Operational Description

- Model RC-S480C -

Version 1.0

Sony Corporation

Reader/Writer Operation

After turning on the power switch, the Reader/Writer transmits 13.56MHz 10% ASK polling signal with the specified intensity until receiving a response from a contactless card. After receiving the response from a card the device starts to communicate with the card by using the same frequency and modulation. Though the reader/writer is a self-operating device according to the program installed in the FLASH memory, it can be connected to a host computer (Controller) for more complicated applications by taking out the reader/writer from the enclosure. For the connection to a host computer, refer to the initialization and communication protocols described below.

1 Connection with *Controller*

- Interface Connector : HKP-40M1 (Honda Tsushin Kogyo Co., Ltd.)

  The interface connector is a 40-pin double row C-antenna connector located at the lower edge of the RF/Control board. The pitch of connector pins is 2.54mm.Connector pins are gilded.

  The left end of the bottom row of connector pins is No. 1. Pin assignment of the connector (CN2) is shown in Fig. 1 and Table 1.

  12V :DC input port (for RF power amplifier)
  5V :DC input port
  GND :Ground port
  SI, SO :Serial Data I/O (CMOS 5*V*)
  DA0-7 :Parallel Data I/O (CMOS 5*V*)
  DA0-7 are connected to PG0-7 of DPU IC CXD8680R. In order to control DA0-7, it is necessary to load other program code to RF/Control board. (see "*Reader/Writer* Programmer's Reference Manual")
  DB0-7 :Parallel Data I/O (CMOS 5*V*)
  DB0-7 are connected to PH0-7 of DPU IC CXD8680R. In order to control DB0-7, it is necessary to load other program code to RF/Control board. (see "*Reader/Writer* Programmer's Reference Manual")
  HS0-3 :Parallel Data I/O (CMOS 5*V*)
  HS0-2 are connected to PF4-6 of DPU IC CXD8680R, and HS3 is connected to both PF7 and PF2. In order to control HS0-3, it is necessary to load other program code to RF/Control board. (see "*Reader/Writer* Programmer's Reference Manual")
  Mode :No connection in usual operation.
  Only in loading program, high level voltage (5*V*) shall be applied to the pin before RF/Control board is powered on

- Power

  voltage :DC12*V* (CN2 pin1 and 3)
  :DC5*V* (CN2 pin34 and 36)
  voltage allowance :DC12*V* +4*V*, -0.5*V*
  :DC5*V* ±0.5*V*
  current :DC12*V* ≈ 90mA
  :DC5*V* ≈150mA
  voltage ripple allowance :100*mV* (peak-to-peak)

  The *Reader/Writer* can be operated in the voltage range of 5 - 11.5*V* and the voltage ripple > 100*mV* for DC12*V*, however operating distance cannot be assured in such condition.

- External Interface

serial 1 port : CMOS logic level (5*V*)
software selectable, non-inverted or inverted, and baud rate
(default setting : non-inverted, 115.2*kbps*)
parallel 20bit I/O port : CMOS logic level (5*V*)

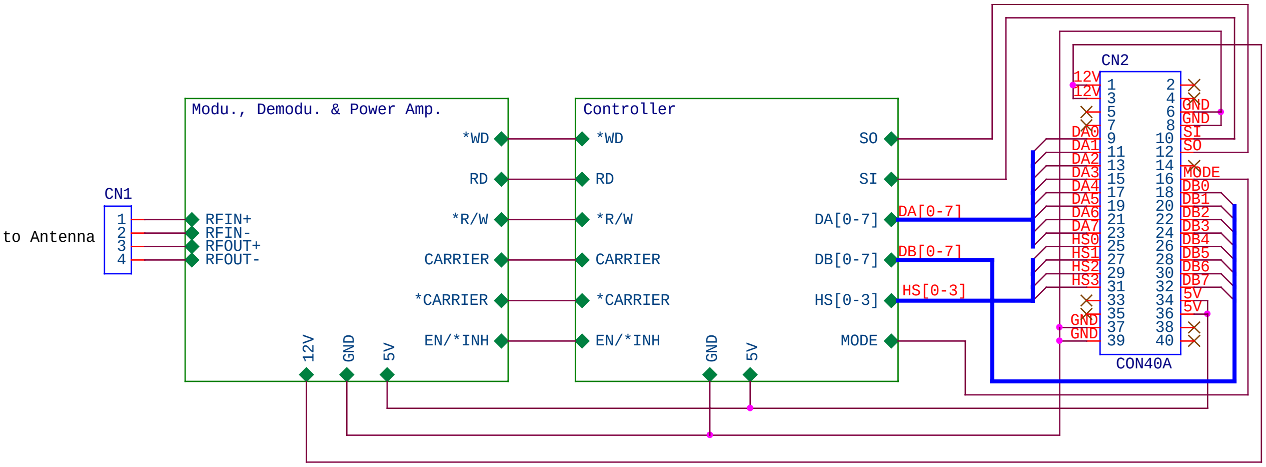

Fig.1 : Pin Assignment of Connectors CN1-2

Pin No.	Pin Assignment	Pin Assignment	Pin No.
1	12V	No Connection	2
3	12V	No Connection	4
5	No Connection	GND	6
7	No Connection	GND	8
9	DA0	SI	10
11	DA1	SO	12
13	DA2	No Connection	14
15	DA3	MODE	16
17	DA4	DB0	18
19	DA5	DB1	20
21	DA6	DB2	22
23	DA7	DB3	24
25	HS0	DB4	26
27	HS1	DB5	28
29	HS2	DB6	30
31	HS3	DB7	32
33	No Connection	5V	34
35	No Connection	5V	36
37	GND	No Connection	38
39	GND	No Connection	40

Table 1 : Pin Assignment of Interface Connector CN2

2 Transaction Overview

2.1 Communication Protocol

There are two communication protocols, namely, data link level and application level protocol.

Either ACK or NACK packet is returned in every packet transfer. ACK indicates a successful transfer, NACK means unsuccessful.

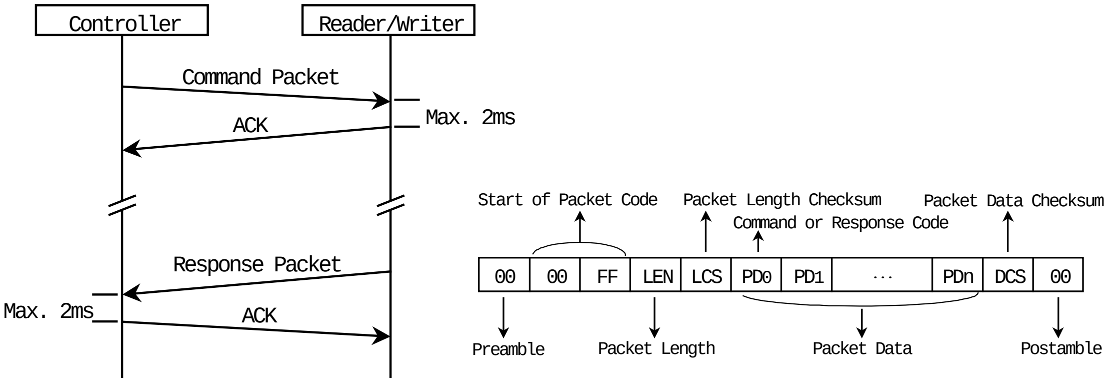

Fig. 2 : Communication Protocol and Packet Structure

2.2 Re-sending Protocol

Reader/Writer supports the re-sending procedure in *Controller* interface. Re-sending handling is triggered or required in the two cases below :

1. NACK packet is returned.
2. Neither ACK nor NACK response comes. (time out)

Controller should re-send the same packet within 5*ms* after receiving NACK or detecting time out.

2.3 ACK / NACK Packet

ACK / NACK packet format is as follows :
ACK : LEN = 00h & LCS = ffh without Packet Data part and DCS
NACK : LEN = ffh & LCS = 00h without Packet Data part and DCS

2.4 Mutual Authentication

Mutual Authentication is a process that is performed between *Controller* and *Reader/Writer* to authenticate each other mutually in order to avoid the fraud usage.
This authentication is based on the following elements :

1. two 8*byte* (64*bit*) keys
2. three pass authentication model (ISO 9758)
3. cryptography algorithm mentioned in section 3.2.5.

2.5 Encryption and Decryption

The cryptography algorithm is used for the following three stages :

1. mutual authentication between *Controller* and *Reader/Writer*
2. mutual authentication between *Reader/Writer* and *Card*
4. commands and data encryption through *Reader/Writer*

3 Communication Commands

3.1 General

In this section, the communication commands between *Controller* and *Reader /Writer* are described.

Table 1-3 shows all commands between *Controller* and general *Reader/Writer*. All commands are categorized into 3 groups as follows :

1. *Reader/Writer* internal operation command
2. *Card* operation command
3. *Card* management command

Card management command group is for issue *Reader/Writer* and not for general *Reader/Writer* .

3.2 *Reader/Writer* Internal Operation Command

3.2.1 Attention Command

Attention Command enables *Reader/Writer* and *Controller* to recognize each other and is the only command available before the authentication completes. The main purpose of this Attention Command is to recognize its partner before authentication and to force *Reader/Writer* to be in the idle state.

3.2.2 Authentication 1 Command

Authentication 1 Command enables *Controller* to authenticate *Reader/Writer*.

3.2.3 Authentication 2 Command

Authentication 2 Command enables *Reader/Writer* to authenticate *Controller*.

3.2.4 Disconnect Command

Disconnect Command is for *Controller* to terminate the communication with *Reader/Writer*.

Command	Command Code	Response Code
Attention	00h	01h
Authentication 1	02h	03h
Authentication 2	04h	05h
Disconnect	06h	07h
Change Reader/Writer Access Key	20h	21h
Self-Diagnosis	40h	41h
Check Firmware Version	44h	45h
Change Communication Mode	46h	47h
Kill Module	4ah	4bh
Reader/Writer Reset	4ch	4dh
Firmware Maintenance	52h	53h

Table 2 : *Reader/Writer* Internal Operation Command

Command	Command Code	Response Code
Polling	80h	81h
Request Service	82h	83h
Request Response	84h	85h
Mutual Authentication	86h	87h
Read Block	88h	89h
Write Block	8ah	8bh
Release	8eh	8fh
Read Without Encryption	98h	99h
Write Without Encryption	9ah	9bh

Table 3 : *Card* Operation Command

Command	Command Code	Response Code
Register Issue ID	c0h	c1h
Register Area	c2h	c3h
Register Service	c4h	c5h
Register Manufacture ID	e0h	e1h
Card Self-Diagnosis	f0h	f1h

Table 4 : *Card* Management Command

3.2.5 Change *Reader/Writer* Access Key Command

Change *Reader/Writer* Access Key Command performs alteration of the access keys, which are stored in *Reader/Writer* for the mutual authentication between *Controller* and *Reader/Writer*.

3.2.6 Self-Diagnosis Command

Self-Diagnosis Command activates self-diagnosis test of *Reader/Writer*. After the Diagnosis completion, *Reader/Writer* sends back the test result.

3.2.7 Check Firmware Version Command

Check Firmware Version Command is used for checking the version of *Reader/Writer* firmware.

3.2.8 Change Communication Mode Command

Change Communication Mode Command performs the following changes : baud rate, logic level interface(non-inverted or inverted), encryption on/off, time-out.

3.2.9 Kill Module Command

Kill Module Command is used for killing the specified module within *Reader/Writer*.

3.2.10 *Reader/Writer* Reset Command

Reader/Writer Reset Command executes the initialization routine.

3.2.11 Firmware Maintenance Command

Firmware Maintenance Command is used for updating the firmware within *Reader/Writer*.

3.3 *Card* Operation Command

3.3.1 Polling Command

Polling Command enables *Reader/Writer* to give a call to *Card* and to detect existence of *Card* by the response from *Card*.

3.3.2 Request Service Command

Request Service Command enables *Reader/Writer* to check whether the specified service code is registered to *Card* or not. In case that the specified service is registered to *Card*, key version of the service is available by the response from *Card*.

3.3.3 Request Response Command

Request Response Command enables *Reader/Writer* to check which mode *Card* is in. There are 4 modes, 'before Authentication', 'after Authentication 1', 'after Authentication 2' and 'after Register xxx Command (see 4.4 *Card* Management Command)'.

3.3.4 Mutual Authentication Command

Mutual Authentication Command activates the mutual authentication procedure between *Reader/Writer* and *Card*.

3.3.5 Read Block Command

Read Block Command activates *Reader/Writer* to read the specified block data from *Card* after the mutual authentication between the *Reader/Writer* and *Card* has been established successfully.

Read Block Command enables a Service Provider with successful mutual authentication to read blocks that this Service Provider has the right to access.

With one Read Block Command, up to 8 block can be read simultaneously. If more than 8 blocks should be read, more than one Read Block Command shall be called separately.

The response of Read Block Command is a 1*byte* Read result and Block Data that has been read. In the Read result, a 1*byte* consequence of one block Read is given in 1*bit*. As there are up to 8 blocks, 1*byte* is enough to record all the Read consequence.

3.3.6 Write Block Command

Write Block Command activates *Reader/Writer* to write the specified block data to *Card* as new data after the mutual authentication between *Reader/writer* and *Card* has been established successfully.

With one Write Block Command, up to 8 block can be written simultaneously. If more than 8 blocks should be written, more than one Write Block Command shall be called separately.

The response of Write Block Command is a 1*byte* Write result. In the Write result, a 1*byte* consequence of one block Write is given in 1*bit*. As there are up to 8 blocks, 1*byte* is enough to record all the Write consequence.

The purse operation can be performed with Write Block Command.

3.3.7 Release Command

Release Command enables *Card* to be released from established communication sequence with *Reader/Writer*.

3.3.8 Read Without Encryption Command

Read Without Encryption Command activates Reader/Writer to read the specified block data from *Card* without the mutual authentication between the *Reader/Writer* and *Card*. Read Without Encryption Command can be applied only to blocks which service code is registered security-free.

The number of blocks that can be read simultaneously and the response of Read

Without Encryption Command are the same as those for Read Block Command (see 4.3.5).

3.3.9 Write Without Encryption Command

Write Without Encryption Command activates Reader/Writer to write the specified block data to *Card* without the mutual authentication between the *Reader/Writer* and *Card*, however can be applied only to blocks which service code is registered security-free.

The number of blocks that can be write simultaneously and the response of Write Without Encryption Command are the same as those for Write Block Command (see 4.3.6).

3.4 *Card* Management Command

The commands described in this section are for issue *Reader/Writer* and not for general *Reader/Writer* .

3.4.1 Register Issue ID Command

Register Issue ID Command makes it possible to register Issue ID(IDi) , Issue Parameter(PMi), System Code and Area 0000 Key to *Card*, and also makes it to erase other services and to initialize Memory Allocation Information in *Card*.

3.4.2 Register Area Command

Register Area Command makes it possible to register new Area and the parameters of new Area to *Card*, which are Service Code Range, Available Block Number and Area Key.

3.4.3 Register Service Command

Register Service Command makes it possible to register new Service and the parameters of new Service to *Card*, which are Service Code, Block Number and Service Key.

3.4.4 Register Manufacture ID Command

Register Manufacture ID Command makes it possible to register Manufacture ID(IDm) , Manufacture Parameter(PMm), System Code, System Key and Area 0000 Key to *Card*, and also makes it to clear Issue ID of *Card*.

In order to execute Register Manufacture ID Command, Manufacture ID must be all 00h. This means that Register Manufacture ID Command is effective to *Card* once for all.

3.4.5 Card Self-Diagnosis Command

Card Self-Diagnosis Command activates self-diagnosis test of *Card*. After the Diagnosis completion, *Card* sends back the test result.