NSP Bootloader for Sinclair Interplanetary Hardware
Rev 1.2
September 5 2008

1 Scope

This document describes how to use the NSP bootloader software that is found on a number of Sinclair Interplanetary spacecraft components. These include reaction wheels and sun sensors that are not configured for CAN communications. Sinclair Interplanetary devices that do not permit on-orbit code modification, such as the battery charge/discharge regulator, do not use this bootloader.

2 Overview

The NSP bootloader is a small, reliable piece of software that is loaded into the device in the factory. It is started whenever the device processor is reset.

The bootloader allows NSP communications over an appropriate link. It allows the user to load new application software into the device, or to validate existing application software. Finally, it allows the user to execute application software. While the application software executes the bootloader remains running in the background providing continued NSP communications.

Very careful effort has gone into protecting the bootloader from damage. While it can be used to load and modify application software, the bootloader cannot change itself. Nor can application software modify the bootloader. There should be no way to "brick" the device with a badly chosen command.

3 NSP Module Commands

The NSP bootloader interprets incoming telecommands. The command code section of the message control field is compared to the following table of known commands:

0x00	PING
0x01	INIT
0x02	PEEK
0x03	POKE
0x04	TELEMETRY
0x06	CRC
0x07	APPLICATION-TELEMETRY
0x08	APPLICATION-COMMAND

If the command code is unknown (and if the poll bit is set) then a reply is generated with a NACK and no further processing is performed. Otherwise the command is executed as shown in the following sections.

3.1 PING Command (0x00)

The PING command is typically used during testing to verify communications. Incoming data is ignored. The reply packet contains a human-readable text string containing:

- The type of device and the manufacturer
- The compile date and time of the NSP bootloader
- The name, and compile date and time of the currently running application module, if applicable.

The string is not NULL terminated.

This command is unusual in that data sent in the telecommand is lost. The reply message contains only human-readable string.

3.2 INIT Command (0x01)

The INIT command is used to change the operating mode of a device. An INIT with no data causes a complete reset of the device. It will reboot to the NSP bootloader, with no application module running. Note that if a reply has been requested ("Poll" bit set to '1') then the reset will occur after the reply transmission is complete.

An INIT command with 4 bytes of data causes the NSP bootloader to run an application module at the corresponding 32-bit start address. If an application module is already running, the request will be NAKed. A NAK will also be generated if the start address lies within the NSP module or is outside the valid memory range.

By convention, devices will ship from the factory with their primary application program stored at address 0x00001000. Thus, a command of INIT 0x00001000 will start the default behaviour.

3.3 PEEK Command (0x02)

The PEEK command is used to read the device memory. Five bytes of data are required. The first four are interpreted as a 32-bit pointer to the start of the memory to be read. The fifth byte is the number of bytes to read. A value of zero in this field will cause 256 bytes to be read. The reply message contains the start address, followed by bytes read from memory. The number of bytes to read is not echoed back.

The memory map is as follows:

Address Range	Function
0x00000000 – 0x00007DFF	32 kB Program memory (flash)
0x00010000 – 0x000107FF	2 kB XRAM (RAM)
0x00020000 – 0x000200FF	256 B IRAM (RAM)
0x00030080 – 0x000300FF	128 B SFR (RAM)

Address ranges not mentioned above are unsupported, and attempted reads will generate NAKs. The SFR space refers to the Special Function Registers of the processor. Reads to some of these registers will have consequences, and there is no guarantee that careless PEEKs will not cause unexpected software operation.

3.4 POKE Command (0x03)

The POKE command is used to write the device memory. Five or more bytes of data are required. The first four are interpreted as a 32-bit pointer to the start of the memory to be written. Each subsequent byte is then a byte to be written. A maximum of 256 bytes

may be written in a single POKE. The reply message contains all of the data from the telecommand message. The message control field will contain ACK if the write has been successful, or NAK otherwise.

The memory map is as follows:

Address Range	Function
0x00001000 – 0x00007DFF	32 kB Program memory (flash)
0x00010000 – 0x000107FF	2 kB XRAM (RAM)
0x00020000 – 0x000200FF	256 B IRAM (RAM)
0x00030080 – 0x000300FF	128 B SFR (RAM)

POKEs to flash memory are not permitted when any application module is running. Flash memory 0x00000000 to 0x00000FFF and 0x000007C00 to 0x00007DFF is reserved for the NSP bootloader and may not be written to.

Each 512 byte block of program memory has a lifetime of only 20,000 write cycles. One cycle is consumed for each POKE telecommand that accesses a particular block. This lifetime is more than sufficient for occasional software patches, but the user is cautioned that a looping sequence of POKE telecommands could easily wear out a block.

3.5 TELEMETRY Command (0x04)

The TELEMETRY command gathers telemetry from the NSP bootloader only. A TELEMETRY request has a single data byte to indicate the telemetry address. The response adds a 32-bit telemetry quantity.

Telemetry Address	Function
0	Last reset reason
1	Reset count
2	Framing error count
3	Runt packet count
4	Oversize packet count
5	Bad CRC count

All of the "count" channels are stored internally as 16-bit unsigned integers. They will wrap around to 0 after reaching 65535.

3.5.1 Last Reset Reason

The last reset reason telemetry channel indicates the reason for the most reset processor reset.

0	Power cycle
1	Realtime clock reset
2	Flash memory reset
3	Comparator0 reset
4	Watchdog timer reset
5	Missing clock reset
6	External /reset pin reset
7	INIT reset
8+	Application triggered reset

3.5.2 Reset Count

This telemetry channel counts the number of times the processor has been reset since the last power cycle. When first turned on, reset count will be zero.

3.5.3 Framing Error Count

After each reset this count is zeroed. It is incremented each time a character sequence is received that violates the SLIP framing rules (FESC must be followed by TFESC or TFEND).

3.5.4 Runt Packet Count

After each reset this count is zeroed. It is incremented each time two FEND characters are received, separated by between one to four bytes. The minimum length for a telecommand is five bytes, so these cannot be valid. Note that consecutive FEND characters do not count as runts. For a runt to be counted its first byte (the nominal destination address) must be equal to the device's NSP address or the device must use an SPI link.

3.5.5 Oversize Packet Count

After each reset this count is zeroed. It is incremented each time an incoming telecommand is determined to be too large. The NSP bootloader tolerates a maximum of 260 data bytes on incoming telecommands. Oversize packets are only counted if they are addressed to this device.

3.5.6 Bad CRC Count

After each reset this count is zeroed. It is incremented each time an incoming telecommand, addressed to this device, has a bad CRC.

3.6 CRC Command (0x06)

The CRC command is used to calculate a checksum on an area of program memory. It takes a total of eight data bytes: a 32-bit start address, and a 32-bit end address. Both addresses must be within the flash memory limits (0x00000000 – 0x00007DFF) and the start must be before the end. Failure of any of these criteria will result in a NAK reply with no data.

If successful, the return message appends a 32-bit CRC of the flash memory between the start and the end. This feature can be used to verify that a large block of program memory (bootloader or application) has not suffered any corruption.

Consult Sinclair Interplanetary for details on the polynomial and setup conditions for the 32-bit CRC.

3.7 APPLICATION-TELEMETRY Command (0x07)

Application telemetry requests are NAKed if no application program is running. Otherwise the command packet is passed to the application program which interprets it and returns an appropriate response.

3.8 APPLICATION-COMMAND Command (0x08)

Application commands are NAKed if no application program is running. Otherwise the command packet is passed to the application program which interprets it and returns an appropriate response.

4 Revision History

4.1 Rev 1.0 to Rev 1.2

Corrected erroneous correction to APPLICATION_TELEMETRY and APPLICATION_COMMAND codes.