I²C Peripheral Interface Wrapper

The I²C BSL protocol interface is implemented in multiple packets. The first packet is sent as a write request to the BSL slave address and contains the BSL Core Command and its wrapper. Table 8 shows this format.

Table 8. I²C BSL Command

I2C	Header	Length	Length	BSL Core Command	CKL	CKH
S/A/W	0x80	NL	NH	See Section 4.1.5	CKL	CKH

The second packet is sent as a read request to the BSL slave address and contains the BSL acknowledgment and the BSL Core Response. Table 9 shows the format of this BSL response.

Table 9. I²C BSL Response

I2C	ACK	Header	Length	Length	BSL Core Response[1]	CKL	CKH	I2C
S/A/R	ACK from BSL	0x80	NL	NH	See Section 4.1.4	CKL	CKH	STOP

(1) BSL Core Response is not always included.

3.1.2 I²C BSL

I2C protocol used by BSL is defined as:

- The MSP430 BSL is the slave, and the master must request data from the BSL slave.
- 7-bit addressing mode is used, and the slave address is 0x48.
- Handshake is performed by an acknowledge character in addition to the hardware ACK.
- The minimum time delay before sending new character after characters have been received from MSP430 BSL is 1.2 ms.
- Repeated starts are not required by the BSL but can be used.

4.1.4 BSL Core Response and BSL Core Message

For some commands, the BSL replies with certain BSL core response that contains single byte message on it. This 1-byte message is defined as BSL Core Message. For details about which command has the BSL core message on its response, see the Section 4.1.5 examples.

Table 11. BSL Core Response Structure (Has the BSL Core Message Byte)

CMD Byte	BSL Core Message
0x3B	Message (see Table 12)

Table 12. BSL Core Messages

Message	Meaning
0x00	Operation successful
0x01	Memory (for example, flash or FRAM) write check failed. After programming, a CRC is run on the programmed data. If the CRC does not match the expected result, this error is returned.
0x04	BSL locked. The correct password has not yet been supplied to unlock the BSL.
0x05	BSL password error. An incorrect password was supplied to the BSL when attempting an unlock.
0x07	Unknown command. The command given to the BSL was not recognized.

4.1.5 BSL Core Commands

Table 13 summarizes the BSL core commands.

Table 13. BSL Core Commands

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response	Section
RX Data Block	Yes	0x10	(AL)	(AM)	(AH)	D1…Dn	Yes	Section 4.1.5.1
RX Password	No	0x11	–	–	–	D1…D32	Device dependent	Section 4.1.5.2
Mass Erase[1]	No	0x15	–	–	–	–	Device dependent	Section 4.1.5.3
CRC Check[1]	Yes	0x16	(AL)	(AM)	(AH)	Length (low byte), Length (high byte)	Yes	Section 4.1.5.4
Load PC	Yes	0x17	(AL)	(AM)	(AH)	–	No	Section 4.1.5.5
TX Data Block	Yes	0x18	(AL)	(AM)	(AH)	Length (low byte), Length (high byte)	Yes	Section 4.1.5.6
TX BSL Version[1]	Yes	0x19	–	–	–	–	Yes	Section 4.1.5.7
RX Data Block Fast[1]	Yes	0x1B	(AL)	(AM)	(AH)	D1...Dn	No	Section 4.1.5.8
Change Baud Rate[1][2]	No	0x52	–	–	–	D1	No	Section 4.1.5.9

(1) Not supported for FR4xx, FR21xx, and FR20xx
(2) Applicable for UART peripheral interface only

AL, AM, AH

Address bytes. The low, middle, and upper bytes, respectively, of an address.

D1...Dn

Data bytes 1 through n (Note: n must be 4 less than the BSL buffer size.)

Length

A byte containing a value from 1 to 255 describing the number of bytes to be transmitted or used in a CRC. In the case of multiple length bytes, they are combined together as described to form a larger value describing the number of required bytes.

4.1.5.1 RX Data Block

Structure BSL Core Command

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
RX Data Block	Yes	0x10	(AL)	(AM)	(AH)	D1…Dn	Yes

Description

The BSL core writes bytes D1 through Dn starting from the location specified in the address fields. This command differs from RX Data Block Fast in that it returns the status of the write operation.

NOTE: When a block is written partly outside the device's memory (for example, starting to write in FRAM but exceeding the end of the memory) the whole data block will not be written.

Protection

This command is password protected and fails if the password has not been sent.

Command

0x10

Command Address

Address where the received data should be written.

Command Data

Command consists of the data D1 through Dn to be written. The command consists of n bytes, where n has maximum 256.

Command Returns

BSL acknowledgment and a BSL core response with the status of the operation. See Section 4.1.4 for more information on BSL core responses.

Example for I²C PI

Write data 0x76543210 to address 0x010000:

I2C	Header	Length	Length	CMD	AL	AM	AH	D1	D2	D3	D4	CKL	CKH
S/A/W	0x80	0x08	0x00	0x10	0x00	0x00	0x01	0x10	0x32	0x54	0x76	0x93	0xCA

BSL response for a successful data write:

I2C	ACK	Header	Length	Length	CMD	MSG	CKL	CKH	I2C
S/A/R	0x00	0x80	0x02	0x00	0x3B	0x00	0x60	0xC4	STOP

4.1.5.2 RX Password

Structure BSL Core Command

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
RX Password	No	0x11	–	–	–	D1…D32	Yes

Description

The BSL core receives the password contained in the packet and unlocks the BSL protected commands if the password matches the top 16 words in the BSL interrupt vector table (located between addresses 0xFFE0 and 0xFFFF).

When an incorrect password is given, a mass erase is initiated. For MSP430FR5xx and MSP430FR6xx devices, this means all code FRAM is erased but not information memory. For MSP430FR2xx and MSP430FR4xx devices, this means all code FRAM including the information memory is erased.

After a mass erase is performed, the password is always 0xFF for all bytes. This is commonly used to gain access to an empty device or to load a new application to a locked device without password. The mass erase security feature can be disabled by setting the BSL signatures as described in the corresponding family user's guide (see Section 1.2).

Protection

This command is not password protected.

Command

0x11

Command Address

N/A

Command Data

The command data is 32 bytes long and contains the device password.

Command Returns

The MSP430FR5xx and MSP430FR6xx bootloader does not send the BSL core response for the incorrect password. The BSL acknowledgment is either 0x00 or 0xFF. Ignore the acknowledgment and initialize the communication with BSL again.

The MSP430FR2xx and MSP430FR4xx bootloader sends the BSL acknowledgment and BSL core response with the status of operation. See Section 4.1.4 for more information on BSL core responses.

Example for I²C PI

Unlock a blank device:

I2C	Header	Length	Length	CMD	D1	D2	D3	D4	D5
S/A/W	0x80	0x33	0x00	0x11	0xFF	0xFF	0xFF	0xFF	0xFF

D6	D7	D8	D9	D10	D11	D12	D13	D14	D15
0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF

D16	D17	D18	D19	D20	D21	D22	D23	D24	D25
0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF

D26	D27	D28	D29	D30	D31	D32	CKL	CKH
0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF	0x9E	0xE6

BSL response for a successful password:

I2C	ACK	Header	Length	Length	CMD	MSG	CKL	CKH	I2C
S/A/R	0x00	0x80	0x02	0x00	0x3B	0x00	0x60	0xC4	STOP

4.1.5.3 *Mass Erase*

Structure BSL Core Command

For FR23xx, FR25xx, and FR26xx:

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
Mass Erase	No	0x15	–	–	–	–	Yes

For FR5xx and FR6xx:

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
Mass Erase	No	0x15	–	–	–	–	No

Description

All code FRAM in the device is erased. For MSP430FR5xx and MSP430FR6xx devices, this function does not erase information memory. For MSP430FR23xx, MSP430FR25xx , MSP430FR24xx, and MSP430FR26xx devices, this function erases information memory.

The BSL on the FR4xx, FR21xx, and FR20xx MCUs does not support the Mass Erase command. A RX Password command containing an incorrect password can be sent instead to trigger a mass erase.

Protection

This command is not password protected.

Command

0x15

Command Address

N/A

Command Data

N/A

Command Returns

The MSP430FR5xx and MSP430FR6xx bootloader do not send the BSL core response for the mass erase execution. The BSL acknowledgment is either 0x00 or 0xFF. Ignore the acknowledgment and initialize the communication with BSL again.

The MSP430FR2xx and MSP430FR4xx bootloader send the BSL acknowledgment and BSL core response with the status of operation. See Section 4.1.4 for more information on BSL core responses.

Example for I²C PI

Initiate a mass erase:

I2C	Header	Length	Length	CMD	CKL	CKH
S/A/W	0x80	0x01	0x00	0x15	0x64	0xA3

BSL response (successful operation):

I2C	ACK	Header	Length	Length	CMD	MSG	CKL	CKH	I2C
S/A/R	0x00	0x80	0x02	0x00	0x3B	0x00	0x60	0xC4	STOP

4.1.5.4 CRC Check

Structure BSL Core Command

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
CRC Check	Yes	0x16	(AL)	(AM)	(AH)	Length (low byte), Length (high byte)	Yes

Description

The MSP430 performs a 16-bit CRC check using the CCITT standard. The address given is the first byte of the CRC check. Two bytes are used for the length. See the CRC chapter of each family user's guide (see Section 1.2) for more details on the CRC hardware calculation that is used.

Protection

This command is password protected and fails if the password has not been sent.

Command

0x16

Command Address

Address to begin the CRC check.

Command Data

The 16-bit length of the CRC check. D1 is the low byte of the length, and D2 is the high byte of the length.

Command Returns

BSL acknowledgment and a BSL core response with the CRC value. See Section 4.1.4 for more information on BSL core responses.

Example for I²C PI

Perform a CRC check from address 0x4400 to 0x4800 (size of 1024):

I2C	Header	Length	Length	CMD	AL	AM	AH	D1	D2	CKL	CKH
S/A/W	0x80	0x06	0x00	0x16	0x00	0x44	0x00	0x00	0x04	0x9C	0x7D

BSL response where 0x55 is the low byte of the calculated checksum and 0xAA is the high byte of the calculated checksum:

I2C	ACK	Header	Length	Length	CMD	D1	D2	CKL	CKH	I2C
S/A/R	0x00	0x80	0x03	0x00	0x3A	0x55	0xAA	0x12	0x2B	STOP

4.1.5.5 *Load PC*

Structure BSL Core Command

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
Load PC	Yes	0x17	(AL)	(AM)	(AH)	–	No

Description

Causes the BSL to begin execution at the given address using a CALLA instruction. As BSL code is immediately exited with this instruction, no core response can be expected. The BSL can be returned to by the main application using the BSL Action function 2, Return to BSL. See Section 3.3.1.2 for more information.

Be aware that password protection is not active at this time. Jumping to the user application does not reset the device and, therefore, the register configuration from the BSL application is kept. This might cause unexpected behavior in the user application. One example is the blink LED application, which does not have any clock module configuration (so it uses the default 1-MHz clock) and will blink faster, because the clock module is set by the BSL application to run at 8 MHz.

Protection

This command is password protected and fails if the password has not been sent.

Command

0x17

Command Address

Address to set the Program Counter

Command Data

N/A

Command Returns

The BSL does not return acknowledgment.

Example for I²C PI

Set program counter to 0x4400:

I2C	Header	Length	Length	CMD	AL	AM	AH	CKL	CKH	I2C
S/A/R	0x80	0x04	0x00	0x17	0x00	0x44	0x00	0x42	0x0F	STOP

The BSL does not respond once the application gains control.

4.1.5.6 *TX Data Block*

Structure BSL Core Command

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
TX Data Block	Yes	0x18	(AL)	(AM)	(AH)	Length (low byte), Length (high byte)	Yes

Description

The BSL transmits data starting at the command address and with size command data. This command initiates multiple packets if the size is greater than or equal to the buffer size.

Protection

This command is password protected and fails if the password has not been sent.

Command

0x18

Command Address

Address to begin transmitting data from.

Command Data

The 16-bit length of the data to transmit. D1 is the low byte of the length, and D2 is the high byte of the length.

Command Returns

BSL acknowledgment and a BSL core response with *n* data packets where *n* is:

$$n = \text{ceiling}\left(\frac{length}{buffer\ size - 1}\right)$$

For example, if 512 bytes are requested with a buffer size of 260, the BSL sends two packets, the first packet with a length of 259 and the second with a length of 253.

See Section 4.1.4 for more information on BSL core responses.

Example for I²C PI

Transmit 4 bytes of data from RAM address 0x1C00:

I2C	Header	Length	Length	CMD	AL	AM	AH	D1	D2	CKL	CKH
S/A/W	0x80	0x06	0x00	0x18	0x00	0x1C	0x00	0x04	0x00	0x87	0x81

BSL response where D1..D4 are the data bytes requested:

I2C	ACK	Header	Length	Length	CMD	D1	D2	D3	D4	CKL	CKH	I2C
S/A/R	0x00	0x80	0x05	0x00	0x3A	0x11	0x33	0x55	0x77	0x90	0x55	STOP

4.1.5.7 *TX BSL Version*

Structure BSL Core Command

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
TX BSL Version	Yes	0x19	–	–	–	–	Yes

Description

BSL transmits its version information (see Section 3.5 for more details).

Protection

This command is password protected and fails if the password has not been sent.

Command

0x19

Command Address

N/A

Command Data

N/A

Command Returns

BSL acknowledgment and a BSL core response with its version number. The data is transmitted as it appears in memory with the following data bytes:

Version Byte	Data Byte
BSL Vendor	D1
Command Interpreter	D2
API	D3
Peripheral Interface	D4

See Section 4.1.4 for more information on BSL core responses.

Example for I²C PI

Request the BSL version:

I2C	Header	Length	Length	CMD	CKL	CKH
S/A/W	0x80	0x01	0x00	0x19	0xE8	0x62

BSL response (version 00.07.34.B2 of the BSL):

I2C	ACK	Header	Length	Length	CMD	D1	D2	D3	D4	CKL	CKH	I2C
S/A/R	0x00	0x80	0x05	0x00	0x3A	0x00	0x07	0x34	0xB2	0x14	0x90	STOP

4.1.5.8 *RX Data Block Fast*

Structure BSL Core Command

BSL Command	Protected	CMD	AL	AM	AH	Data	BSL Core Response
RX Data Block Fast	Yes	0x1B	(AL)	(AM)	(AH)	D1…Dn	No

Description

This command is identical to RX Data Block, except there is no reply to indicate that the data was correctly programmed. RX Data Block Fast is used primarily to speed up USB programming on the MSP430F5xx and MSP430F6xx family of devices.

NOTE: When a block is written partly outside the device memory (for example, starting to write in FRAM but exceeding the end of the memory), the whole data block will not be written.

Protection

This command is password protected and fails if the password has not been sent.

Command

0x1B

Command Address

Address to write the received data to.

Command Data

Command consists of the data D1 through Dn to be written. The command consists of n bytes, where n has a maximum of 256.

Command Returns

BSL acknowledgment

Example for I²C PI

Write data 0x76543210 to address 0x010000:

I2C	Header	Length	Length	CMD	AL	AM	AH	D1	D2	D3	D4	CKL	CKH
S/A/W	0x80	0x08	0x00	0x10	0x00	0x00	0x01	0x10	0x32	0x54	0x76	0x93	0xCA

BSL Response:

I2C	ACK	I2C
S/A/R	0x00	STOP

The detailed document,please see below URL

http://www.ti.com/lit/ug/slau550s/slau550s.pdf