This function sequence has two purposes; it communicates to subordinate SCAM initiators that they may resume normal SCSI operations (and scan the SCSI bus) and it confirms that SCAM targets with unassigned ID's shall remain in this state and not respond to normal SCSI selection.
Dominant SCAM initiators may be implemented in several ways so long as the functions of SCSI ID catego-rization and assignment are performed as specified below.
00b A level 1 SCAM initiator
01b A level 2 SCAM initiator for which code 11b does not apply
10b reserved

11b A level 2 SCAM initiator that knows it was dominant in the previous invocation of the SCAM protocol or has non-SCAM knowledge that it should attempt to become the dominant SCAM initiator

working draft SCSI-3 Parallel Interface ~~Ammendment~~ Amendment
18 revision 00
Once a SCAM target has reached the ID Assigned state it functions as a SCAM tolerant device with the ID assigned. That is, it shall respond to SCSI selection within a SCAM tolerant selection response time and shall not recognize nor respond to SCAM selection.
A reset indication shall cause a SCAM target to enter the Reset Delay state, in which it may perform local initialization. The SCAM target shall leave this state and enter the SCAM monitor state within a SCAM reset to SCAM selection delay.
A.5.3 Level 2 SCAM target
Level 2 SCAM target operation is illustrated in Figure B-3 below. State names are referenced in the descrip-tion that follows. ~~Note a~~ A reset indication shall cause an exit from any state and places the SCAM target in the Reset Delay state.
When a SCAM target is powered-on, it immediately enters the Power-On Delay state and may per-form local initialization. The SCAM target shall leave this state and enter the Initiate SCAM Protocol state within a SCAM power-on to SCAM selection delay.
In the Initiate SCAM Protocol state, a level 2 SCAM target shall arbitrate for the SCSI bus without an ID and perform SCAM selection. After a SCAM selection delay, the SCAM target shall examine the SCSI bus to determine the state of the C/D signal. If the C/D signal is true, there is a SCAM initiator present and the SCAM target shall enter the ID Assignable state. If the C/D signal is false, no SCAM initiator is present and the SCAM target shall enter the SCAM Monitor state. Note that level 2 SCAM targets make only one attempt to initiate SCAM protocol after power-on.

While in the SCAM Monitor state, a SCAM target shall monitor the SCSI bus for both SCAM selection and normal SCSI selection. If the SCAM target detects the initiation of SCAM protocol, it shall enter the ID Assignable state. If a selection indication for the SCAM target's current ID is received after the SCSI bus sig-Figure 3:

each SCAM protocol invocation. Level 1 SCAM initiators shall be capable of detecting and participating in dominant initiator contention. Level 1 SCAM initiators should also perform dominant initiator contention unless they can guarantee through non-SCAM means that they are the only initiator present. SCAM targets shall ignore dominant initiator contention.

Following a Dominant Initiator Contention function code, SCAM initiators participate in an isolation stage. After the isolation stage completes the single remaining SCAM initiator is the dominant SCAM initiator. It remains the dominant SCAM initiator until the next invocation of the SCAM protocol.

SCAM initiators shall not prematurely terminate isolation after a Dominant Initiator Contention function code. If a SCAM initiator detects the DB(4) signal true or detects an error condition during the isolation stage, it may attempt recovery by releasing all signals and waiting for bus free indication, or by ~~making~~ generating a reset request.

working draft SCSI-3 Parallel Interface ~~Ammendment~~ Amendment
revision 00

15 Each SCAM initiator broadcasts a dominance preference code in the priority code filed of the type code bytes during isolation. The dominance preference code indicating the status of the participating SCAM initia-tors is defined in table B.9.

A.5 SCAM operations

SCAM operations encompass all those functions, for both SCAM initiators and targets, that are necessary to differentiate SCAM tolerant and SCAM devices and to subsequently assign ID's to SCAM devices. It is nec-essary to understand the operations of both SCAM initiators and targets, as described below, and their inter-actions to obtain a clear picture of SCAM operations.

A.5.1 SCAM initiator

Subsequent to power-on, a SCAM initiator should complete its local initialization and shall wait at least a SCAM power-on to SCAM selection delay before initiating any SCSI bus activity. A SCAM initiator that is a level 1 SCAM device or that can determine by means beyond the scope of this annex that it is the dominant SCAM initiator should ~~make~~ generate a reset request after power-on. A level 2 SCAM initiator that cannot a priori determine that it is the dominant SCAM initiator should not ~~make~~ generate a reset request but should initiate SCAM protocol, as described below, as if a reset indication had occurred.

After a SCAM initiator has made a reset request or received a reset indication, it shall initiate SCAM protocol after the bus free indication that immediately follows a reset request or indication. The first function sequence should be a Dominant Initiator Contention function. If the SCAM initiator broadcasts the numeri-cally highest identification string during the isolation stage, it becomes the dominant SCAM initiator. If the SCAM initiator does not have the highest identification string, it becomes a subordinate SCAM initiator.

Note 12 Level 1 SCAM initiators are not required to perform dominant initiator contention, but they shall detect a dominant initiator contention function broadcast by another SCAM ini-tiator. The identification string of a level 1 SCAM initiator is defined so that it cannot win contention with a level 2 SCAM initiator; thus the losing level 1 SCAM initiator assumes the role of a subordinate SCAM initiator.

Level 2 SCAM initiators shall always be enabled to detect the initiation of SCAM protocol by another SCAM device.

A.5.1.1 Dominant SCAM initiator

A dominant SCAM initiator is responsible to categorize possible SCSI ID's as assigned or unassigned and then to assign ID's to SCAM devices as necessary. Once this process of ID assignment is complete, the dominant SCAM initiator should broadcast a Configuration Process Complete function.

after the device is powered-on.
c) shall enable its response to SCAM selection within a SCAM reset to SCAM selection delay after a reset indication.
d) shall, once selection response is enabled and provided that the device ID is unassigned, recognize and respond to SCAM selection within a SCAM selection response time.
e) shall not, while its ID remains unassigned, generate a selection indication unless the SEL signal and the SCSI ID bit that encodes the unassigned ID are true and the BSY and I/O signals are false for at least a SCAM unassigned ID selection response delay. The selection confirmation generated subsequent to such a selection indication shall cause the device to have an assigned ID equal to its current ID.
f) shall, once assigned an ID, behave as a SCAM tolerant device until a subsequent power-on or reset indication. Note that SCAM devices with assigned ID's neither recognize, respond to nor ini-tiate SCAM selection.
g) shall not ~~make~~ generate a reset request upon a selection timeout.
h) shall not implement the soft reset alternative as defined in SCSI-2.

i) shall be capable of arbitration without an ID. Subsequent to power-on, a level 2 SCAM target shall initiate SCAM protocol provided that the device does not have an assigned ID and no reset indica-tion has occurred.

---

Editors Note 4 - GOP: All the figure and table references are B.x. They should be changed to x.

---

working draft SCSI-3 Parallel Interface ~~Ammendment~~ Amendment
14 revision 00
The Locate On and Off action codes instruct the isolated device(s) to provide assistance for users or service personnel to physically locate the device. Upon receiving a Locate On action code, the recommended action is for the isolated device(s) to flash their fault indicator or activate some similar indication. The indication should be cleared upon receiving a Locate Off action code, a reset indication, after a time delay or upon other vendor specific actions or conditions.
A SCAM target that receives a valid ID assignment should release all bus signals and cease participating in the SCAM protocol until the next reset indication or power-on. SCAM targets shall continue participating in the SCAM protocol if they receive any other action code, receive an invalid or reserved action code, or do not receive an action code. Failure to receive an action code is typically caused by a SCAM initiator choosing to abort a function by asserting the synchronization pattern.
A.4.1.4.2Isolate and set priority flag function The Isolate and Set Priority Flag function operates exactly as the Isolate function described above except that the only valid action codes are those that assign an ID to the isolated device(s). This function also causes the device's priority flag to be set to one.
A.4.1.4.3Configuration process complete function The Configuration Process Complete function is issued by the dominant SCAM initiator when the bus config-uration is complete and no further ID's are to be assigned. SCAM initiators that did not win dominance should avoid using the bus until this function code is observed. A SCAM target with an unassigned ID that observes this function code should not respond to selection until a reset indication, power on or the assign-ment of an ID during a subsequent SCAM protocol invocation.
A.4.1.4.4Dominant initiator contention function The Dominant Initiator Contention function selects one SCAM initiator, called the dominant SCAM initiator, from possibly multiple SCAM initiators. Level 2 SCAM initiators shall perform Dominant Initiator Contention as the first function sequence following

after the device is powered-on.
c) shall enable its response to SCAM selection within a SCAM reset to SCAM selection delay after a reset indication.
d) shall, once SCAM selection response is enabled and provided that its device ID is unassigned, rec-ognize and respond to SCAM selection within a SCAM selection response time.
e) shall not, while its ID remains unassigned, generate a selection indication unless the SEL signal and the SCSI ID bit that encodes the unassigned ID are true and the BSY and I/O signals are false for at least a SCAM unassigned ID selection response delay. The selection confirmation generated subsequent to such a selection indication shall cause the device to have an assigned ID equal to its current ID.
f) shall, once assigned an ID, behave as a SCAM tolerant device until a subsequent power-on or reset indication. Note that SCAM devices with assigned ID's neither recognize, respond to nor ini-tiate SCAM selection.
g) shall not ~~make~~ generate a reset request upon a selection timeout.
h) shall not implement the soft reset alternative as defined in SCSI-2.
A.3.3.4 Level 2 SCAM initiator
A level 2 SCAM initiator:
a) shall recognize reset indications at all times.

Note 7 SCAM implementations, whether in firmware or hardware, are expected to monitor


7 the RST signal even while engaged in SCAM protocol.
b) shall be capable of initiating SCAM protocol and utilizing SCAM function sequences to assign ID's to SCAM devices. Level 2 SCAM initiators are also required to detect and respond to SCAM selec-tion initiated by other SCAM devices.
c) shall perform dominant initiator contention each time SCAM protocol is initiated.
d) shall have either an assigned ID or be able to arbitrate without an ID.
e) shall be able to operate with a selection timeout greater than the SCAM tolerant selection response time and less than the SCAM unassigned ID selection response delay. A level 2 SCAM initiator shall also be able to operate with a selection timeout greater than the SCAM unassigned ID selection response delay.
f) shall not ~~make~~ generate a reset request upon a selection timeout.
g) shall, provided an assigned or current ID is available, satisfy the requirements for a SCAM tolerant device.
Note 8 A level 2 SCAM initiator without a current ID may receive an assigned ID by one of two methods: either it assigns itself an ID or, by means of SCAM protocol functions, is assigned an ID by another SCAM initiator. A level 2 SCAM initiator that has a current ID may receive an assigned ID by either of these two methods or its current ID may become its assigned ID if a selection indication for the SCAM initiator's current ID is received after the SCSI bus signals required for selection have been continuously valid for at least a SCAM unassigned ID selection response delay.
A.3.3.5 Level 2 SCAM target
A level 2 SCAM target:
a) shall recognize reset indications at all times.
Note 9 SCAM implementations, whether in firmware or hardware, are expected to monitor the RST signal even while engaged in SCAM protocol.
b) shall enable its response to SCAM selection within a SCAM power-on to SCAM selection delay

In addition, all SCAM devices shall disable active negation of SCSI bus signals during SCAM protocol.

A.3.3.1 SCAM tolerant target

A SCAM tolerant target:

a) shall enable its response to selection within a SCAM tolerant power-on to selection delay after the device is powered-on.

b) shall enable its response to selection within a SCAM tolerant reset to selection delay after a reset indication.

c) shall recognize a valid selection of the device's current ID whether or not an initiator ID is included in the selection IDs parameter of the selection indication.

d) shall, once selection response is enabled, respond to a selection of its current ID by generating a selection confirmation no later than a SCAM tolerant selection response time after the selection indication.

The current ID becomes the assigned ID when the SCAM tolerant device responds to selection.

Note 2 It is recommended that initiators clear the DiscPriv bit in the IDENTIFY message if selection is performed without an initiator ID.

Note 3 The requirement for rapid response to selection by SCAM tolerant devices and delayed response to selection by SCAM devices that do not have assigned ID's permits SCAM initiators to distinguish between the two. A SCAM initiator may use a relatively short selection timeout (SCAM tolerant selection response time plus two bus settle delays) to scan the bus for SCAM tolerant devices without causing the assignment of an ID.

working draft SCSI-3 Parallel Interface ~~Ammendment~~ Amendment

6 revision 00

A.3.3.2 Level 1 SCAM initiator

A level 1 SCAM initiator:

a) shall recognize reset indications at all times.

Note 4 SCAM implementations, whether in firmware or hardware, are expected to monitor the RST signal even while engaged in SCAM protocol.

b) shall be capable of initiating SCAM protocol and utilizing SCAM function sequences to assign ID's to SCAM devices. Level 1 SCAM initiators are not required to detect or respond to SCAM selec-tion.

c) shall be capable of detecting a Dominant Initiator Contention function code and subsequently par-ticipate in the isolation stage for the dominant initiator.

Note 5 It is recommended that level 1 SCAM initiators perform Dominant Initiator Conten-tion each time SCAM protocol is initiated.

d) shall have an assigned ID.

e) shall be able to operate with a selection timeout greater than the SCAM tolerant selection response time and less than the SCAM unassigned ID selection response delay. A level 1 SCAM initiator shall also be able to operate with a selection timeout greater than the SCAM unassigned ID selection response delay.

f) shall not ~~make~~ generate a reset request upon a selection timeout.

g) shall satisfy the requirements for a SCAM tolerant device.

A.3.3.3 Level 1 SCAM target

A level 1 SCAM target:

a) shall recognize reset indications at all times.

Note 6 SCAM implementations, whether in firmware or hardware, are expected to monitor the RST signal even while engaged in SCAM protocol.

b) shall enable its response to SCAM selection within a SCAM power-on to SCAM selection delay

SCAM tolerant selection response time 1 ms
SCAM unassigned ID selection response delay 4 ms
SCAM power-on to SCAM selection delay 1 s
SCAM reset to SCAM selection delay 250 ms
SCAM selection response time 250 ms
Recommended SCAM selection response time 1 ms

Wide arbitration time 7.2 us

working draft SCSI-3 Parallel Interface ~~Ammendment~~ Amendment
revision 00

5 A level 2 SCAM target shall initiate SCAM protocol within this time limit.
A SCAM initiator shall wait at least a SCAM power-on to SCAM selection delay before initiating SCAM pro-tocol.
A.3.2.6 SCAM reset to SCAM selection delay
The minimum time, measured from the bus free indication that immediately follows a reset indication, a SCAM device shall delay after a reset indication before initiating SCAM protocol.
A.3.2.7 SCAM selection response time
The maximum time a SCAM device shall require to detect and respond to SCAM selection. This is also the minimum time a SCAM initiator should maintain SCAM selection in situations where a slow response by other SCAM devices is anticipated (e.g. firmware SCAM implementations).
A.3.2.8 Recommended SCAM selection response time
The minimum time a SCAM device should maintain SCAM selection in situations where a rapid response by other SCAM devices is anticipated (e.g. hardware SCAM implementations). This is also the recommended maximum time a SCAM device should require to detect and respond to SCAM selection.

---

Editors Note 2 - GOP: The SCAM selection response time and the recommanded SCAM selection response time assume the SCAM device some how knows the kind of system it has been placed into. How is this possible? This issue should be dealt with in a future standard.

---

A.3.2.9 Wide arbitration time
The maximum time after the assertion of BSY within which a SCAM device with an ID greater than 7 shall conclude its examination of the data bus to determine the outcome of arbitration.
Note 1 This requirement is necessary for arbitration without an ID to work on mixed width buses. It is based on the assumption that all wide SCSI devices implement arbitration logic in hardware and therefore can be relied on to assert the SEL signal quickly if they win arbitra-tion.

---

Editors Note 3 - GOP: The wide arbitration time, in effect, places a maximum arbitration time for all wide SCSI devices. This should be dealt with in a future standard.

---

A.3.3 Device requirements
The following subclauses define the operational requirements of SCAM and SCAM tolerant devices that may be configured on the same SCSI bus.

working draft SCSI-3 Parallel Interface ~~Ammendment~~ Amendment
4 revision 00
d) Multiple level 2 SCAM initiators are permitted on the bus, which they may share with up to one level 1 SCAM initiator;
e) All SCAM tolerant and level 1 SCAM targets on the bus shall be powered on before or con-cur-rently with a SCAM initiator;
f) If the only SCAM initiator is a level 1 SCAM initiator, all devices should be powered on before or concurrently with the level 1 SCAM initiator. ~~Level 2 SCAM targets powered on after the level 1 SCAM initiator has completed SCAM protocol cannot be detected by the level 1 SCAM initiator until a subsequent reset indication~~. The SCAM protocol dos not provide the capability for SCAM level 1 initiators to detect level 2 SCAM targets powered on after the level 1 SCAM initiator has completed SCAM protocol, until a subsequent reset indication.
Some of these configuration requirements may be overcome by means outside the scope of this annex.
A.3.2 Timing requirements
Unless otherwise indicated, the time measurements for each SCAM or SCAM tolerant device, shown in table ~~B.~~1, shall be measured for signal conditions existing at that SCSI device's own SCSI bus connection.
A.3.2.1 SCAM tolerant power-on to selection delay
The maximum time a SCAM tolerant device may delay after power-on before enabling its response to selec-tion.
A.3.2.2 SCAM tolerant reset to selection delay
A SCAM tolerant device shall enable its response to selection within this time limit, measured from the bus free indication that immediately follows a reset indication.
A SCAM initiator shall wait at least a SCAM tolerant reset to selection delay before starting SCSI ID catego-rization.

---

Editors Note 1 - GOP: The term 'SCSI ID categorization' Should be cross referecned to secion A.5..1.1.1

---

A.3.2.3 SCAM tolerant selection response time

A SCAM tolerant device shall respond to selection of its current ID within this time limit, provided that both the SCAM tolerant power-on to selection and reset to selection delays have been satisfied.
A SCAM initiator should use a minimum selection timeout delay of a SCAM tolerant selection response time plus two bus settle delays when scanning the bus for SCAM tolerant devices.
A.3.2.4 SCAM unassigned ID selection response delay
The minimum time a SCAM device shall delay before responding to selection of its current ID, pro-vided that the SCAM device has not been assigned an ID since the last power-on or reset indication.
A SCAM initiator should use a maximum selection timeout delay less than a SCAM unassigned ID selection response delay when scanning the bus for SCAM tolerant devices.
A.3.2.5 SCAM power-on to SCAM selection delay
A level 1 SCAM device shall enable its response to SCAM protocol initiation within this time limit.

Description Value
SCAM tolerant power-on to selection delay 5 s
SCAM tolerant reset to selection delay 250 ms

- SCSI-3 Serial Bus Protocol (SBP) [X3T10/992D]
- SCSI-3 Generic Packetized Protocol (GPP) [X3T10/991D]
- SCSI-3 Architecture Model (SAM) [X3T10/994D]
- SCSI-3 Primary Commands (SPC) [X3T10/995D]
- SCSI-3 Block Commands (SBC) [X3T10/996D]
- SCSI-3 Stream Commands (SSC) [X3T10/997D]
- SCSI-3 Graphic Commands (SGC) [X3T10/998D]
- SCSI-3 Medium Changer Commands (SMC) [X3T10/999D]

3.1 Table 9

In table 9 the column labeled "P cable signals" should be labeled "Primary cable signals"; the column labeled "Q cable signals" should be ~~labled~~ labeled "Secondary cable signals".

3.2 Sub-clause 10.11.3

Replace "The DB(15-8,P1) signals are undefined and parity may not be valid." with, "At the receiving device the DB(15-8,P1) signals are undefined and parity may not be valid."

3.3 Annex B

Annex B is replaced in its entirety with the material in Annex A of this ~~ammendment~~ amendment.

3.4 Annex D.1

Replace item ~~d~~ b) with:

b) Remove ~~5.0~~ 5,0 cm of outer jacket at each end of the cable sample.

Replace item ~~d~~ e) with

e) Strip insulation from all conductors at both cable ends 0,6 cm.

working draft SCSI-3 Parallel Interface Amendment
2 revision 00
3Changes to SCSI-3 Parallel Inference (x3.253-1996) ~~Clauses~~

3.x Clause 1

Replace figure 1 with the following:

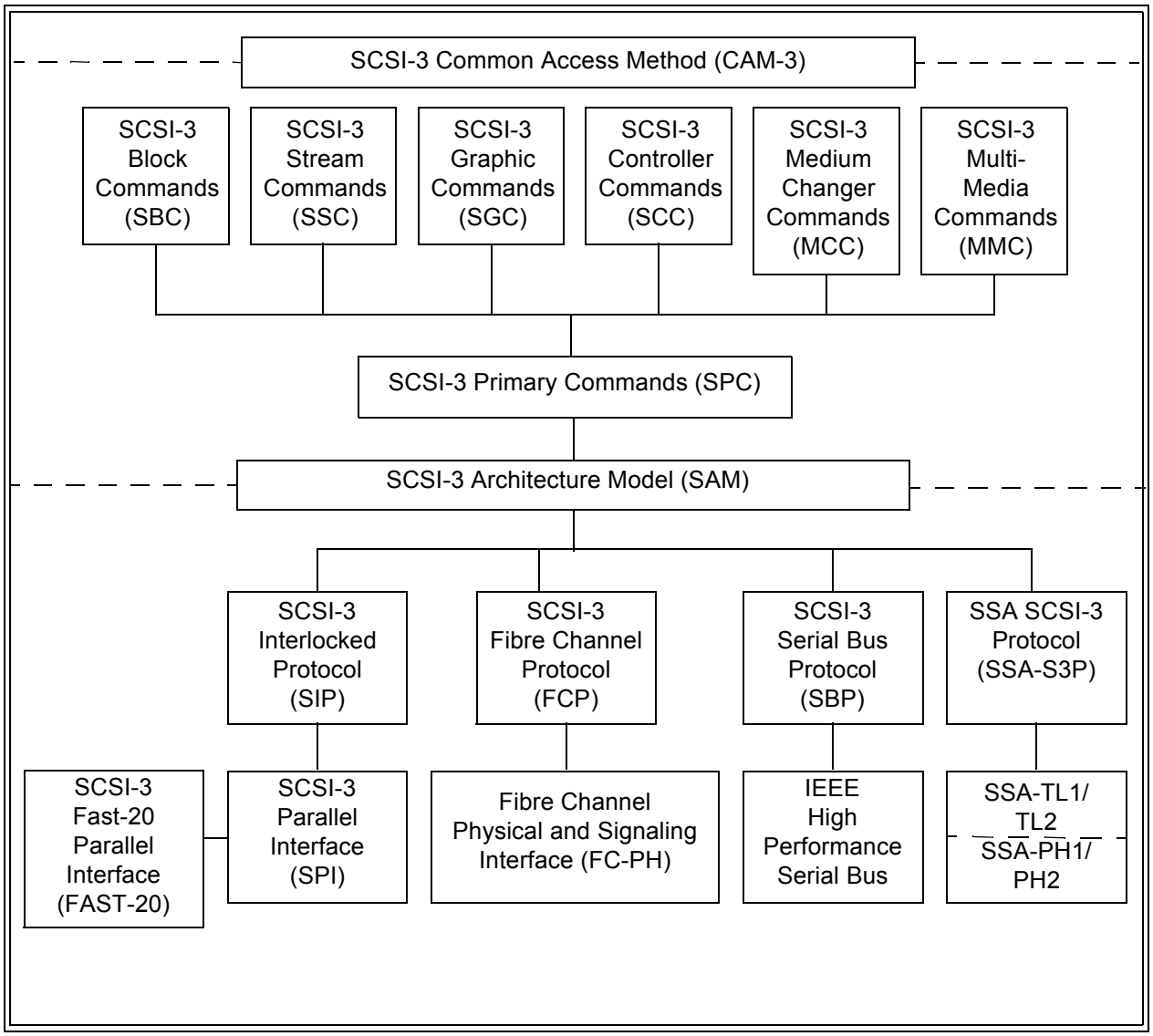


Figure 1 - SCSI-3 document road map

Delete the following:

The term SCSI-3 refers collectively to the following documents that fall under the jurisdiction of X3T10:

- SCSI-3 Parallel Interface (SPI) [X3T10/855D]
- SCSI-3 Interlocked Protocol (SIP) [X3T10/856D]
- SCSI-3 Fiber Channel Protocol (FCP) [X3T10/993D]

working draft SCSI-3 Parallel Interface Amendment

revision 00 <

1Scope

This amendment corrects several technical and editorial defects in the SCSI-3 Parallel Interface Standard (X3.253-1996).

2Normative references

~~The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. The Standards are subject to revision, and parties to agreements based on this International Standard are encouraged to inves-tigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.~~

None.

To: X3T10 Committee (SCSI)
From: George Penokie (IBM) and Gene Milligan (Seagate Technology)

Subject: Comments on SCSI-3 Parallel Interface ammendment rev 00

# X3T10/855A revision 00

# draft proposed amendment to American National Standard Information Technology -SCSI- 3 Parallel Interface


~~ASC~~ X3T10 Technical Editor:

Lawrence J. Lamers Adaptec 691 South Milpitas Blvd San Jose, CA 95035 Telephone: 408-957-7817 Facsimile: 408-957-7193 Email: ljlamers@aol.com

Abstract

This is an amendment providing corrections to the SPI standard that ~~This standard~~ defines mechanical, electrical, and timing requirements for the SCSI-3 Parallel Inter-face. ~~This standard~~ The SPI standard is principally intended to be used in conjunction with the SCSI-3 Interlocked Pro-tocol Standard. ~~Alternatively, the SCSI-3 Generic Packetized Protocol (GPP) may be used in conjunction with this standard~~. The resulting interface facilitates the interconnection of computers and intelligent peripherals and thus provides a common interface specification for both systems inte-grators and suppliers of intelligent peripherals.

Patent Statement
The developers of this standard have requested that holder's of patents that may be required for the implementation of the standard, disclose such patents to the publisher. However neither the develop-ers nor the publisher have undertaken a patent search in order to identify which if any patents may apply to this standard.
As of the date of publication of this standard and following calls for the identification of patents that may be required for the implementation of this standard, no such claims have been made. No further patent search is conducted by the developer or publisher in respect to any standard it processes. No representation is made or implied that license are not required to avoid infringement in the use of this standard.
Document Status
Revision Comments

0 First pass at putting together the amendment