enable setting	0x89	0xAB	0xCD	0xEF

■ SL (1 byte)

SL is a flag data to lock the system area. Table 2-4 shows the SL settings and corresponding values. Setting the SL to MODE1 or MODE2 allows to lock the write operation to parameters of the system area.

By default, the SL is set to 0x00 (MODE0).

Table 2-4 SL Settings and Corresponding Values

Mode	MODE0		MODE1		MODE2	
Setting value (Address: 0x01FE)	0x00		0x0F		0xFF	
Interface to be accessed	RF	Serial	RF	Serial	RF	Serial
EEK *)	R/W	R/W	RO	RO	RO	RO
EMK *)	R/W	R/W	RO	RO	RO	RO
COUNTER	R/W	R/W	RO	RO	RO	RO
CFEN	R/W	R/W	RO	RO	RO	RO
MC	R/W	R/W	RO	RO	RO	RO
SC	R/W	R/W	RO	RO	RO	RO
IDM	R/W	R/W	RO	RO	RO	RO
PMM	R/W	R/W	RO	RO	RO	RO
AFI	R/W	R/W	RO	RO	RO	RO
FWI	R/W	R/W	RO	RO	RO	RO
HW1	R/W	R/W	RO	RO	RO	RO
RORF	R/W	R/W	RO	R/W	RO	RO
ROSI	R/W	R/W	RO	R/W	RO	RO
SECURITY	R/W	R/W	RO	R/W	RO	RO
TNPRM	R/W	R/W	RO	R/W	RO	RO
HW2	R/W	R/W	RO	R/W	RO	RO
SL	R/W	R/W	RO	R/W	RO	RO
BCC	R/W	R/W	RO	R/W	RO	RO

*) All-0 is always read. R/W: Read/Write, RO: Read Only

In addition, Figure 2-2 illustrates the state transition diagram between system lock modes. Writing 0x0F to SL allows to transition from MODE0 to MODE1. Writing 0xFF to SL allows to transition from MODE0 or MODE1 to MODE2. The transition from MODE2 to MODE1 is disabled.

Note: SL is the flag data for locking the system area.

In order to release the system area that was once locked, dedicated command using the serial

The disclosure of this dedicated command, NDA is required.

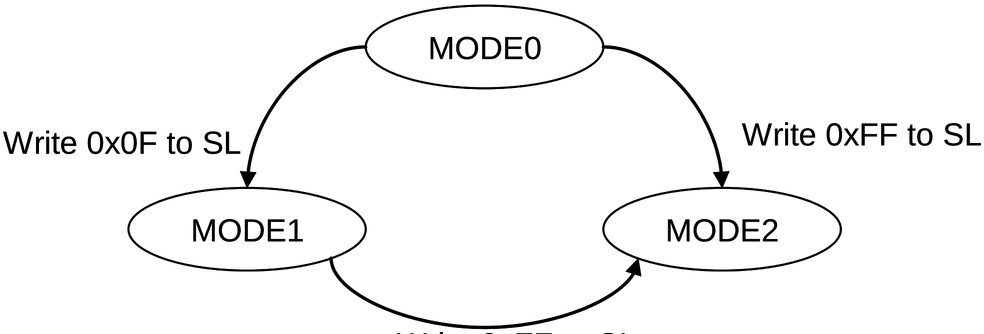

Figure 2-2 State Transition Diagram between System Lock Modes

■　BCC (1 byte)

BCC is a flag data to validate the setting values in the system area of FeRAM. Table 2-5 shows the valid setting value for system area. Until valid values are written to BCC and CFEN, default values (implemented in hardware) are used for each parameter. For information about the default values, see Section 3.3 in the User's Manual and the descriptions for each parameter in this section.

Table 2-5 Valid BCC Setting Value for System Area

Address	0x01FF
System area enable setting	BCC setting value

BCC setting value is obtained by adding the values at 0x01D8 to 0x01EF and 0x01FC to 0x01FE of the system area, byte-by-byte, to the default value 0x00 of 1 byte and subtracting the lower one byte of the calculation result from 0x100.

BCC is calculated by hardware at power-on of this RFID or at a reset.

If the calculation result generates an error, this LSI operates with default values for each parameter and the error state can be read with a response to the RREG command in serial communication.

2.2.2 Parameter Application Timing

Table 2-6 lists the setting application timings after rewriting parameters in the system area while CFEN is enabled.

Table 2-6 Parameter Application Timing

	A timing at which new parameter setting is applied after rewriting parameters while CFEN is enabled.
EEK	Apply immediately after rewrites.
EMK	Apply immediately after rewrites.
COUNTER	Apply immediately after rewrites.
CFEN	Apply after turning power ON from OFF following rewrites.
MC	Apply after turning power ON from OFF following rewrites.
SL	Apply after turning power ON from OFF following rewrites.
BCC	Apply after turning power ON from OFF following rewrites.

Note: Power OFF means power supplies from both VDDEX and RF interface are OFF.

Chapter 3 Cipher Functionality

3

Chapter 4 Error Code

4

4.1 Error Code

This section provides the error codes related to this Administrator's Manual by interface, which are not described in the User's Manual.

4.1.1 JISX6319-4

Table 4-1 lists the meanings of statuses for JISX6319-4, which are not described in the User's Manual.

Table 4-1 Status Flag

Status flag 1	Status flag 2	Meaning	Description
0xFF	0xA2	Block count specification error	When writing to EEK and EMK, the data size was other than 16 bytes.
0xFF	0x60	Self-diagnosis error	・ MAC verification error occurred in encryption WRITE command processing. ・ Data was written over EEK and EMK. ・ Write access to the system area (SL function) was performed while the system is locked.

4.1.2 ISO/IEC14443 TypeB

Table 4-2 lists the meanings of statuses for ISO/IEC14443 TypeB, which are not described in the User's Manual.

Table 4-2 Status Word

SW1	SW2	Meaning	Description
0x67	0x00	Lc/Le specification error	When writing to EEK and EMK, the data size was other than 16 bytes.
0x6F	0x00	Self-diagnosis error	・ MAC verification error occurred in encryption WRITE command processing. ・ Data was written over EEK and EMK. ・ Write access to the system area (SL function) was performed while the system is locked.

4.1.3 Serial Interface (I2C)

Table 4-3 lists the meanings of statuses for serial interface (I2C), which are not described in the User's Manual.

Table 4-3 Status

Value	Meaning	Description
0x26	Command parameter error	・ When writing to EEK and EMK, the data size was other than 16 bytes. ・ Write access to the system area (SL function) was performed while the system is locked. ・ Data was written over EEK and EMK.

Chapter 5 Annex

5

5.1 Configuring the System Area

When configuring the system area in the manufacturing process, you must follow some precautions. This section describes the precautions and the setting procedures.

5.1.1 Precautions

Precautions are as follows:

- 1: When configuring the system area by using a contactless reader/writer while the contactless reader/writer turns carrier off every time a command is issued, it is necessary to observe the writing unit and order. For example, the parameters (e.g., SC, IDM) related to communication command can change their values when configuring the system area or when writing a valid value to CFEN (*). In this case, when writing a valid value to CFEN, writing data to Blocks 29 to 31 by a single command prevents the system area setting from being complicated.
- 2: Data must be written to EEK (Block 27) and EMK (Block 28) each in units of one block. Use a WRITE command to write a block (16 bytes) of plaintext.
- 3: All-0 is always read from EEK (Block 27) and EMK (Block 28), regardless of the value of written data. When verifying data writes to these blocks, check if the RFID responds normally to the encryption WRITE command.

(*) As an example, we assume that data is written to Blocks 29 and 30 in units of one block while the contactless reader/writer turns carrier off every time a command is issued.

● Description

(1) Writing to Block 29: Write a valid value to CFEN (CFEN has invalid value before executing (1)).

(2) Writing to Block 30: Write a given value to IDM.

When data is written in the order of (1) and (2), the value of IDM changes as follows.

Before executing (1): default value (0x02FE000000000000);

After executing (1): the value of FeRAM that is not written is set since (2) has not yet been executed.

Whe using READ and WRITE commands based on JISX6319-4, IDM must be specified. Although you can acquire the IDM of this RFID using a REQ command, it is necessary to insert a REQ command between (1) and (2) to acquire IDM and set that IDM to the IDM to which a value is to be written by a WRITE command in (2).

When writing a valid value to CFEN, it is recommended to use a single WRITE command for Blocks 29 to 31.

5.1.2 Setting Procedures of System Area

This section provides two setting procedures of the system area (Steps 1 and 2).

Figure 5-1 shows Step 1 (writing all data only in one process).

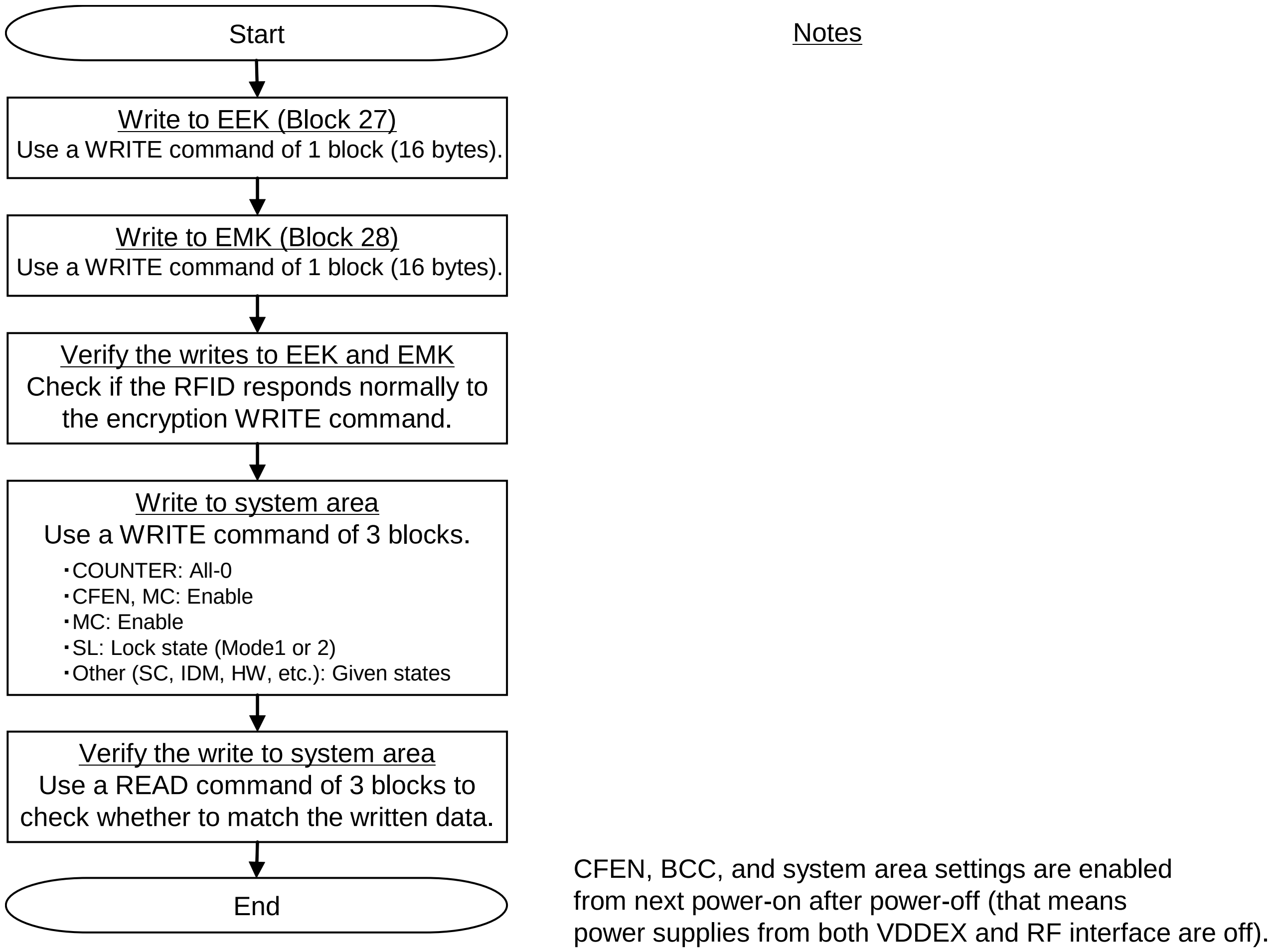

Figure 5-1 System Area Setting Procedure (Step 1)

Figure 5-2 shows Step 2 (writing all data in two processes). This step, for example, can be applied to the case in which first you configure the system area and then configure the user area in another process.

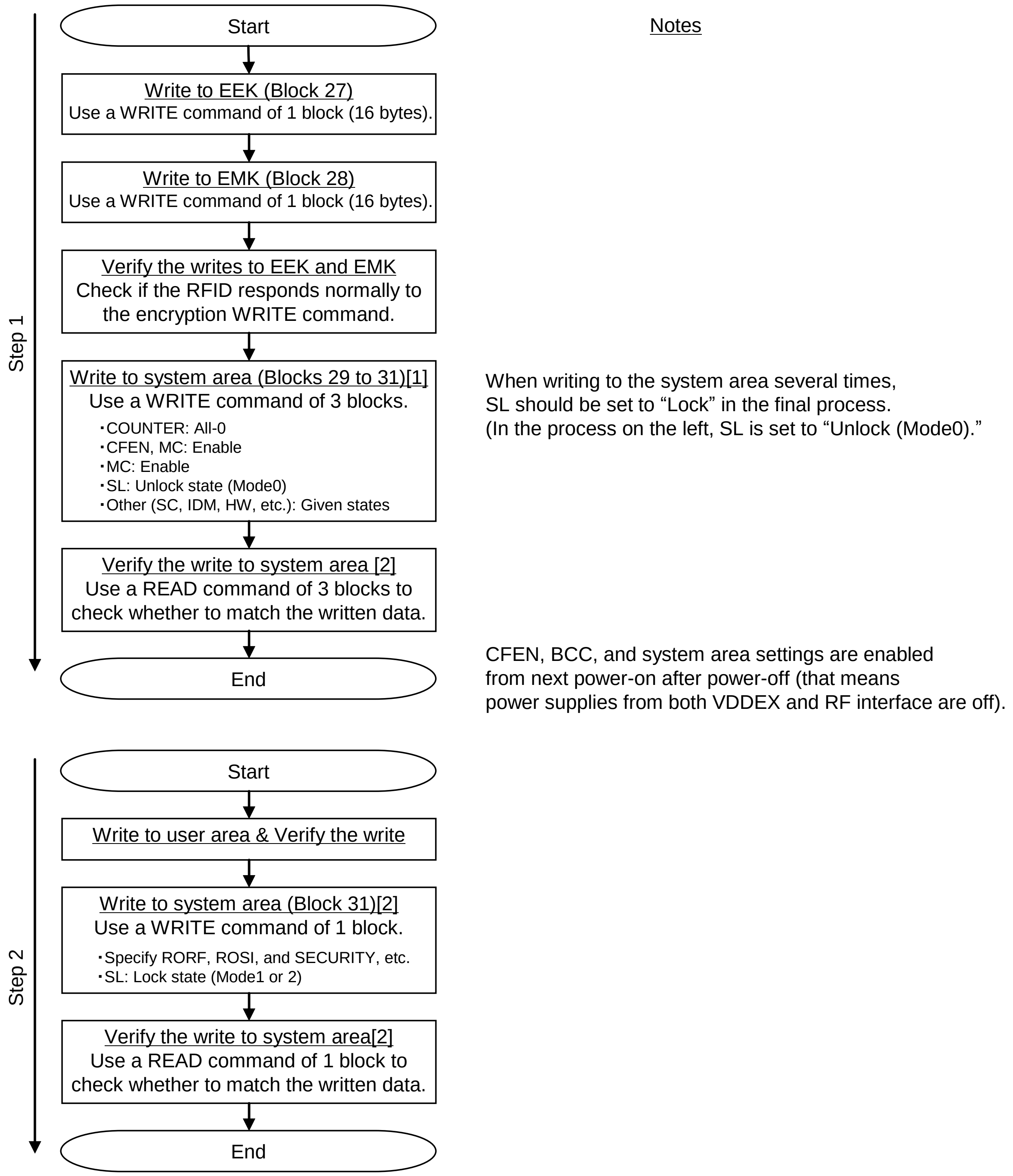

Figure 5-2 System Area Setting Procedure (Step 2)

Revision History

Revised on May 16, 2013

Purpose	Version 1.0			Version xx		
	Page	Section	Comments	Page	Section	Comments
-	-	-	Initial edition	-	-	-

Revised on Jul 18, 2014

Purpose	Version 1.0			Version 1.1		
	Page	Section	Comments	Page	Section	Comments
Add	-	-	-	P13	-	Add Note, “SL is flag data for locking the system area…”

MN63Y1208-E1
Administrator's Manual

Jul. 18, 2014, Version 1.1

Issued by
Panasonic Semiconductor Solutions Co., Ltd.

Edited and produced by
Panasonic Semiconductor Solutions Co., Ltd.

Request for your special attention and precautions in using the technical information and semiconductors described in this book

(1) If any of the products or technical information described in this book is to be exported or provided to non-residents, the laws and regulations of the exporting country, especially, those with regard to security export control, must be observed.

(2) The technical information described in this book is intended only to show the main characteristics and application circuit examples of the products. No license is granted in and to any intellectual property right or other right owned by Panasonic Corporation, Nuvoton Technology Corporation Japan or any other company. Therefore, no responsibility is assumed by our company as to the infringement upon any such right owned by any other company which may arise as a result of the use of technical information de-scribed in this book.

(3) The products described in this book are intended to be used for general applications (such as office equipment, communications equipment, measuring instruments and household appliances), or for specific applications as expressly stated in this book.
Please consult with our sales staff in advance for information on the following applications, moreover please exchange documents separately on terms of use etc.: Special applications (such as for in-vehicle equipment, airplanes, aerospace, automotive equipment, traffic signaling equipment, combustion equipment, medical equipment and safety devices) in which exceptional quality and reliability are required, or if the failure or malfunction of the products may directly jeopardize life or harm the human body.
Unless exchanging documents on terms of use etc. in advance, it is to be understood that our company shall not be held responsible for any damage incurred as a result of or in connection with your using the products described in this book for any special application.

(4) The products and product specifications described in this book are subject to change without notice for modification and/or improvement. At the final stage of your design, purchasing, or use of the products, therefore, ask for the most up-to-date Product Standards in advance to make sure that the latest specifications satisfy your requirements.

(5) When designing your equipment, comply with the range of absolute maximum rating and the guaranteed operating conditions (operating power supply voltage and operating environment etc.). Especially, please be careful not to exceed the range of absolute maximum rating on the transient state, such as power-on, power-off and mode-switching. Otherwise, we will not be liable for any defect which may arise later in your equipment.
Even when the products are used within the guaranteed values, take into the consideration of incidence of break down and failure mode, possible to occur to semiconductor products. Measures on the systems such as redundant design, arresting the spread of fire or preventing glitch are recommended in order to prevent physical injury, fire, social damages, for example, by using the products.

(6) Comply with the instructions for use in order to prevent breakdown and characteristics change due to external factors (ESD, EOS, thermal stress and mechanical stress) at the time of handling, mounting or at customer's process. We do not guarantee quality for disassembled products or the product re-mounted after removing from the mounting board.
When using products for which damp-proof packing is required, satisfy the conditions, such as shelf life and the elapsed time since first opening the packages.

(7) When reselling products described in this book to other companies without our permission and receiving any claim of request from the resale destination, please understand that customers will bear the burden.

(8) This book may be not reprinted or reproduced whether wholly or partially, without the prior written permission of our company.

No.070920