APPLIED WIRELESS ID

PCB-915RM-SD Communication Protocol - 041492

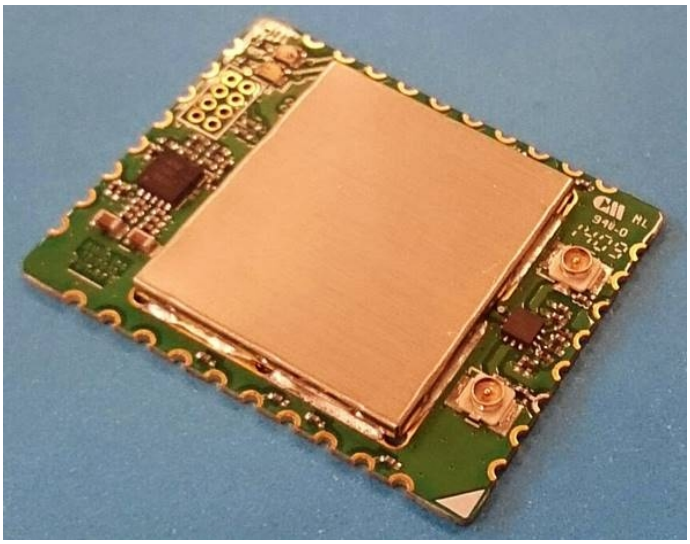


Table of Contents

REVISION HISTORY 3

1 PURPOSE AND SCOPE 4

1.1 DEFINITIONS AND ACRONYMS 4

2 REFERENCES 5

3 PHYSICAL LAYER 6

4 DATA LINK LAYER/COMMUNICATION PACKET 7

4.1 PACKET STRUCTURE 7
4.2 CHECKSUM ALGORITHM 7
4.3 POLL RESPONSE 8

5 MESSAGE LAYER 9

5.1 STOP COMMAND 10
Stop (0x00) 10
5.2 SYSTEM COMMAND (0X00) 11
Firmware Version (0x00) 11
Temperature (0x01) 12
RF Power ON (0x05) 13
RF Power OFF (0x06) 14
Reader Status (0x0B) 15
Antenna Select (0x0D) 18
RF Power Level Control (0x12) 19
Soft Reset (0x80) 20
5.3 EPC CLASS 1 GENERATION 2 COMMAND (0X20) 21
Read Single Tag ID (0x00) 21
Sensitivity Control (0x07) 22
Read Memory (0x1D) 23
Write Memory (0x5F) 25

6 APPENDIX 27

6.1 DATA FLOW 27
6.2 MESSAGES RESPONSES 29

REVISION HISTORY

Version No.	Revised By	Date	Sections Affected	Remarks
1.0	AWID Engineering	1/2015	-	Initial version

1 Purpose and Scope

This document describes the serial (RS232) communication protocol for communications among and between AWID's RFID device PCB-915RM-SD and other HOST systems and equipment.

A HOST system for purposes of this specification could be a personal computer, a POS system or a data collector.

Protocol commands listed in this document are a small subset of those listed in AWID's MPR Communication Protocol (041479).

The device handles one command at a time, applications can be developed to issue a sequence of commands of different categories (system, tag read/write, etc.) with each command following receipt of response from the previous command.

1.1 Definitions and Acronyms

Terms Used	Description of Terms
RFID	Radio Frequency IDentification
MPR	Multi Protocol RFID
POS	Point Of Sale

2 References

Document Title	Document#
MPR Serial Communication Manual (legacy version)	041300
MPR Communication Protocol Manual	041479

3 Physical Layer

The device will be connected to the host via RS-232. It will be a three-wire connection (TX, RX and GD) with 57600, 8, N, 1 as the default setting.

- Baud Rate: 57600
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

4 Data Link Layer/Communication Packet

This section describes the data link layer of the protocol. In particular it provides sufficient information to describe how devices should implement the data transmission mechanism in order to provide reliable communications of data via communication packets (request or response) for which the structure is defined below.

4.1 Packet Structure

The packet structure is shown below:

LEN (1)	TYPE (1)	CMD (1)	DATA (variable)	CHECKSUM (2)

Where

- LEN – Total number of bytes in packet
- TYPE – Command type: commands are categorized into system (0x00), tag type specific (0x20).
- CMD – Command code, i.e., command ID within the command category.
- DATA – Data (if any) of variable length depending on the CMD.
- CHECKSUM – CRC-16.

For example, the "RF Power ON" system command should be issued as "05 00 05 xx xx" where "05" in the 1st byte denotes the total bytes in packet, "00" in the 2nd byte the command's type: system, "05" in the 3rd byte the command id. The final 2 bytes are placeholders for CRC. See section 5.1 for command details.

4.2 Checksum Algorithm

The checksum is calculated as follows:

Transmit Link:

CRC Definition:

CRC Type	**Length**	**Polynomial**	**Preset**	**Residue**
CCITT 16	16 bits = 2 bytes	0x1021	0xFFFF	0

Receive Link:

CRC Definition:

CRC Type	**Length**	**Polynomial**	**Preset**	**Residue**
CCITT 16	16 bits = 2 bytes	0x1021	0xFFFF	0xFFFF

The user can use the same routine to do the CRC generate and check. The result for received packet check should be 0xFFFF when input the whole received packet.

Example C program (for transmit):

```
//*****************************************************************************************
unsigned int CRC_Check(unsigned char *ary,unsigned char len)
{
  unsigned int crc;
  unsigned char i,j;

  crc = 0xFFFF;

  for(i=0;i<len;i++,ary++)
          {
          crc = ((unsigned int)*ary << 8) ^ crc;
          for(j=0;j<8;j++)
                  {
                  if(crc & 0x8000)
                          crc = (crc << 1) ^ 0x1021;
                  else
                          crc <<= 1;
                  }
          }

  return (crc ^ 0xFFFF);

}
//*****************************************************************************************
```

Example:
Forward packet:
IN: 0x05, 0x00, 0x00
Out: 0xD8, 0x93

Received packet:
IN:
Out:

4.3 Poll Response

The protocol is poll-response only and therefore half-duplex. The MPR device will respond with 0x00 or 0xFF after it receives the complete command packet. The maximum delay the host has to wait for the response is about 100 ms.

5 Message Layer

This section describes all the commands that can be issued via RCSP packets. They are categorized (or typed) into System, tag type (protocol) specific and multi-protocol. Examples are shown in hexadecimal and include an xx in the placeholder CRC bytes.

If data in a response message are for multiple tags, 1 tag's worth of data per packet are returned. Data exceeding the length of the packet are truncated.

All commands should expect an acknowledgement from the PCB-915RM-SD, some should also expect (a) subsequent response(s). These are noted in the description for each of the commands in sub-sections that follow.

The *Stop* command is applicable to those commands that repeatedly execute and/or generate multiple, continuous responses (see Appendix in section 6.1). Applicable command are *Read Single Tag ID* and *Write Memory* which takes a *TryTimes* parameter.

A response packet follows the same structure definition as illustrated in section 4.1 for a request command: 1st byte the number of bytes in response, 2nd byte the command type (system or protocol/tag type, e.g., 0x20), 3rd byte the command id (e.g., 0x00 for *Read Single Tag ID* command), 4th through 3rd –from-last the tag ID/data. For responses that do not contain tag ID data, the 2nd byte is 0xFF indicating that this is (just) a *message* (i.e., no *data*), e.g., “06 FF 5F 00 xx xx" for the “Write Success” result of the ePC C1 Gen 2 *Write Memory* command.

5.1 Stop Command

Before listing commands of System and tag type specific categories, the *Stop* command is described due to the fact that it does not exactly fall into either category. It should be noted that Stop is the only command the PCB-915RM-SD accepts any time (even multiple times) during operation with or without another command in execution. It therefore serves as a simple way to verify the basic well being of communication with the PCB.

Issuing the *Stop* command is a required step to terminate those commands that repeatedly execute and/or generate multiple, continuous responses (see Appendix in section 6.1 *Data Flow*). e.g., *Read Single Tag ID* and *Write Memory* (with a zero value specified for the *TryTimes* parameter) fall into this sub-category and should be handled accordingly. For these commands[1], until a Stop is issued and responded to, their execution is not terminated and another command (system or tag type specific) should ***not*** be issued as it most likely would produce undesirable outcome due to data flow disruptions.

It is recommended that applications on exiting always check if there's any ongoing continuous tag reading activity and issue the essential Stop command if so before the actual exit.

Stop (0x00)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	00	00

This one-byte (0x00) command is issued to stop the reader from executing and sending any more data generated by the previously issued command.

Example:
Command: 00

ACK: 00

Response: None

[1] Also, a second Stop is advisable in these circumstances where the 1st Stop functions as described above and the 2nd Stop ensures RF power's being turned off. By the same token, a good practice is to issue a Stop command after every command execution especially before a subsequent tag read/write command as it basically achieves the tag re-set effect.

5.2 System Command (0x00)

Firmware Version (0x00)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	05 00 00 xx xx	00 or FF 17 00 00 55 53 30 2D 56 31 2E 33 30 2D 31 30 2E 30 31 2E 53 31 xx xx

Example:
Command: 05 00 00 XX XX

ACK: 00 – Command received correct
FF – Command received error

Response: 17 00 00 55 53 30 2D 56 31 2E 33 30 2D 31 30 2E 30 31 2E 53 31 xx xx
Where:
55 53 30 2D 56 31 2E 33 30 2D 31 30 2E 30 31 2E 53 31
- Version Identification

In this example the result is “US0-1.30-10.01.S1”

Temperature (0x01)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	05 00 01 xx xx	00 or FF 07 00 01 01 1D xx xx

This is the command to get the temperature[2] reading of PCB-915RM-SD in centigrade.

Example:
Command: 05 00 01 XX XX

ACK: 00 – Command received correct
FF – Command received error

Response: 07 00 01 01 1D xx xx where the 4th byte is Temp1 and 5th byte Temp2 and the temperature reading should be calculated as follows:

When Temp1 is less than 255 (0xFF) the resulting reader temperature should be (Temp1*256 + Temp2)/10 (yields to 28 degrees Celsius from this response)

If Temp1 is a negative value the resulting reader temperature should be –((256 – Temp2) / 10)

[2] This refers to temperature of the embedded module and is ok to be higher (e.g., by 20°C) than what's documented in reader's installation/user manual (sec 2) for (the upper limit of) the operating (ambient) temperature.

RF Power ON (0x05)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	05 00 05 xx xx	00 or FF

This is the command to turn on the RF Power of the PCB-915RM-SD. There is no need to explicitly turn on the RF power before issuing a Read or Write command which automatically turns on the RF power. This command is only useful in generating CW.

Example:
Command: 05 00 05 XX XX

ACK: 00 – Command received correct
FF – Command received error

Response: No

RF Power OFF (0x06)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	05 00 06 xx xx	00 or FF

Example:
Command: 05 00 06 XX XX

ACK: 00 – Command received correct
FF – Command received error

Response: No

Reader Status (0x0B)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	05 00 0B xx xx	00 or FF 19 00 0B 00 24 00 09 01 FF FF FF FF FF FF FF FF FF FF 04 04 FF FF 00 xx xx

This is the command to retrieve current system settings for the reader. All except for protocol data rate and frequency related fields are user settable. It should be noted that the same command applies to all of AWID's MPR devices and some fields are therefore not relevant to PCB-915RM-SD.

Example:
Command: 05 00 0B XX XX

ACK: 00 – Command received correct
FF – Command received error

Response: 19 00 0B 00 24 00 09 01 FF FF FF FF FF FF FF FF FF FF 04 04 FF FF 00 xx xx
Where:
00 24 00 09 01 FF FF FF FF FF FF FF FF FF FF 04 04 FF FF 00 - Status

Byte 1: RF Power On/Off
0x00 – Off
0x01 – On

Byte 2: Protocol Data Rate
Bit 0 – N/A
Bit 1 – N/A
Bit 2 – N/A
Bit 3 – N/A
Bit 4 – N/A
Bit 5 – ePC C1 Gen 2
0: 40k
1: 160k
Bit 6 – N/A
Bit 7 – N/A

Byte 3: Region Code for Operation Frequency Band[3]
0x00 - 902~928 America[4]
0x01 - 902~928 US 2
0x02 - 922~928 Taiwan
0x03 - 920~925 Singapore, Thailand, Hong Kong

[3] See http://www.gs1.org/docs/epcglobal/UHF_Regulations.pdf for up-to-date definitions.
[4] Argentina, Canada, Chile, Costa Rica, Dominican Republic, Mexico, Peru, Puerto Rico, United States, Uruguay.

0x04 - 910~914 Korea
0x05 – 920~925 China
0x06 – 919~923 Malaysia
0x07 – Reserved
0x08 - 920~926 Australia
0x09 – 915.4~919 South Africa
0x0A – 902~907.5 Brazil 1
0x0B – Reserved
0x0C – Reserved
0x0D – 915~928 Brazil 2
0x0E – N/A
0x0F – N/A
0x10 – 952~954 Japan (High)
0x11 – 952~955 Japan (Low)
0x12 – 922~926 Taiwan 3

Byte 4: Frequency Index Number – frequency table index currently hopped to/at
0x00 ~ 0x32

Byte 5: Frequency Hopping Status – whether frequency hopping is on
0x00 – Fixed
0x01 – Hopping

Byte 6: N/A

Byte 7: N/A

Byte 8: N/A

Byte 9: N/A

Byte 10: N/A

Byte 11: N/A

Byte 12: N/A

Byte 13: N/A

Byte 14: N/A

Byte 15: N/A

Byte 16: RF Power level setting

0x00 ~ 0xFF

Byte 17: N/A

Byte 18: ePC C1 Gen 2 Channel I sensitivity setting
0x00 ~ 0xFF

Byte 19: ePC C1 Gen 2 Channel Q sensitivity setting
0x00 ~ 0xFF

Byte 20: N/A

Antenna Select (0x0D)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	06 00 0D Number xx xx	00 or FF

This command can be issued to specify which of the two (2) antennae is selected for use. By default Antenna 1 is selected.

Number: 01 or 02

Example:
Command: 06 00 0D 02 xx xx

RF Power Level Control (0x12)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	06 00 12 Index xx xx	00 or FF

This is the command to control reader's RF Power Level. PCB-915RM-SD has an adjustable Output Power range of 20 dB. The *Index* (for *Output Attenuation*[5]) in this command is a one-byte value ranging from 0x00 to 0xFF that can be specified for the adjustment/control. The Output Power decreases when the Index value increases. All subsequent tag Read/Write operations will use this setting until re-set

Example:
Command: 06 00 12 00 xx xx – Maximum Output Power
06 00 12 FF xx xx – Minimum Output Power

ACK: 00 – Command received correct
FF – Command received error

Response: No

[5] Thus a value of zero (0) means no attenuation yielding maximum output power and 255 is maximum attenuation for minimum output power.

Soft Reset (0x80)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	05 00 80 xx xx	00 or FF

Upon receiving this command, in one second PCB-915RM-SD will reset itself by clearing all buffers and start from the beginning.

Example:
Command: 05 00 80 XX XX

ACK: 00 – Command received correct
FF – Command received error

Response: None

5.3 EPC Class 1 Generation 2 Command (0x20)

Read Single Tag ID (0x00)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	05 20 00 xx xx	00 or FF 15 20 00 30 00 30 00 21 41 60 C0 04 00 10 00 01 15 yy yy xx xx or, 11 20 00 20 00 30 00 21 41 60 C0 04 00 yy yy xx xx

This command provides the ability to read single ePC Class 1 Gen 2 tag ID in the reading field.

Example:
Command: 05 20 00 XX XX

ACK: 00 – Command received correct
FF – Command received error

Response: 15 20 00 30 00 30 00 21 41 60 C0 04 00 10 00 01 15 yy yy xx xx
Where:
30 00 21 41 60 C0 04 00 10 00 01 15 – ePC Number
30 00 (preceding ePC number) – Protocol Code (PC)
yy yy – tag CRC bytes
or,

11 20 00 20 00 30 00 21 41 60 C0 04 00 yy yy xx xx
Where:
30 00 21 41 60 C0 04 00 – ePC Number
20 00 (preceding ePC number) – Protocol Code (PC)
yy yy – tag CRC bytes

This command will repeat until user sends a STOP command (0x00)

Sensitivity Control (0x07)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	07 20 07 00 SensitivityLevel xx xx	00 or FF

This is the command used to set Sensitivity for the selected protocol (ePC Class1 Gen 2. This sensitivity control allows for increasing or decreasing the Receiver[6] detection threshold, to enhance sensitivity (more susceptible to ambient noise) or to decrease sensitivity with improved noise immunity.

Example:
Command: 07 20 07 00 FF xx xx – maximum sensitivity

07 20 07 00 00 xx xx – minimum sensitivity

ACK: 00 – Command received correct
FF – Command received error

Response: No

[6] This receiver uses quadrature I/Q channels. I/Q sensitivity is the detection threshold for each. Once issued, the command causes sensitivity levels for both channels to be set. It should be noted that changing to other value from system default for this setting is *unnecessary* for tag reading operations though sometimes useful in a printer application.

Read Memory (0x1D)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	08 20 1D MemoryBank WordAddress WordCount xx xx	00 or FF 1A 20 1D 11 11 11 11 11 11 11 11 11 11 22 22 22 22 00 00 52 16 D3 A1 00 xx xx

This command provides the ability to read data of specified word length from the specified location in the specified memory bank of an ePC Class 1 Gen 2 tag in reading field. The command continuously executes until data is located (and responded with) or a Stop command is received.

MemoryBank: 1-byte specification of memory bank from which data will be retrieved. 0x00 for Reserved, 0x01 EPC, 0x02 TID or 0x03 for User Data.

WordAddress: 1-byte number 0x00 ~ manufacturer's limit for identifying user memory location to retrieve data from.

WordCount: 1-byte number 0x01 ~ manufacturere's limit[7] for specifying length (in no. of *word*s) of data to read

Example:
Command: 08 20 1D 01 02 0F XX XX
Where:
01 – memory bank 1 for ePC Number
02 – starting word address
15 – 15 words (30 bytes) of data to be retrieved

ACK: 00 – Command accepted
FF – Command received in error

Response: 23201D1122334455667788990011223344556677889900112233445566778899 00XXXX
where starting at the 4th byte is a 240-bit (i.e., 30 bytes or 15 words) ePC Number previously written

Command: 08 20 1D 03 00 08 XX XX
Where:
03 – memory bank 3 for user data
00 – starting word address, 1st word

[7] A reasonable value has to be specified to ensure of retrieval. e.g., if WordCount is > 6 and ReadMemBank is 1 then the reader will simply time out. For User data (ReadMemBank=3) up to 25 words can be retrieved in one command execution.

08 – 8 words (16 bytes) of data to be retrieved

ACK: 00 – Command accepted
FF – Command received error

Response: 1A 20 1D 11 11 11 11 11 11 11 11 11 22 22 22 22 00 00 52 16 D3 A1 00 xx xx
Where user data of 10 bytes (5 words) of 22's and 4 bytes (2 words) of 44's were previously written[8].

[8] After shifting data should be 22 22 22 22 22 22 22 22 22 22 44 44 44 44 00 00 A4 2D A7 42; in response before shifting, 16 D3 were the "handle" bytes, A1 00 tag CRC's and byte preceding handle (w/ value 52) was used up by shifting.

Write Memory (0x5F)

FROM	TO	MSG Example	ACK/RESPONSE Example
Host	Reader	NN 20 5F MemoryBank WordID WordCount DataWords TryTimes xx xx	00 or FF 06 FF 5F 00 xx xx 06 FF 5F 10 xx xx 06 FF 5F 80 xx xx 06 FF 5F FF xx xx

This command provides the ability to write data starting at the specified word position within the specified memory bank of an ePC Class 1 Gen 2 tag. The command is issued to write at least one or more (16-bit) word(s). Packet length is therefore dependent on how many words are to be written.

NN: 1-byte packet length, value depending on how many data words are to be written, i.e., NN = 9 + 2*WordCount

MemoryBank: 1-byte specification of whether the Write occurs in Reserved (0x00), EPC (0x01), TID[9] (0x02) or User Memory (0x03)

WordID: 1-byte word number identifying position (or address) within memory bank to start writing at, 0[10] denotes 1st word

WordCount: 1-byte specification of the number of 16-bit words[11] to be written. If WordCount=0x01, the tag shall write a single data word.

DataWords: the 16-bit words to be written and shall be 16xWordCount bits in length.

TryTimes: 0x00 – Repeat until write success or user sends a STOP command (0x00)

0x01~0xFF – Repeat until write success or counter reaches the specified number of tries

Example:
Command: 0F 20 5F 01 02 03 11 22 33 44 55 66 00 XX XX
Where:

[9] Depending on tag manufacturer's policy, this area may be locked and not writable.
[10] It should be noted that when writing in MemoryBank 01 (EPC), one should start writing at WordID=02 since 00 and 01 are used by (tag) CRC and PC and had better not be overwritten.
[11] Up to 20 words (e.g., User data) are supported.

01 – to write in EPC area
02 – to write starting at the 3rd word
03 – to write 3 words
11 22 33 44 55 66 – 3-word (48-bit) data to write
00 – try times

ACK: 00 – Command received correct
FF – Command received error

Response:

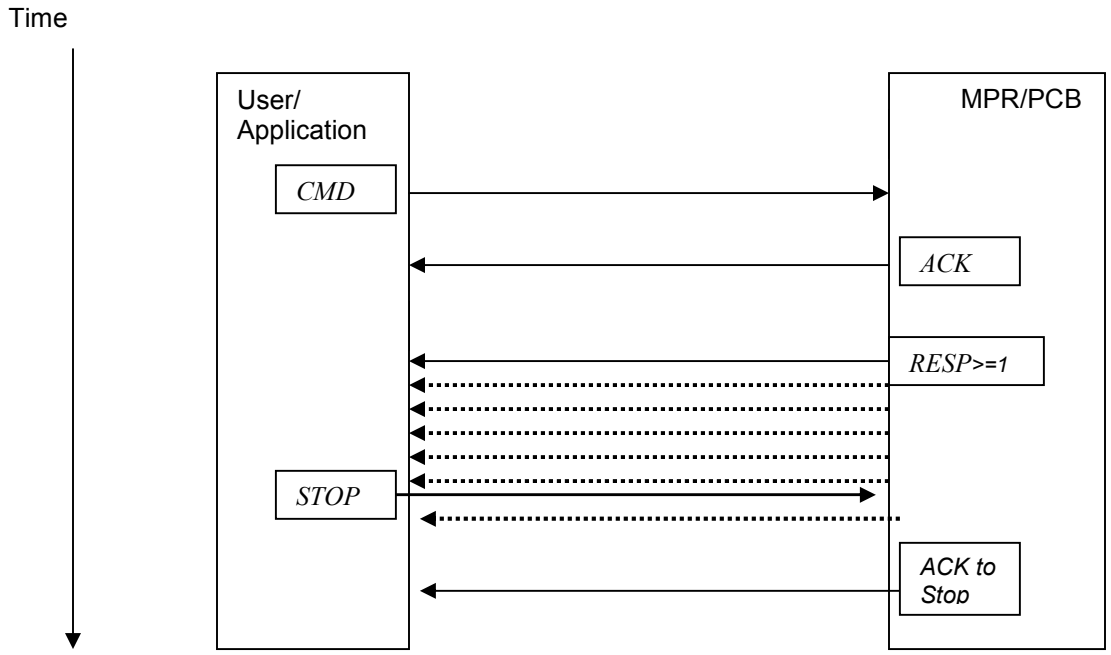
06 FF 5F 00 XX XX – Write Success
06 FF 5F 10 XX XX or 06 FF 5F FF XX XX – Write Fail
06 FF 5F 80 XX XX
– WriteTime-Out when TryTimes is 0x01~0xFF

6 Appendix

6.1 Data Flow

Included in this section are diagrams illustrating possible exchanges between an application and the MPR device.

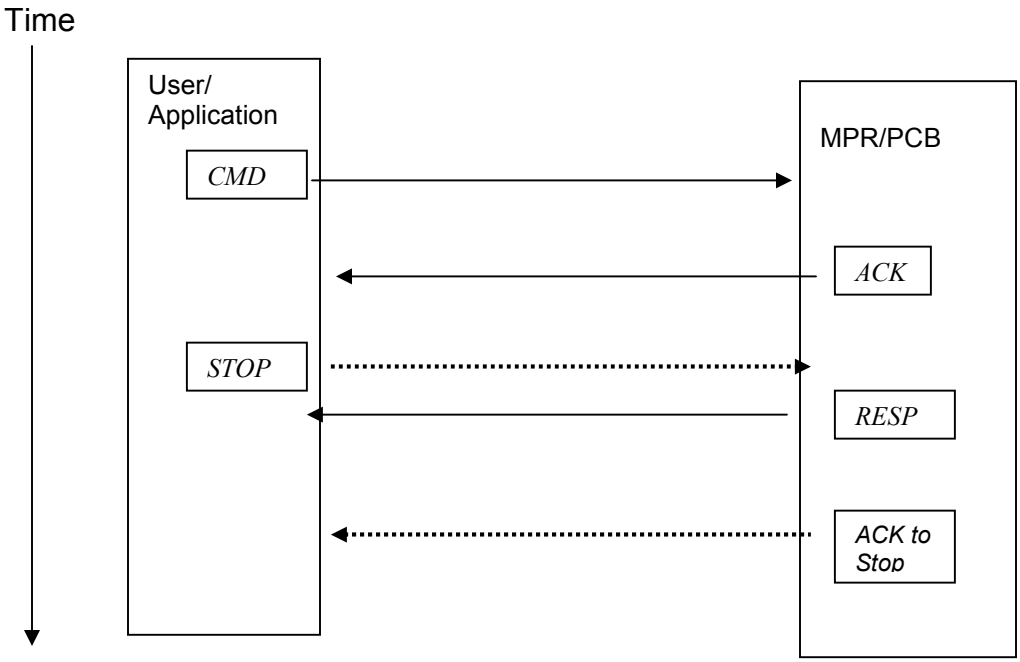
(1) Commands that repeatedly execute and generate continuous, multiple responses until STOP is received. (*Read Single Tag ID*)



It should be noted that after an extensive, long period of execution of such a command, response data may sometimes get out-of-sync[12]. So some re-synchronization and recovery of data may be necessary for some applications. In addition to check for valid response packet length (1st byte) and calculate the Receive Link CRC's (sec. 4.2), command code that's supposed to be the 3rd byte in packet and/or protocol code (2nd byte in packet) if applicable.

[12] This is more likely in TCP/IP networks.

(2) Commands that repeatedly execute (and generate 1 response of either tag ID data or execution result message) until STOP is received or timed out (*Write Memory w/ zero-valued TryTimes*)



6.2 Messages Responses

For those responses that do not contain tag data (i.e., tag ID or user data), they are categorized as (the non-data) *Messages* that provide the status/result of a command execution. For such a *Message* response, the 2nd byte in the packet is always FF, the 3rd byte is as usual the command id, starting at the 4th byte, there can be one or more of the status byte. The table below summarizes these.

Status Byte Value	*Definition*	*Command Example*
00	Success	
10	Fail	Write Memory
80	Time-Out or User Stop	(commands w/ “tryTimes”) Write Memory
FF	Fail	Write Memory