Application Note AN001:

GeoS-3/3M® FW Update Procedure in Embedded Applications

R&D Center “GeoStar navigation” Ltd.

Moscow, 2012

Table of Contents

List of Figures

Scope

The document presents description of firmware (FW) update procedure for GeoS-3/3M modules in embedded applications. All descriptions below apply to both GeoS-3 and GeoS-3M modules without any limitations.

FW update of GeoS-3 module installed in Evaluation Board and GeoS-3M module installed in Demo Board can be done with the use of **GeoSDemo3®** software.

1. Introduction

FW update is performed on any receiver's serial port (Port #0 or Port #1) which is working on binary protocol. Serial port baud rate should be at least 19200 bit/s; recommended value is 115200 bit/s. For 115200 bit/s, the update procedure takes about 20 seconds.

FW update file has following format: *geos3_XXX.bin*. The file can be downloaded from www.geostar-navigation.com.

Update file has fix size of 57344 of 32-bit words, or 224KB. The significant part of the file has variable length, and the rest part is complemented with 0xFF.

2. Serial Port Connection Options

There are three options of serial ports communication between HOST and GeoS-3 receiver (Figure 1):

1. Both serial ports are used: the first serial port is set to binary protocol and second one is set to NMEA. Data protocol assignment to serial port number does not matter
2. Single serial port is used (#0 or #1): data protocol is binary
3. Single serial port is used (#0 or #1): data protocol is NMEA.

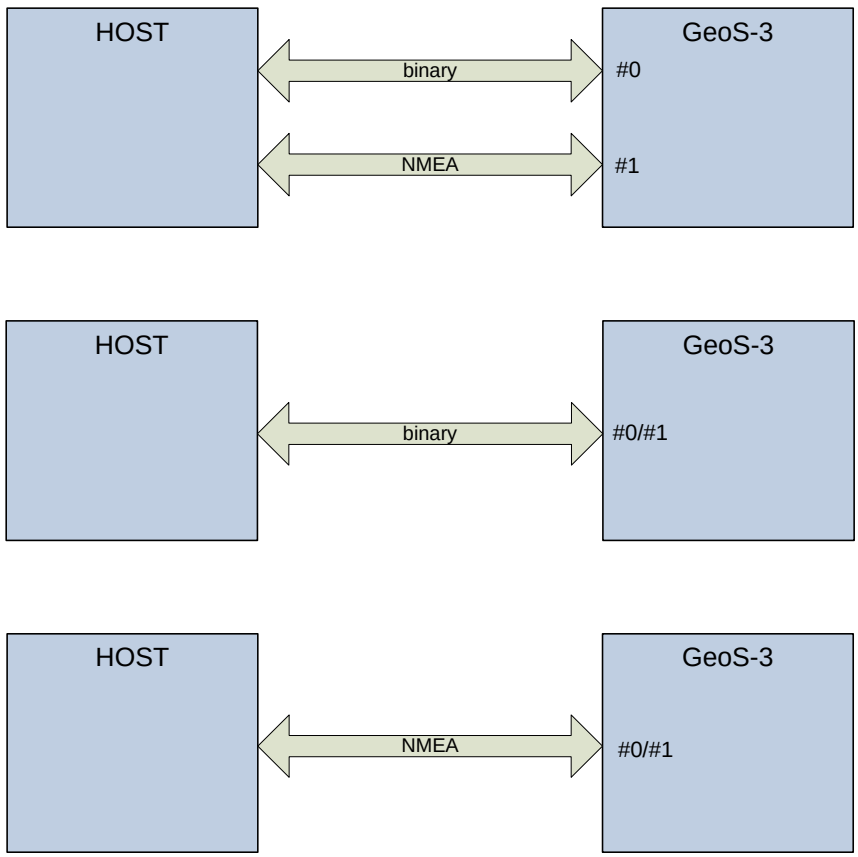

Figure 1: Serial Port Connection Options

3. Update Procedure Description

For options 1 and 2, the procedure includes four steps as follows:

1. Data integrity check
2. Switching receiver to FW update mode
3. Transferring data to the receiver
4. Activating updated FW.

For option 3, two extra steps are necessary so the procedure includes totally six steps as follows:

1. Switching the receiver from NMEA to binary
2. Data integrity check
3. Switching the receiver to FW update mode
4. Transferring data to the receiver
5. Activating updated FW
6. Switching the receiver back from binary to NMEA.

3.1. Data Integrity Check

Data flow diagram of this stage is depicted in Figure 2:

- ArDtUpd[0…57343]: data array consisting of 57344 elements (32-bit words)
- ArDtUpd[0]: first 32-bit word is the file ID (0x5F7D4BC2)
- ArDtUpd[1]: second 32-bit word is the size of significant part of the file (bytes)
- ArDtUpd[2]: third 32-bit word is checksum. Checksum is calculated as a bitwise XOR of all 32-bit words of significant part of the data array: the first word is ArDtUpd[3] and length is defined in ArDtUpd[1]. Please note that ArDtUpd[1] should be divided by four because it is specified in bytes while the procedure works with 32-bit words
- ArDtUpd[4]: fifth 32-bit word is 0xEAFFFFFE.

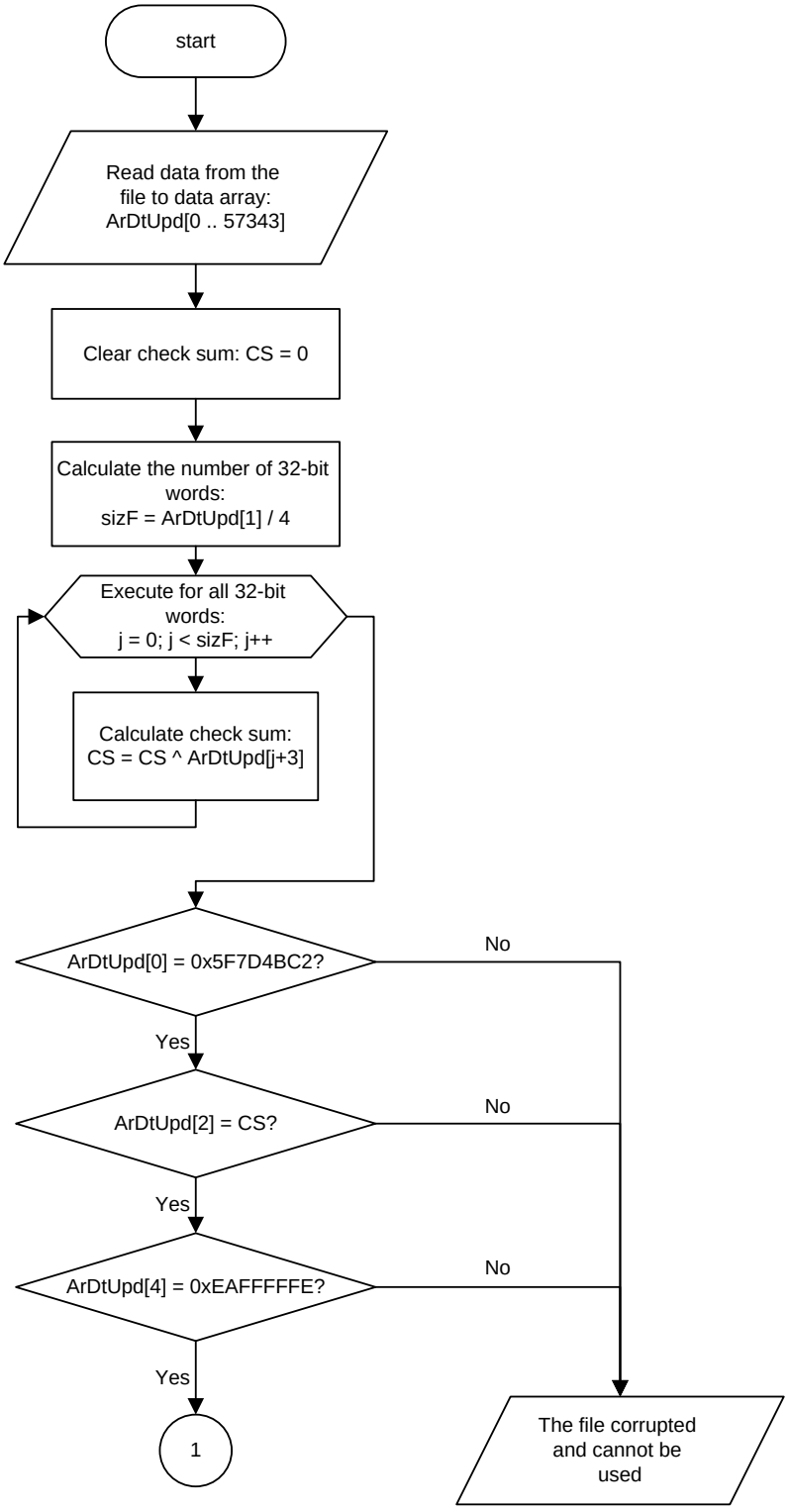

Figure 2: Data integrity block diagram

After reading out data from update file, calculate check sum. Calculated check sum should coincide with ArDtUpd[2]. Moreover, ArDtUpd[0] should be 0x5F7D4BC2 and ArDtUpd[4] should be 0xEAFFFFFE.

3.2. Switching the Receiver to FW Update Mode

Data flow diagram of this stage is depicted in Figure 3.

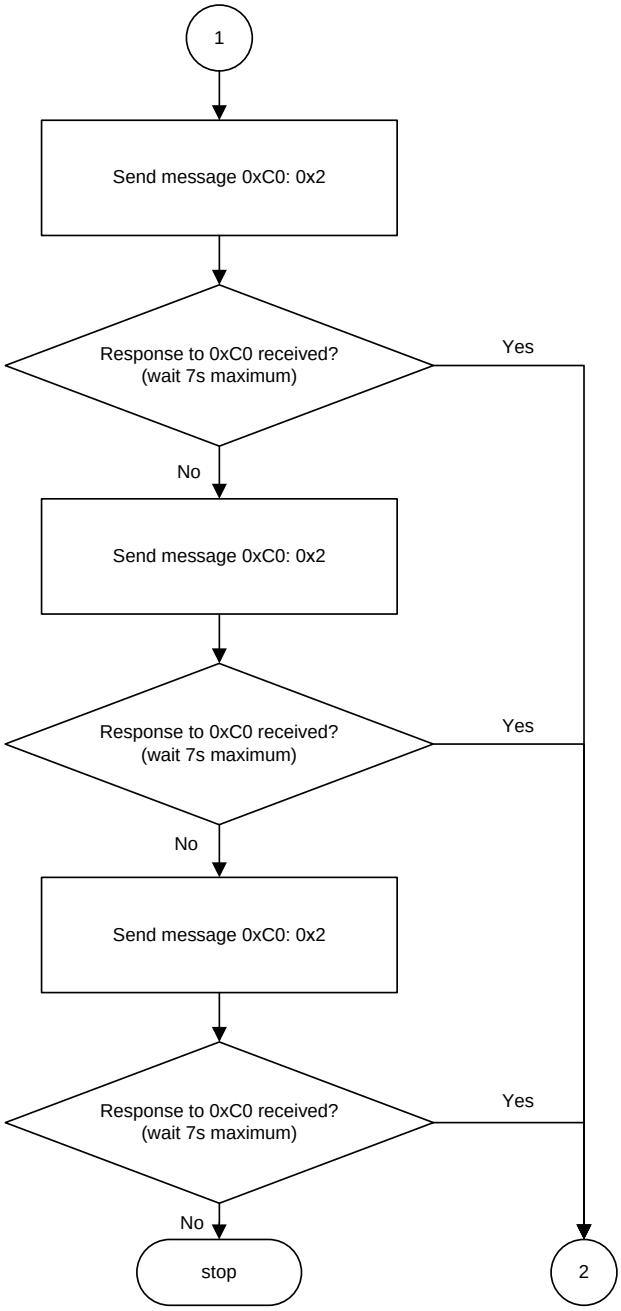

Figure 3: Switching to FW update mode block diagram

Release 0xC0 message with 0x2 parameter. As soon as the message has been received, the receiver acknowledges to the HOST by sending back 0xC0 message. If the HOST does not receive the response within 7 seconds, repeat sending 0xC0 message again three times. In case of all attempts are failed, stop the procedure and check the integrity of hardware connections.

3.3. Transferring Data to the Receiver

Data flow diagram of this stage is depicted in Figure 4.

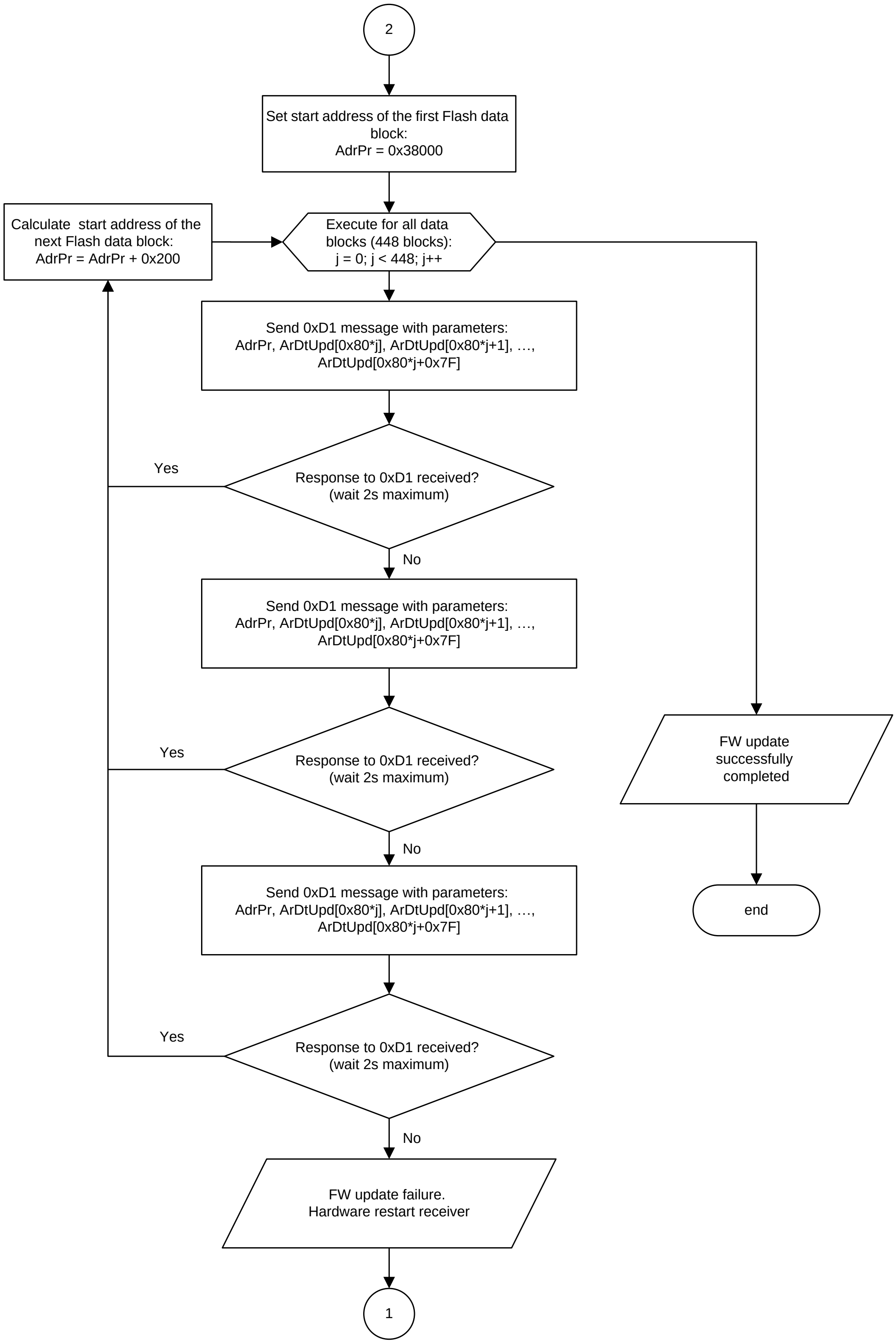

Figure 4: Transferring data block diagram

Divide the data array into 448 blocks of 128 32-bit words (512 bytes) each. Use 0xD1 message to transfer data block to the receiver. Start address of the first data block in the Flash memory is 0x38000; it is incremented by 0x200 for every other data block. Transferring data block is considered OK if the receiver acknowledges to the HOST by sending back 0xD1 message: this means that the receiver has received the data block and stored it in the Flash memory. If the HOST does not receive the response to current data block within 2 seconds, repeat sending 0xD1 message again three times. If all attempts are failed, release hardware restart and begin procedure over again.

The stage is considered successfully finished once the HOST has transferred all 448 data blocks and received related acknowledges.

3.4. Activating Updated FW

To activate updated FW, please do following:

1. Hardware restart the receiver
2. Release program cold start by using 0xC2 message with 0x3 parameter.

Hardware restart can be done in one of the following ways:

1. NRESET=0 → NRESET=1. Logic low duration should be at least 100ns
2. ON/OFF=0 → ON/OFF=1. Logic low duration should be at least 1ms.

3.5. Switching between NMEA and Binary Protocols

3.5.1 Switching from NMEA to Binary Protocol

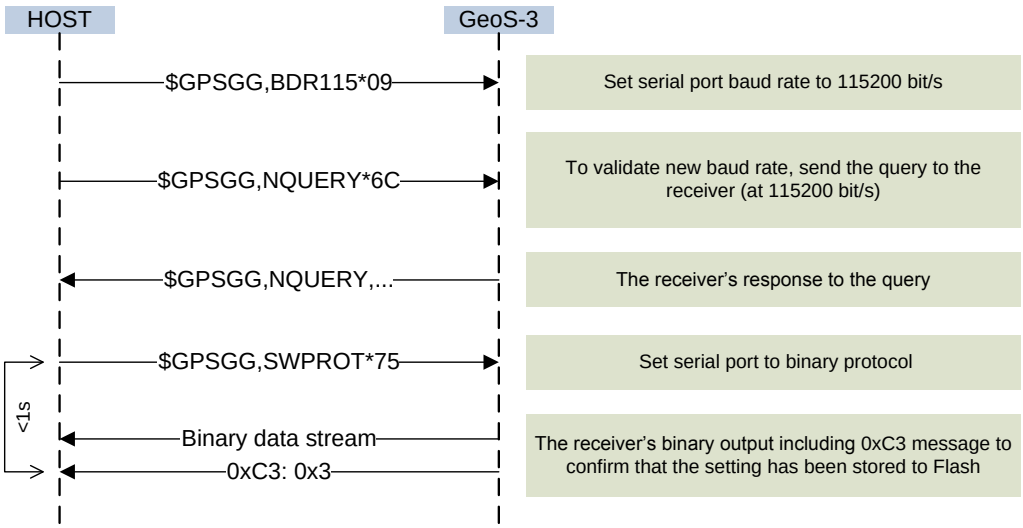

Figure 5: Switching from NMEA to binary protocol

To set 115200 bit/s baud rate, release $GPSGG,BDR115. In order to check that the baud rate has been set correctly, $GPSGG,NQUERY can be sent to the receiver. In response to this query, the receiver returns $GPSGG,NQUERY,… message.

To switch to binary protocol, release $GPSGG,SWPROT. The receiver doesn't reply any acknowledgement to this message and starts transmitting binary messages. Within 1 second the receiver will output 0xC3 message with 0x3 parameter which acknowledges that the setting has been stored to Flash. This indicates that switching to binary protocol has been successfully completed.

3.5.2 Switching from Binary Protocol to NMEA

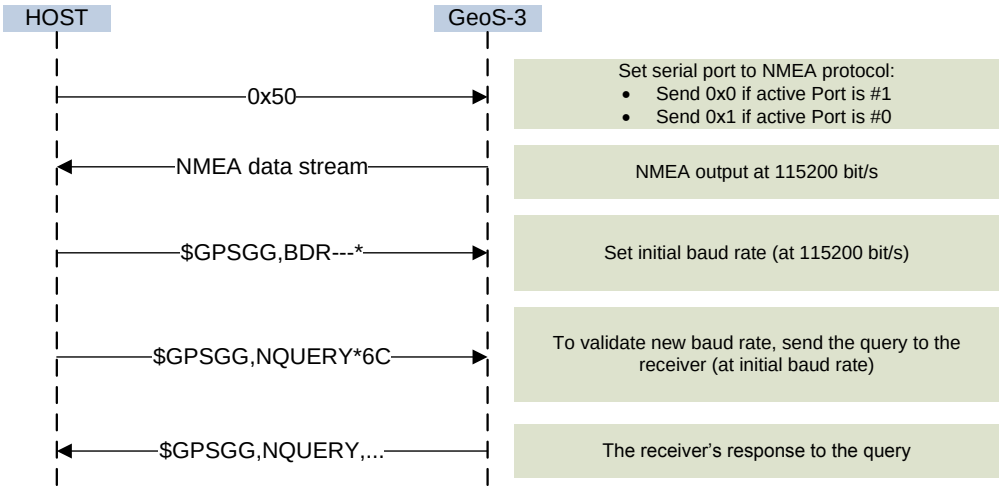

Figure 6: Switching back from binary to NMEA protocol

The receiver is switched back from binary protocol to NMEA with 0x50 message:

- Send 0x0 parameter if active Port is #1
- Send 0x1 parameter if active Port is #0.

The receiver doesn't reply any acknowledgement to this message and immediately starts transmitting NMEA messages at 115200 bit/s.

To restore new (initial) baud rate, release $GPSGG,BDR---, where "---" fields correspond to new baud rate. Please note that the message should be sent at 115200 bit/s.

In order to check that the baud rate has been set correctly, $GPSGG,NQUERY can be sent to the receiver. In response to this query, the receiver returns $GPSGG,NQUERY,… message.

4. Appendix A. Dedicated Binary Messages Description

4.1. 0xC0: Change Operation Mode, Response to Change Operation Mode

Message length (words): 1.

Word #	Type	Units	Parameter
1	u_int		Mode: 0: normal 1: test mode (on simulator) 2: FW update 3: operation with Flash memory

Example:

534F4547 53503372: preamble

000100C0: message ID – 0xC0, length – 1

00000000: data

001E76F5: check sum

4.2. 0xD1: Set Data Block for Programming Flash

Message length (words): 129.

Word #	Type	Units	Parameter
1	u_int		Start address of programmed block in Flash memory
2			1st word of data block
3			2nd word of data block
.....			
129			129th word of data block

Example:

534F4547 53503372: preamble

008100D1: message ID – 0xD1, length – 129

0000CA00 E59D3048 E1A02005 E1A0000A E1A0100B EB005637 E1A02007 E1A03008 EB005634 E1A09000 E28DC008 E58D1018 E89C0003 E59D304C E1A02006 EB00562D E59D3018 E1A02009 EB00544D E28D2030 E8820003 E28D9020 E899000C E1A0000A E1A0100B EB005623 E28D2018 E8820003 E1A0C000 E1A09001 E28D2038 E8920003 E2842F86 E8820003 E28D2030 E8920003 E2842E22 E8820003 E28D2018 E8920003 E2842F8A E8820003 E1A01009 E28D9080 E899000C E1A0000C EB00560E E1A09000 E28DC010 E58D1050 E89C0003 E1A02007 E1A03008 EB005607 E28D2028 E8820003 E28DC008 E89C0003 E89D000C EB005601 E28DC028 E89C000C EB005421 E59D3050 E1A02009 EB0057A6 E59D304C E1A02006 EB0055F8 E1A09000 E58D1028 E1A02007 E1A03008 E1A0000A E1A0100B EB0055F1 E89D000C EB0055EF E28DC040 E89C000C EB00570F E59D3048 E1A02005 EB0055E9 E59D3028 E1A02009 EB005791 E58D0058 E28DC020 E89C000C E1A09001 E1A0000A E1A0100B EB0055DF E28DC080 E89C000C EB0055DC E28DC050 E88C0003 E28DC010 E89C0003 E1A02007 E1A03008 EB0055D5 E28D2028 E8820003 E28DC008 E89C0003 E89D000C EB0055CF E28DC028 E89C000C EB0053EF E28DC050 E89C000C EB005774 E59D3048 E1A02005 EB0055C6 E1A05000 E58D1008 E1A02007 E1A03008 E1A0000A E1A0100B EB0055BF E89D000C EB0055BD E28DC040: data

0D3732FD: check sum

4.3. 0xD1: Response to Set Data Block for Programming Flash

Message length (words): 1.

Word #	Type	Units	Parameter
1	u_int		Start address of programmed block in Flash memory

Example:

534F4547 53503372: preamble

000100D1: message ID – 0xD1, length – 1

0000CA00: data

001EBCE4: check sum