Michael Alexenko
Senior Design Engineer
2400 Trade Centre Longmont, CO 80503
(303) 682-8378 (303) 682-8787(fax)
internet: Mike.Alexenko@conner.com

This document addresses several issues relating to Revision 13 of the SPI, Annex B (normative), SCSI Configured Automatically (SCAM).

First, this document identifies and attempts to correct various typographical problems as well as identify areas that require clarification. Next, this document requests changes to the specification, based on the experience of developing Plug and Play (SCAM) disk drives. Lastly this document shares a few implementation observations.

This document does address issues that are outside of the scope of Annex B, and I apologize for that. This was done primarily to use this forum as a means of sharing our experiences, and issues with other interested parties. While these issues may fall outside of the scope of Annex B (at this time), it is our feeling that one of the purposes of a standards organization is to insure a usable and fully interoperable system that operates seamlessly and flawlessly to the user. In striving to attain this goal we may need to reconsider the extent of Annex B's definition, or create another Annex to address some of these other issues.

All SCAM technical references are from Revision 13 of the SPI, Annex B (normative), SCSI Configured Automatically (SCAM).

EDITORIAL ISSUES

1. Section B.4.1.2, item #4 reads:

   > "Read and latch data from the DB(4-0) signals."

   This should read:

   > "Read and latch data from the DB(4-0) signals. All devices assert the DB(6) signal."

   (this is section B.4.1.1 in rev. 15)

2. The note under figure 1 in Section B.4.1.2 reads:

   > "Note - Signals are shown".

   This should read:

   > "Note - Signals are shown asserted low."

   (this is figure B.5, section B.4.1.1 in rev. 15, and has been corrected)

3. Section B.4.1.1 is confusing, and needs review.

   In particular the references to the "device" requires some conscious interpretation. In this section "device" is interpreted as any SCSI electronic object that implements SCAM and is capable of initiating the SCAM protocol. I have pondered variations of this section, and can only offer some suggestions, as opposed to a rewritten section:

   a) In paragraph one and two, "device" should be replaced with "SCAM device", as in paragraph three.

   b) Clarification in paragraph one that the protocol is initiated by either a SCAM level 1 initiator, or a SCAM level 2 target, similar to what has been done in paragraph two.

   (this is section B.4.1 in rev. 15)

4. Section B.4.1.1, paragraph two states "...After a variable delay, devices responding to SCAM selection release the MSG signal.....SCAM targets should release the MSG signal quickly, perhaps never asserting it at all. ...."

   This section does not state <u>when</u> this signal is asserted by SCAM devices that have responded to a SCAM selection. This needs to be defined in a clear manner.

   (this is section B.4.1 in rev. 15)

TECHNICAL ISSUES

1. Section B.4.1.4 describes the ID string to be a maximum of 31 bytes, and that SCAM initiators should be able to accept strings of 32 bytes, for future extensions.

   It is assumed that this 32nd byte is appended to the Vendor Specific Code field (bytes 10-30), and there should be no reason why it can, or cannot be transmitted today (as a zeroed byte).

   Conner requests that acceptance of the 32nd byte by SCAM initiators should become mandatory, and this byte should be reserved (contents = 00h) at this time, to avoid problems in the future with backward compatibility.

   (this is section B.5.1.2 in rev. 15)

2. Currently, it appears that no initiators are supporting the Configuration Process Complete function code. Section B.4.1.5.3 *(section B.5.1.3 in rev. 15)* defines this function code (from a target perspective): "...A SCAM target with an unassigned ID that observes this function code should not respond to selection until a reset condition, power on or the assignment of an ID during a subsequent SCAM protocol invocation."

   Although section B.5.2 *(section B.6.2, note 10, in rev. 15)* includes an implementation note: "Some SCAM targets do not recognize the Configuration Process Complete function code and return to the SCAM Monitor state when SCAM protocol is terminated.", there are possible opportunities for problems by NOT supporting this function code.

Conner requests that the implementation of this function code should become mandatory for initiators and targets, to avoid problems such as ID conflicts with fully loaded (and overloaded) busses.

It has been observed that in an illegally configured bus (one initiator and eight targets), some initiators will assign all available IDs, and when detecting another device requesting an ID, it will reset the bus and NOT retry the SCAM protocol, allowing ALL devices to use their default IDs. Potentially all devices on the bus may have the same ID, as defined in revision 1.0 of the "Plug and Play SCSI Specification", dated March 30, 1994, depending on the device types used.

Granted, this may be beyond the scope of Annex B, and those initiators may be behaving incorrectly, but mandatory implementation of the Configuration Process Complete function code will help solve this and related issues. It will also create a mechanism for applications to provide added value to the end-user by correctly identifying illegal bus configurations, and still allowing the bus to operate.

3. Section B.5.1.1.1, paragraph two *(section B.6.1.1 in rev. 15)* , describes a situation where the initiator is polling the bus to identify SCAM tolerant devices by attempting a selection. SCAM tolerant devices will respond by asserting BSY, and the initiator will categorize that ID as assigned. This section goes on to describe the next action by the initiator: "...In this case, the dominant SCAM initiator should complete an Inquiry or similar command sequence to gracefully conclude selection of the SCSI device...".

   It has been observed that some initiators do not issue any command(s) to gracefully conclude selection, but release signals, and\or issue resets.

   It is Conner's position that this section should be modified, and it should be made mandatory for initiators to issue only an INQUIRY or TEST UNIT READY command when polling the bus for legacy devices. (Conner requests choosing one, and not leaving it open to choice.)

4. It has been observed that some initiators are not implementing Wired-OR Glitch Filtering correctly (as defined in section B.4.1.3, *or section B.5.1.1 in rev. 15)*). These initiators will cease to participate in the SCAM protocol when DB7 is glitched. Although it is the responsibility of all initiators and targets to make every effort to not glitch the bus, all targets and initiators have the added responsibility of properly deglitching the bus.

   The following changes to this section are being requested by Conner:

   a) Delete the last paragraph regarding the "alternate method" of calculating the iteration count.

   b) In item "2" require that the iteration count be 32, and delete references to devices determining the width of the bus. This will insure a consistent and interoperable solution between vendors.

5. Section B.4.1.5.1, paragraph 1 *(section B.5.3.1 in rev. 15)* states: "...At this point, the SCAM initiator may transmit an action code to assign an ID to the device or perform an additional function....". (This is for the case where the initiator has transmitted the Isolate function code (00000b).)

This may be interpreted as follows:

A device wins isolation, and the initiator then issues a Locate On action code. At this point the initiator would transmit another Synchronization function code, and all devices would participate in another round of isolation. The same device would win, and wait for the next action code. The initiator would then transmit an Assign ID action code, and this device would accept the new ID, and cease to participate in the SCAM protocol.

It has been observed that some SCAM targets will only accept an Assign ID action code after winning isolation, meaning that if a Locate On action code is transmitted, it seems to be discarded, and that device no longer participates in the SCAM protocol. This device will then respond only to its default ID, causing potential ID conflicts with legacy devices

It is requested by Conner that the implementation of ALL function codes described in section B.4.1.5, and ALL action codes described in section B.4.1.5.1 become mandatory. The table may look like this:

Function Codes

code	initiators	targets
isolate	**M**	**M**
isolate and set priority flag	**O**	**M**
configuration process complete	**M**	**M**
dominant initiator contention	**M**	**---**

Action Codes

code	initiators	targets
assign id 00nnnb	**M**	**M**
assign id 01nnnb	**(depends)**	**(depends)**
assign id 10nnnb	**(depends)**	**(depends)**
assign id 11nnnb	**(depends)**	**(depends)**
clear priority flag	**O**	**M**
locate on	**O**	**M**
locate off	**O**	**O**

(se*ction B.5.1.3, table B.7, and section B.5.1.3.1, table B.8, respectively, in rev. 15)*

IMPLEMENTATION OBSERVATIONS

1. Annex B does not define timeouts for any errors that may occur during the protocol, such as:

   - during SCAM Selection, any of the control lines or data lines used for handshaking are never released by an initiator or target.

   - the second quintet of an action code is never received.

   - during the transfer cycles, a target or initiator never releases a handshake line (DB7-DB5).

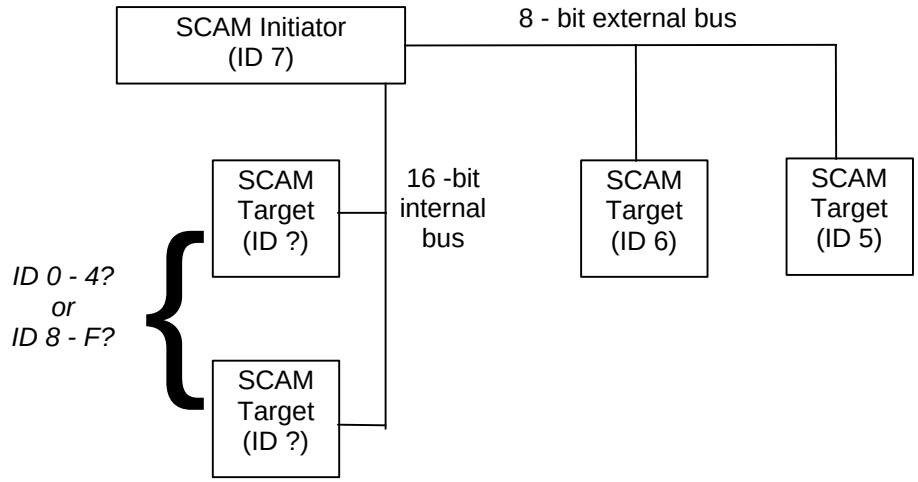
   These issues should be examined, and appropriate timeouts and recovery actions should be implemented. A suggestion is to use the SCAM selection response time (250ms). After this time has elapsed, the initiator(s) detecting the timeout should reset the bus. This solution is obviously too simplistic, but may serve as a starting point for discussions.

   Granted, an endless cycle of resetting the bus when the failing device continues to "hang" is not desirable, but the current implementation of having no timeouts and allowing the system to hang is not desirable either. By defining some gross level of timeouts, a means of allowing the application to be notified of an error is created.

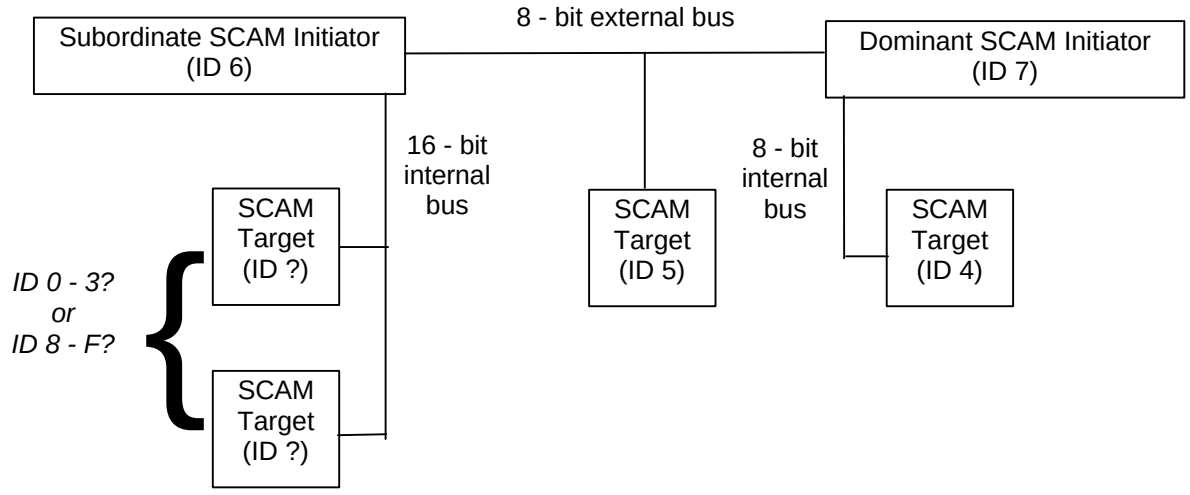
2. SCAM tolerant reset to selection delay is defined to be 250ms. This duration is defined to be "The maximum time a SCAM tolerant device may delay after a reset condition before enabling its response to selection". This is mentioned again in section B.5.1.1.1, paragraph one *(section B.6.1.1.1 in rev. 15)*: "After a reset condition, a dominant SCAM initiator shall wait as necessary to insure that a SCAM tolerant reset to selection delay has elapsed....".

   The time from Reset to the polling of the bus to detect SCAM tolerant devices has been measured on some host adapters to be in the range of 7-30ms. This short duration causes situations where some legacy devices do not respond to the initial Selection to determine the bus configuration. The result is potential ID conflicts with SCAM devices.

3. The area of ID assignment for mixed bus widths is not specifically addressed. Two diagrams below describe such situations. The first example is a 16-bit bus internally (with devices that will support a 16-bit bus), and an 8-bit external bus. The second example describes a multi-initiator system with mixed bus widths.



Example 1 - Single Initiator, mixed bus widths.
Question: Do the devices on the 16-bit bus receive IDs greater than 07?



Example 2 - Multiple Initiators, mixed bus widths.
Question: Do the devices on the 16-bit bus receive IDs greater than 07?

While perhaps beyond the scope of Annex B, it is Conner's position that Annex B should make some reference to SCSI IDs in mixed bus width configurations.