AN 936: Executing SDM Commands via JTAG Interface
1. Executing SDM Commands via JTAG Interface

This application note provides information on using the System Console packet service to send Secure Device Manager (SDM) commands from System Console to the SDM, and to read the response from the SDM via the JTAG interface. Intel® Quartus® Prime Pro Edition software provides the System Console as a debugging tool using JTAG. When you send an SDM command using the packet service, the System Console translates the command into a lower level JTAG instruction and drives the JTAG pins accordingly.

This document serves as an extension to the Mailbox Client Intel FPGA IP User Guide, which provides details on the device family support, and SDM commands and responses. The document provides additional guidance on how to execute SDM commands via the JTAG interface.

Related Information
Mailbox Client Intel FPGA IP User Guide
1.1. Overview

The Intel FPGA implements Secure Device Manager (SDM) architecture starting with Intel Stratix® 10 devices and all future FPGA devices. The SDM consists of the triple-redundant lockstep processors and other components described in the *Intel Stratix 10 Configuration User Guide*.

You can interact with the SDM via the mailbox interface. Use any of the following interfaces to access the mailbox block in the SDM as indicated in Figure 1:

1. JTAG interface
2. HPS interface
3. FPGA core interface using soft IPs

This application note only provides information on accessing the SDM via the JTAG interface.

For information on accessing the SDM from the FPGA core interface, refer to the *Mailbox Client Intel FPGA IP User Guide*.

The figure below is a block diagram of the Secure Device Manager hardware, showing the various interfaces the SDM can use to communicate with devices.

![SDM Block Diagram](image)

**Related Information**

*Mailbox Client Intel FPGA IP User Guide*
1.2. Installing the SDM Command Tool in System Console

The SDM command tool consists of two Tcl scripts located in the Download Tcl Scripts (.zip) folder:

- **sdm_command.tcl**: Contains all example functions
- **mailbox_data.tcl**: SDM Command Tool extension. This script contains the error codes definition and MSEL settings.

The Intel Quartus Prime Pro Edition software uses system console to execute the SDM command tool.

1. Use one of the below methods to launch the System Console:
   - In the Intel Quartus Prime Pro Edition software, click **Tools ➤ System Debugging Tools ➤ System Console**.
   - In the Nios® II command shell Windows OS or Terminal in Linux OS, execute `system-console` command.
   - In the Quartus Standalone Programmer (if installed without the Quartus software), launch System Console by executing:
     - `system_console.exe` in the `<programmer_path>\syscon\bin` folder using the Windows OS.
     - `system-console` in the `<programmer_path>\syscon\bin` folder using the Linux OS.

2. In the System Console window, change the working directory to the location of the saved `sdm_command.tcl` and `mailbox_data.tcl` scripts.

3. Source the SDM command tool using the following command:

   ```bash
   % source sdm_command.tcl
   ```

**Related Information**

Download Tcl Scripts

The `sdm_command.tcl` and `mailbox_data.tcl` scripts that implements all example functions and includes error codes definitions.

1.3. Identifying SDM Devices Detected in the Host Machine

With each launch, System Console detects a device connected to the host machine. The host machine may detect multiple SDM devices if there are multiple SDM devices in the same JTAG chain on a board, or there are multiple Intel Download Cable connected to the host machine and each cable connect to different board and detect single SDM device in the JTAG chain separately. If you connected multiple SDM devices, you must first identify your target device by executing the `sdm_device_list` command.

The following output is an example of detecting a single SDM device.

```bash
% sdm_device_list
Device #1 - /devices/1SX280HH1(.|S3)|1SX280HH2|..01#3-2.1.2\n#Stratix 10H SoC Dev Kit#10.219.70.15:44943/(link)/JTAG/packet
```
The following output is an example of detecting multiple SDM devices.

```
% sdm_device_list
Device #1 - /devices/1SG280HH1(.|S3|AS|BK)|..@2#USB-1/(link)/JTAG/packet
Device #2 - /devices/1SM21BHN1(.|AS|BK)|1SM21BHN2|..@1#USB-1/(link)/JTAG/packet
```

1.4. Executing SDM Commands

The `sdm_command.tcl` describes the SDM command procedures available for use. For information about these commands and their codes, refer to the *Mailbox Client Intel FPGA IP User Guide*.

The sections below describe some of the procedures defined in the `sdm_command.tcl` file.

**Related Information**

*Mailbox Client Intel FPGA IP User Guide*

1.4.1. Configuration Status Command

The `sdm_config_status <device_index>` command provides information about the device configuration state, the status of the various configuration pins, and the MSEL pin setting on your device. If you connected a single SDM device, the device index is an optional parameter. If you connected multiple SDM devices and your target device is other than the device #1, you must specify the device index.

The following examples are the expected output of executing the `sdm_config_status` function.

**Example 1. Identifying Successful Configuration using `sdm_config_status`**

```
$sdm_config_status

MSEL[2:0] : 011 (AS (Normal POR))

Configuration pin signals:
  nSTATUS : 1
  nCONFIG : 1
  CONF_DONE : 1
  INIT_DONE : 1
  CvP_DONE : 0
  SEU_ERROR : 0
  HPS_WARMRESET : 0
  HPS_COLDRESET : 0

MSEL[2:0] Table:
  3'b000 AvST x32
  3'b101 AvST x16
  3'b110 AvST x8
  3'b001 AS (Fast POR)
  3'b011 AS (Normal POR)
  3'b111 JTAG only
```
### Example 2. Identifying Failed Configuration using `sdm_config_status`

```
$sdm_config_status

MSEL[2:0] : 011 (AS (Normal POR))

Configuration pin signals:
nSTATUS : 1
nCONFIG : 1
CONF_DONE : 0
INIT_DONE : 0
CvF_DONE : 0
SEU_ERROR : 0
HPS_WARMRESET : 0
HPS_COLDRESET : 0

MSEL[2:0] Table:
3'b000 AvST x32
3'b101 AvST x16
3'b110 AvST x8
3'b001 AS (Fast POR)
3'b011 AS (Normal POR)
3'b111 JTAG only

State : 0xf0010040
Error location : 0x0000c400
Error detail : 0x00000003

Configuration fail!
Major code: 0xF001
Bitstream error, usually due to unsigned bitstream used.

Minor code: 0x0040
Config clock PLL fail error detection, ensure OSCCLK_1 clock source free running and stable.
```

You may need to provide the `device_index` argument for multiple detected devices. If you select device #1, the `device_index` is an optional argument with 1 as a default value. If you select a target device different from device #1, you must specify `device_index` argument. In this example, 1 is device #1 identified using the `sdm_device_list` command.

The example below shows the command with selected device #2.

```
%sdm_config_status 2
```

**Note:** For latest information about error codes updates, refer to the *Mailbox Client Intel FPGA IP User Guide*.

### Related Information

- Mailbox Client Intel FPGA IP User Guide
  - Refer to appendix for error codes descriptions.

### 1.4.2. Temperature Sensor Command

The `sdm_read_temperature_s10` command allows you to read the internal temperature sensor of the Intel Stratix 10 device.
The example below depicts a sample output of the `sdm_read_temperature_s10` command:

```
%sdm_read_temperature_s10
Channel 0: 25.000°C (Core Fabric)
Channel 1: No valid value returned from SDM (Bank 1C, 1D, 1E, 1F, 8A)
Channel 2: No valid value returned from SDM (Bank 1G, 1H, 1I, 1J, 8B)
Channel 3: No valid value returned from SDM (Bank 1K, 1L, 1M, 1N, 8C)
Channel 4: No valid value returned from SDM (Bank 4C, 4D, 4E, 4F, 9A)
Channel 5: No valid value returned from SDM (Bank 4G, 4H, 4I, 4J, 9B)
Channel 6: No valid value returned from SDM (Bank 4K, 4L, 4M, 4N, 9C)
```

Related Information
Intel Stratix 10 Analog to Digital Converter User Guide
Information about the temperature sensor functions.

### 1.4.3. Voltage Sensor Command

The `sdm_read_voltage_s10` command allows you to read the voltage sensor from the Intel Stratix 10 device.

The example below depicts a sample output of the `sdm_read_voltage_s10` command:

```
%sdm_read_voltage_s10
Channel 0: 0.001V (External Channel 0)
Channel 1: 0.000V (External Channel 1)
Channel 2: 0.897V (VCC)
Channel 3: 1.779V (VCCIO_SDM)
Channel 4: 1.803V (VCCPT)
Channel 6: 0.900V (VCCERAM)
Channel 9: 1.784V (VCCADC)
```

Related Information
Intel Stratix 10 Analog to Digital Converter User Guide
Information about the voltage sensor functions.

### 1.4.4. Execute Command

The `exec_command` procedure allows you to execute any SDM command.

Use the following syntax to execute an SDM command specified in the `sdm_command.tcl` file in the Hex format.

```
%exec_command <sdm_command> {list_of_arguments} <device_index>
```

where

- `{list_of_arguments}`: Optional argument that specifies arguments list. By default, list of arguments is an empty list.
- `<device_index>`: Optional argument that provides the specific device number. By default, the device index is set to 1.

*Note:* If the device index is not 1 and you have 0 argument, you must provide an empty list of arguments in the command. The *Executing GET_USERCODE Command* example uses scenario with an empty list of arguments.
The following examples show various usage of the execute command.

**Example 3. Executing GET_USERCODE Command**

Executing the `GET_USERCODE` command (0x13) with empty list of arguments and the device index set to 2.

```
%exec_command 0x13 {} 2
```

The command returns the response header along with the response returned from the SDM after executing the SDM command.

**Example 4. Reading Data from QSPI Flash**

To read the data from the Quad SPI flash memory, you must execute a sequence of SDM commands:

1. `QSPI_OPEN`
2. `QSPI_SET_CS`\(^{(1)}\)
3. `QSPI_READ`
4. `QSPI_CLOSE`

To perform any additional QSPI operations such as write or erase, refer to the `QSPI_WRITE` and `QSPI_ERASE` commands described in the *Mailbox Client Intel FPGA IP User Guide*.

**Table 1. QSPI Command Codes and Length**

The table displays the SDM commands and their hexadecimal code with appropriate command and response length. The command length description is the QSPI flash memory address location from where the data is read.

<table>
<thead>
<tr>
<th>SDM Command</th>
<th>Code (Hex)</th>
<th>Command Length</th>
<th>Response Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>QSPI_OPEN</td>
<td>0x32</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>QSPI_SET_CS</td>
<td>0x34</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>QSPI_READ</td>
<td>0x3A</td>
<td>2</td>
<td>N</td>
</tr>
<tr>
<td>QSPI_CLOSE</td>
<td>0x33</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

1. Executing the `QSPI_OPEN` command (0x32), command returns the response header value of 0x00000000 indicating the successful command execution.
```
%exec_command 0x32
```

2. Executing the `QSPI_SET_CS` command (0x34), command returns the response header value of 0x00000000 indicating the successful command execution.
```
%exec_command 0x34 {} 0
```

3. Executing the `QSPI_READ` command (0x3A), requires two arguments:

\(^{(1)}\) This command is optional for the AS x4 configuration scheme and required for all other configuration schemes.
- **argument 1**: Represents the QSPI flash address
- **argument 2**: Represents total number of words requested to read from QSPI flash, up to the maximum allowed number per read.

%exec_command 0x3A {0 5}
0x00005000 0x62294895 0x00000010 0x00000400 0x00000000 0x00000000

The command reads the SDM device #1 QSPI at location 0 for 5 words. The first word, 0x00005000 of the response is the response header. Bits[22:12] represent the response length and is set to 5. Bits [10:0] represent error code for the response and is 0. The subsequent five words are the data read out from the QSPI flash.

A single read operation can read up to 1024 words, or 4096 bytes. If you need to read more than the maximum allowed words per operation, you must execute another QSPI_READ command with the appropriate offset address.

*Note*: If the argument list specifies more than one argument, you must specify all arguments within the curly brackets argument list.

4. **Executing the QSPI_CLOSE command (0x33).**

%exec_command 0x33

**Related Information**

Mailbox Client Intel FPGA IP User Guide
## 1.5. Document Revision History for AN 936: Executing SDM Command via JTAG Interface

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021.03.29</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>