Annex B
(normative)
SCSI configured automatically (SCAM)

B.1 Model

The SCAM protocol is defined by this annex. SCAM is defined to ease user problems with the configuration of SCSI ID's on an SCSI bus. Level 2 SCAM defines all the hardware and software requirements necessary to implement all the functionality described in this annex. Level 1 SCAM defines a subset that requires less capable hardware and software; although it does not support all of the advanced features of level 2 (such as hot plugging) it is intended to solve most configuration problems common to the single-user system. Implementation of the SCAM protocol is optional, however, if implemented, the SCSI SCAM protocol shall conform to this annex.

B.2 Definitions

For the purposes of this annex, the following definitions apply in addition to those in the body of the standard.

assigned ID. An SCSI ID which has been inherently (in the case of SCAM tolerant devices), explicitly (by SCAM protocol) or implicitly (by SCSI selection of a minimum duration) established for an SCSI device. When an ID is assigned it also becomes the current ID. Similarly, once an ID is assigned any change to the device's current ID by non-SCAM means (e.g., a MODE SELECT command) also changes the assigned ID.

current ID. The SCSI ID that is available to an SCSI port. It may originate from jumpers, switches, mode parameters or some other source.

SCAM device. Any SCSI device, initiator or target, that implements the SCAM protocol defined in this annex.

SCAM initiator: A SCAM device that is capable of initiating SCAM selection and performing the normal functions of an SCSI initiator. These capabilities permit a SCAM initiator to scan an SCSI bus to discriminate between SCAM tolerant and SCAM devices and assign ID's to the SCAM devices.

SCAM target. A SCAM device that is capable of recognizing and responding to SCAM selection. This capability permits a SCAM target to receive an ID assignment from a SCAM initiator. A SCAM target shall have a current ID, even when it is unassigned.

SCAM tolerant. An SCSI device which does not implement the SCAM protocol but which complies with certain requirements specified by this annex. SCAM tolerant devices can be detected by a SCAM initiator and may be intermixed with SCAM devices.

unassigned ID. The current SCSI ID which is available to the device but has not yet been assigned to the device.

B.3 SCAM requirements

B.3.1 Configuration requirements

SCAM configuration requirements permit SCAM tolerant, level 1 SCAM and level 2 SCAM devices to operate on the same SCSI bus. These requirements are:

a) SCAM intolerant devices (i.e., legacy SCSI devices which are not SCAM tolerant) are not permitted on the bus;

b) Any SCSI initiator on the bus shall be a SCAM initiator;

c) No more than one level 1 SCAM initiator is permitted on the bus;

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 concurrently 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.

Some of these configuration requirements may be overcome by means outside the scope of this annex.

B.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.

Table B.1 — SCAM timing values

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

B.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 selection.

B.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 categorization.

B.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 of a SCAM tolerant selection response time plus two bus settle delays when scanning the bus for SCAM tolerant devices.

B.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, provided 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 less than a SCAM unassigned ID selection response delay when scanning the bus for SCAM tolerant devices.

B.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.

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 protocol.

B.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.

B.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).

B.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.

B.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 2 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 arbitration.

B.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.

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

B.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 3 It is recommended that initiators clear the DiscPriv bit in the IDENTIFY message if selection is performed without an initiator ID.

Note 4 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.

B.3.3.2 Level 1 SCAM initiator

A level 1 SCAM initiator:

a) shall recognize reset indications at all times.

Note 5 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 selection.

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

Note 6 It is recommended that level 1 SCAM initiators perform Dominant Initiator Contention 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 a reset request upon a selection timeout.

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

B.3.3.3 Level 1 SCAM target

A level 1 SCAM target:

a) shall recognize reset indications at all times.

Note 7 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 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, 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 initiate SCAM selection.

g) shall not make a reset request upon a selection timeout.

h) shall not implement the soft reset alternative as defined in SCSI-2.

B.3.3.4 Level 2 SCAM initiator

A level 2 SCAM initiator:

a) shall recognize reset indications at all times.

Note 8 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 2 SCAM initiators are also required to detect and respond to SCAM selection 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 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 9 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.

B.3.3.5 Level 2 SCAM target

A level 2 SCAM target:

a) shall recognize reset indications at all times.

Note 10 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 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 initiate SCAM selection.

g) shall not make 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 indication has occurred.

B.4 SCAM protocol

SCAM is a distributed algorithm collectively executed by a group of participating SCAM devices. The communication is accomplished by shared (wired-OR) SCSI bus signals that may be asserted or released by the SCAM devices, but which shall not be negated by any participating device. Any SCAM device which is capable of active negation of SCSI bus signals shall disable active negation during SCAM protocol.

B.4.1 Initiation

A device initiates the SCAM protocol by first winning bus arbitration, then performing SCAM selection. The device may arbitrate using its current ID or it may arbitrate without an ID. After winning arbitration the device has the BSY and SEL signals asserted. It shall release all DATA BUS signals and assert the MSG signal, then wait at least two deskew delays and release the BSY signal. It shall maintain this pattern of the SEL and MSG signals asserted with the BSY signal released for a minimum of a recommended SCAM selection response time, then release the MSG signal. After releasing the MSG signal the device shall wait, using wired-OR glitch filtering (see table B.1), until the MSG signal has been released by all other devices.

Level 2 SCAM initiators and SCAM targets that have not yet been assigned an ID recognize SCAM selection if a pattern of the SEL and MSG true and the BSY signal false is detected. After a variable delay, devices responding to SCAM selection release the MSG signal, then wait, using wired-OR glitch filtering, until the MSG signal has been released by all devices. SCAM targets should release the MSG signal quickly, perhaps never asserting it at all. SCAM initiators should wait a SCAM selection response time before releasing the MSG signal.

After wired-OR glitch filtering is used to detect the MSG signal false, each SCAM device asserts the BSY signal, waits at least two deskew delays, then asserts several other signals. SCAM initiators assert the BSY signal followed by the I/O, C/D, DB(6) and DB(7) signals. SCAM targets assert the BSY signal followed by the I/O, DB(6) and DB(7) signals. After asserting its signals each device waits at least two more deskew delays, then releases the SEL signal and waits, using wired-OR glitch filtering, until the SEL signal has been released by all devices.

After detecting that the SEL signal has been released by all devices, SCAM devices release the DB(6) signal and examine the bus signals. If the C/D signal is false, then there are no SCAM initiators participating and SCAM targets shall release all signals. If the C/D signal is true, each SCAM device waits, using wired-OR glitch filtering, for the DB(6) signal to be released by all devices and then asserts the SEL signal. Initiation of the SCAM protocol is complete after the SEL signal has been asserted.

B.4.1.1 Transfer cycles

The SCAM protocol functions through sequences of transfer cycles. During each transfer cycle certain devices broadcast data to all participating SCAM devices. The actual data received is the logical-OR of the data broadcast by all the sending devices. Each transfer cycle is fully interlocked in the same sense that asynchronous data transfers are interlocked. Completion of each step of the transfer is explicitly acknowledged, and the transfer rate adapts automatically to the speed of the SCAM devices involved.

Transfer cycles use the DB(7-5) signals as handshake lines and the DB(4-0) signals as data lines. At the beginning and end of each transfer cycle the DB(7) signal is asserted while the DB(6) and DB(5) signals are released. As shown in figure B.1each device repeats the following steps for each transfer cycle:

1) Assert data on the DB(4-0) signals, if the device is broadcasting data. Devices that have no data to broadcast release these signals. All devices assert the DB(5) signal.
2) All devices release the DB(7) signal.
3) Wait, using wired-OR glitch filtering, until the DB(7) signal is released by all devices.
4) Read and latch data from the DB(4-0) signals. All devices assert the DB(6) signal.
5) All devices release the DB(5) signal.
6) Wait, using wired-OR glitch filtering, until the DB(5) signal is released by all devices.
7) Release or change the DB(4-0) signals. All devices assert the DB(7) signal.
8) All devices release the DB(6) signal.
9) Wait, using wired-OR glitch filtering, until the DB(6) signal is released by all devices.

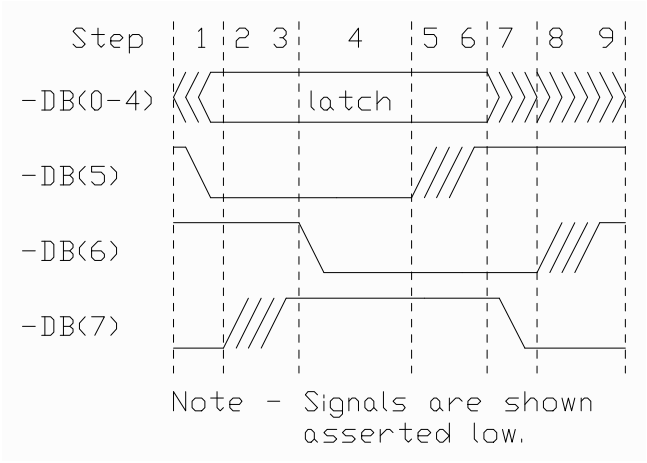

Figure B.5— Transfer cycles

The SCAM protocol continues through successive transfer cycles until the dominant SCAM initiator chooses to terminate it by releasing the C/D signal and all other signals. SCAM targets shall note the release of the C/D signal and release all signals.

B.5.1.1 Wired-OR glitch filtering

Many of the SCSI signals used by SCAM protocol are asserted by more than one SCAM device. Consequently, when one of these signals is released by a SCAM device there may be a transient period in which the signal is observed to be false even though it is still asserted by other SCAM devices. In order to eliminate these incorrect observations (and the consequent malfunction of the SCAM protocol), all SCAM devices shall perform wired-OR glitch filtering on the shared SCSI signals.

Wired-OR glitch filters may be designed into the hardware. In this case the hardware must be capable of detecting that a signal has remained continuously false for at least a bus settle delay. Note that this continuous observation of a signal requires dedicated hardware; it cannot be performed by software alone.

As an alternative, SCAM devices may implement wired-OR glitch filtering in software if the procedure described below is used. The algorithm used relies on the fact that a single device that releases a wired-OR signal can cause the signal to be incorrectly observed false for a maximum of a bus settle delay.

1) Determine the iteration count to be used in the software polling loop. This is typically 8, 16 or 32 if the SCAM device has knowledge (by means beyond the scope of this annex) that the SCSI bus can support the maximum number of devices. SCAM devices that have no means to determine the width of the SCSI bus should use an iteration count of 32.
2) If the signal is observed to be true, reset the iteration count to the initial value determined above. If the signal is observed to be false, decrement the iteration count. If the iteration count is zero, the signal has been released by all devices.
3) Wait sufficient time to guarantee that at least a bus settle delay elapses. Continue with the preceding step.

As an alternative to waiting at least a bus settle delay between samples, the implementor may wish to calculate the iteration count as follows. If the minimum sample interval is known, calculate N equal to a bus settle delay divided by the minimum sample interval. Round the number obtained up to the next higher integer. If the iteration count is set to N times the maximum number of devices on the SCSI bus, the algorithm above can be used without the need to wait between successive samples.

B.5.1.2 Isolation stage

Many SCAM function sequences require an isolation stage, which is used to isolate or identify an individual device to perform some action. During an isolation stage each participating device sends an identification string bit serially. As it sends its identification string, each participating device compares its own identification string with the strings of other devices. If a device observes a numerically higher string than its own identification string, it defers for the remainder of the function sequence and participates in subsequent function sequences only after a synchronization pattern is observed. After the isolation stage completes, only the device with the numerically highest identification string is still participating, and that device performs whatever action is specified by the function code (or subsequent action code). Identification strings are sent starting with the most significant bit of the most significant byte and ending with the least significant bit of the least significant byte.

During each transfer cycle of an isolation stage, the devices that are still participating assert the DB(0) signal if the next bit of their identification string is zero, the DB(1) signal if the next bit of their identification string is one, or release the DB(4-0) signals if they have reached the end of their identification string. SCAM initiators may assert the DB(4) signal to terminate the isolation stage prematurely. Each participating device reads the data transferred during each transfer cycle and acts on the conditions defined in table B.2.

Table B.2 — Transfer cycle conditions

Bit value	Asserted on DB(4-0)	Latched from DB(4-0)	Condition
0	00001b	00001b	Continue
		00011b	Defer
1	00010b	0001xb	Continue
none	00000b	000x1b	Defer
		0001xb	Defer
		00000b	Terminate
any	000xxb	100xxb	Terminate
		any other value	Error

The continue condition means the device shall continue to participate in the isolation stage.

The defer condition means that the device has lost to a device with a higher identification string. The device shall continue to handshake data on the DB(7-5) signals at the same time the DB(4-0) signals are released. The device shall continue in this fashion until the next synchronization pattern is observed, after which the device may respond to the function code that follows.

The terminate condition means that the isolation stage has terminated. The action to be performed by the remaining device(s) is either implicit in the function code or specified by subsequent transfer cycles in the function sequence. Usually only one SCAM device will still be participating and perform the action. However, if a SCAM initiator terminates the isolation phase by asserting the DB(4) signal, multiple devices may perform the action. SCAM targets shall not differentiate these cases, they shall act the same regardless of how the isolation stage was terminated. It is the responsibility of the SCAM initiator(s) to determine whether multiple devices remain (perhaps using configuration knowledge outside the scope of this annex) and ensure that suitable actions are performed.

The error condition implies that a bus error or reserved pattern was encountered. It is typically treated the same as the defer condition; the exact treatment is described in the individual function sequence descriptions.

SCAM initiators typically examine the identification strings for use in determining the nature of the isolated device and what action should be performed. The identification string of the isolated device is obtained from the DB(1) signal. The end of the identification string is recognized when both the DB(0) and DB(1) signals are false.

The structure of the identification string is shown in table B.3.

Table B.3 — Identification string

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			Type code				
1								(LSB)
2	(MSB)			Vendor identification				
9								(LSB)
10	(MSB)			Vendor specific code (up to 21 bytes)				
30								(LSB)

The identification string, at present, has a maximum length of 31 bytes. SCAM initiators shall accept identification strings up to 32 bytes total length in order to permit future SCAM protocol extensions.

The first (most significant) two bytes of a device identification string contain a type code. The contents of the type code bytes are defined in table B.4. Reserved bits in the type code shall be broadcast as zeros. A SCAM device that receives a one in any reserved bit shall defer for the remainder of the function sequence.

Table B.4 — Type code

Bit / Byte	7	6	5	4	3	2	1	0
0	Priority code		Maximum ID code		Reserved	ID Valid		SNA
1	Reserved			ID				

The priority code field contains a value specific to the function code that preceded isolation. If the function code is Isolate or Isolate and Set Priority Flag, the priority code is the device's priority flag followed by a zero. All SCAM devices maintain a priority flag, which is set to one upon power-on or after a reset indication. The value of the priority flag may also be explicitly controlled by SCAM function and action codes. If the function code is Dominant Initiator Contention, the priority code is the dominance preference code (see table B.5).

The maximum ID code encodes the largest SCSI ID that may be assigned to the device is shown in table B.5.

Table B.5 — Maximum ID code

0b	the device may be assigned an SCSI ID up to 1Fh
01b	the device may be assigned an SCSI ID up to 0Fh
10b	the device may be assigned an SCSI ID up to 07h
11b	reserved

The ID valid field encodes the validity and meaning of the contents of the ID field as defined in table B.6.

Table B.6 — ID field meaning

00b	the ID field is not valid and shall be zero
01b	the ID field contains the device's current ID but the device has not yet been assigned an ID
10b	the ID field contains the devices assigned ID
11b	reserved

All SCAM targets have a current ID, but do not necessarily have an assigned ID. It is possible for SCAM initiators to have no ID, in which case they report that the ID field is not valid.

A serial number available (SNA) bit of zero indicates the entire identification string is unavailable and will not be available until a lengthy delay (e.g., for a mechanical device access). A serial number available bit of one indicates the device's entire identification string is present. SCAM devices shall insure that both type code bytes and the most significant bit of the vendor ID code are available at all times. If the device's identification string is not yet available and the device continues to participate in the isolation stage, the device shall stall some subsequent data transfer cycle until its identification information is available.

> Note 11 Some SCAM initiators may assert the DB(4) signal to terminate the isolation stage if this bit is zero, with the intention to retry the function sequence after a delay. For this reason devices should obtain their full identification string as soon as possible in preparation for future isolation stages.

The ID field contains the device's current but unassigned ID, the device's assigned ID or an undefined value as indicated by the ID valid field.

The vendor identification field contains eight bytes of ASCII data identifying the vendor of the SCAM device. The data shall be identical to the vendor identification field returned in INQUIRY data for the device.

The vendor specific code contains up to 21 bytes of data that, together with the vendor identification field, uniquely identify the SCAM device on the bus. The device vendor shall select the vendor specific code such that no two devices from the same vendor on the same bus have identical values. The recommended method for creation of the vendor specific code is to concatenate the model identification with the device serial number.

> Note 12 The vendor specific code should be an ASCII data field that contains only graphic codes (i.e., code values 20h through 7Eh, inclusive). Unused bytes should occupy the least significant bytes of the field and be filled with space characters (20h).

B.5.1.3 Function sequences

Related transfer cycles are grouped into function sequences. Each function sequence serves a distinct purpose, such as assigning an ID to a single device.

Each function starts with a transfer cycle in which a synchronization pattern, all ones on the DB(4-0) signals, is broadcast. SCAM initiators assert the synchronization pattern to begin a new function sequence. SCAM targets shall recognize the synchronization pattern and begin a new function sequence regardless of whether the previous function sequence has been completed. Note that SCAM initiators may assert the synchronization pattern at any time to abort a function sequence and begin a new one.

The second transfer cycle in each function sequence specifies a function code. SCAM initiators may each assert a function code, and the resultant function code is the logical-OR of all of these codes. The operation of the function sequence and the number of subsequent transfer cycles (if any) that comprise the function sequence are determined by this resultant function code.

SCAM targets shall ignore any function sequences whose resultant function codes are reserved or are codes they do not recognize. A SCAM target ignores a function sequence by continuing the transfer cycle handshake sequence, releasing the DB(4-0) signals and ignoring the data received. This continues until the SCAM target receives the next function sequence synchronization pattern.

The following function codes are defined in table B.7.

Table B.7 — Function codes

Function Code	Description
00000b	Isolate
00001b	Isolate and set priority flag
00010b	reserved
00011b	Configuration process complete
00100b to 01110b	reserved
01111b	Dominant initiator contention
10000b to 11110b	reserved
11111b	Synchronization

B.5.1.3.1 Isolate function

This function code may be used by SCAM initiators to assign ID's to SCAM devices. After the function code, SCAM targets with unassigned ID's participate in an isolation stage. This stage normally terminates with a single SCAM target isolated. At this point, the SCAM initiator may broadcast an action code to assign an ID to the device or perform an additional function.

Note that if the SCAM initiator terminates the isolation stage by asserting the DB(4) signal more than one SCAM target may still be participating in the isolation. In this case, all the participating devices receive the action code and perform the requested operation.

Action codes are two quintets broadcast by SCAM transfer cycles on the DB(4-0) signals. In each quintet, the DB(2-0) signals contain a three-bit code value and the DB(4-3) signals contain two check bits. The value in the DB(4-3) signals is the count of zero bits present in the DB(2-0) signals. This scheme ensures conflict detection if multiple SCAM initiators erroneously broadcast different action codes.

The action codes are defined in table B.8 below.

Table B.8 — Action codes

First quintet	Second quintet	Description
11000b	ccnnnb	Assign ID 00nnnb
10001b	ccnnnb	Assign ID 01nnnb
10010b	ccnnnb	Assign ID 10nnnb
01011b	ccnnnb	Assign ID 11nnnb
10100b	11000b	Clear priority flag
	10010b	Locate on
	01011b	Locate off
	others	Reserved
others		Reserved

An action code is valid if the check bits are correct and both quintets are received. ID assignment action codes shall also specify an ID that the device can support. Isolated device(s) perform a valid action code when it is received. Transfer cycles after a valid action code and preceding the next synchronization pattern shall be ignored.

The Clear Priority Flag action code instructs the isolated device(s) to clear the priority flag. This function is typically used when the SCAM initiator wishes to defer the assignment of an ID to the isolated device(s) until a later function sequence.

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.

B.5.1.3.2 Isolate 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.

B.5.1.3.3 Configuration process complete function

The Configuration Process Complete function is issued by the dominant SCAM initiator when the bus configuration 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 assignment of an ID during a subsequent SCAM protocol invocation.

B.5.1.3.4 Dominant 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 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 a reset request.

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 initiators is defined in table B.9.

Table B.9 — Dominance preference code

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

B.6 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 necessary to understand the operations of both SCAM initiators and targets, as described below, and their interactions to obtain a clear picture of SCAM operations.

B.6.1 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 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 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 numerically 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 13 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 initiator. 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.

B.6.1.1 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. 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 categorization and assignment are performed as specified below.

B.6.1.1.1 SCSI ID categorization

After a reset indication, a dominant SCAM initiator shall wait as necessary to insure that a SCAM tolerant reset to selection delay has elapsed. The dominant SCAM initiator shall initialize an internal table of SCSI ID's to indicate that all SCSI ID's are uncategorized. A dominant SCAM initiator shall categorize each uncategorized ID by winning arbitration and selecting the uncategorized ID with a selection timeout delay greater than the SCAM tolerant selection response time and less than the SCAM unassigned ID selection response delay. If the dominant SCAM initiator has an assigned ID, it may use it to arbitrate, otherwise it shall arbitrate without an ID.

If a selection timeout is detected, the dominant SCAM initiator shall categorize the ID as unassigned. If the SCSI device responds to selection with a selection confirmation, the dominant SCAM initiator shall categorize the ID as assigned. In this case, the dominant SCAM initiator should complete an INQUIRY or similar command sequence to gracefully conclude selection of the SCSI device.

The dominant SCAM initiator shall repeat this process until all SCSI ID's have been categorized as either assigned or unassigned. Note that SCSI ID's may be categorized by means outside the scope of this annex, for example, by configuration parameters. This may eliminate the need for SCSI ID categorization altogether.

B.6.1.1.2 SCSI ID assignment

Once all SCSI ID's are categorized, the dominant SCAM initiator should initiate SCAM protocol and iteratively isolate and assign ID's to all SCAM devices. The dominant SCAM initiator should perform a Dominant Initiator Contention function sequence to guaranty that it remains the dominant initiator. If the formerly dominant SCAM initiator loses dominant initiator contention, it should continue to participate in SCAM protocol but function as a subordinate SCAM initiator.

Once the assignment of SCSI ID's is completed, through one or more instances of SCAM protocol, the dominant SCAM initiator should broadcast a Configuration Process Complete function sequence and terminate SCAM protocol.

B.6.1.2 Subordinate SCAM initiator

A subordinate SCAM initiator shall continue to participate in the SCAM protocol and respond to all SCAM function sequences. If the subordinate SCAM initiator does not have an assigned ID, this is necessary so that the dominant SCAM initiator may assign an SCSI ID. Unlike a SCAM target, a subordinate SCAM initiator should not release all signals and stop participation in SCAM protocol once it has been assigned an ID. Instead, it should recognize only synchronization patterns and the Configuration Process Complete function sequence.

If the subordinate SCAM initiator detects the termination of SCAM protocol but has not observed a Configuration Process Complete function sequence, it shall not resume normal SCSI operations. Level 2 SCAM initiators shall continue to be able to detect the initiation of SCAM protocol.

B.6.2 Level 1 SCAM target

Level 1 SCAM target operation is illustrated in figure B.2 below. State names are referenced in the description that follows. Note a reset indication shall cause an exit from any state and places the SCAM target in the Reset Delay state.

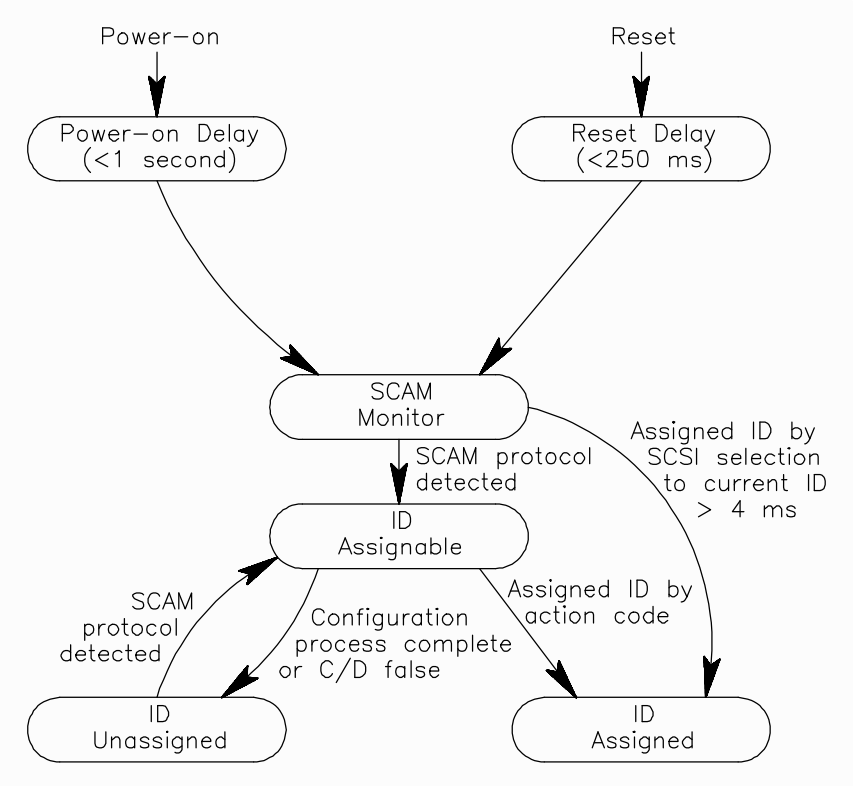

Figure B.7— Level 1 SCAM target states

When a SCAM target is powered-on, it immediately enters the Power-On Delay state and may perform local initialization. The SCAM target shall leave this state and enter the SCAM Monitor state within a SCAM power-on to SCAM selection delay.

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 signals required for selection have been continuously valid for at least a SCAM unassigned ID selection response delay, the SCAM target shall generate a selection confirmation. This response to selection implicitly causes the SCAM target to enter the ID Assigned state just as if an explicit ID assignment had been received. The assigned ID is set to the current ID and the SCAM target now functions as a SCAM tolerant device.

A SCAM target remains in the ID Assignable state as long as SCAM protocol is maintained until explicit SCAM functions change its state. If a SCAM target is isolated and receives an Assign ID action code, the ID specified becomes both the current and assigned ID. The SCAM target releases all SCSI bus signals and enters the Assigned ID state. If the SCAM target receives a Configuration Process Complete function code or if SCAM protocol is terminated (the C/D signal is false), it should release all SCSI bus signals and enter the ID Unassigned state.

Note 14 Some SCAM targets do not recognize the Configuration Process Complete function code and return to the SCAM Monitor state when SCAM protocol is terminated.

A SCAM target in the ID Unassigned state has not had any SCSI ID explicitly or implicitly assigned and shall not respond to SCSI selections for its current ID regardless of the duration. With the exception of a power-on or reset indication, only the detection of SCAM protocol initiation shall cause the SCAM target to leave the ID Unassigned state.

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.

B.7.3 Level 2 SCAM target

Level 2 SCAM target operation is illustrated in Figure B-3 below. State names are referenced in the description that follows. Note a reset indication shall cause an exit from any state and places the SCAM target in the Reset Delay state.

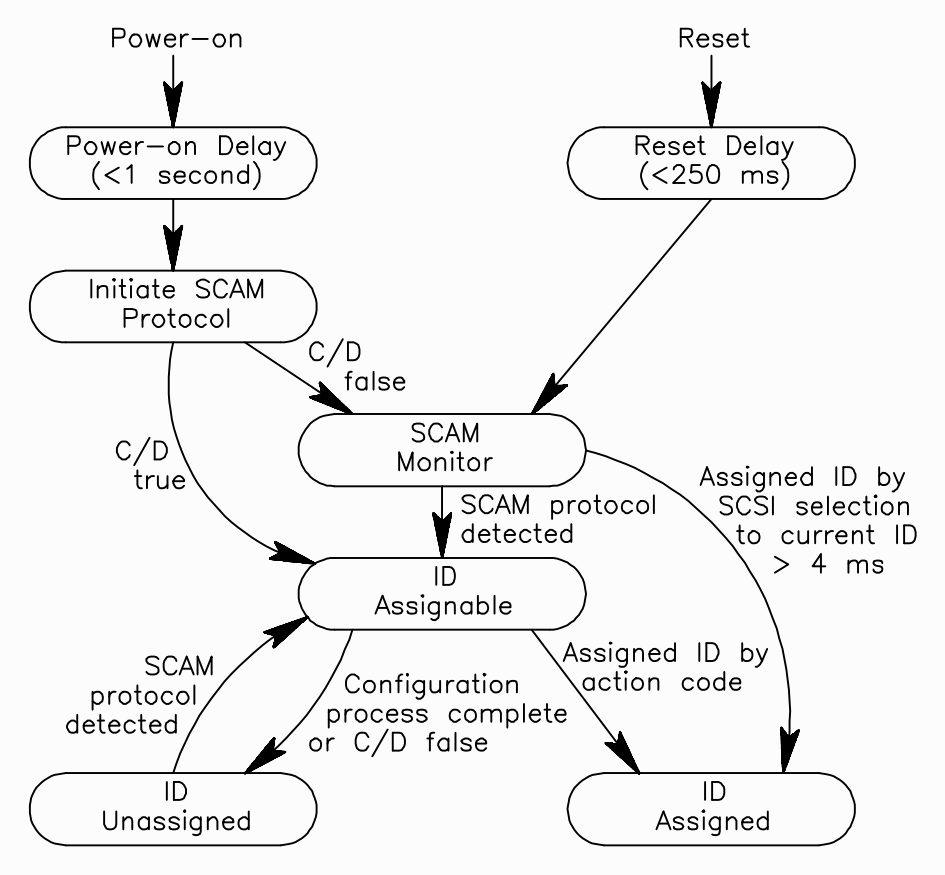

Figure B.8— Level 2 SCAM target states

When a SCAM target is powered-on, it immediately enters the Power-On Delay state and may perform 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-

nals required for selection have been continuously valid for at least a SCAM unassigned ID selection response delay, the SCAM target shall generate a selection confirmation. This response to selection implicitly causes the SCAM target to enter the ID Assigned state just as if an explicit ID assignment had been received. The assigned ID is set to the current ID and the SCAM target now functions as a SCAM tolerant device.

A SCAM target remains in the ID Assignable state as long as SCAM protocol is maintained until explicit SCAM functions change its state. If a SCAM target is isolated and receives an Assign ID action code, the ID specified becomes both the current and assigned ID. The SCAM target releases all SCSI bus signals and enters the Assigned ID state. If the SCAM target receives a Configuration Process Complete function code or if SCAM protocol is terminated (the C/D signal is false), it should release all SCSI bus signals and enter the ID Unassigned state.

Note 15 Some early implementations of SCAM targets do not recognize the Configuration Process Complete function code and return to the SCAM Monitor state when SCAM protocol is terminated.

A SCAM target in the ID Unassigned state has not had any SCSI ID explicitly or implicitly assigned and shall not respond to SCSI selections for its current ID regardless of the duration. With the exception of a power-on or reset indication, only the detection of SCAM protocol initiation shall cause the SCAM target to leave the ID Unassigned state.

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.

Annex D

(informative)

Cabling and cable measurement method recommendations

D.1 Cabling

To minimize discontinuities and signal reflections, the use of cables with different impedances in the same bus should be minimized. Implementations may require trade-offs in shielding effectiveness, cable length, the number of loads, transfer rates, and cost to achieve satisfactory system operation. To minimize discontinuities due to local impedance variation, a flat cable should be spaced at least 1,27 mm (0,050 in) from other cables, any other conductor, or the cable itself when the cable is folded. Also, use of 26 AWG wire in 1,27 mm (0,050 in) pitch flat cable will more closely match impedances of many round shielded cables, resulting in fewer impedance discontinuities and therefore, improved signal quality.

When mixing devices of different widths, particular care should be taken to not exceed the skew allowances provided by the cable skew delay and the deskew delay. These timing parameters can be lowered by reducing SCSI device input capacitance, SCSI device stub length, and the number of SCSI devices attached to the bus. The same precautions should be taken on busses with single-ended devices using fast synchronous data transfers in order to maintain system integrity.

D.2 Cable measurement

The following test procedures are recommended for measuring cable parameters. In addition to the referenced standards, single-ended measurements are made between the signal wire of the pair under test and the ground wire of all pairs connected to the shield.

The following procedure prepares the cable sample for the testing of differential impedance, single-end mode impedance and propagation delay.

a) Cut sample cable length to 6 m.

b) Remove 5.0 cm of outer jacket at each end of the cable sample.

c) Comb out braid wire strands to form a pigtail.

d) Trim filler and tape materials.

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

D.2.1 Impedance, TDR, single-ended

Using a time domain reflectometer with a 500 ps maximum rise time, on a 6 m cable sample length, measure the cable impedance between the signal wire of a particular pair and the ground wire of all pairs connected to the shield. The impedance will be averaged between 2 ns and 4 ns from the test fixture/cable interface.

D.2.2 Impedance, TDR, differential

On a 6 m (20 ft) cable sample length, select the pair to be measured. Tie all other wires and the shield together. Using a time domain reflectometer with a 500 ps maximum rise time, make the three measurements indicted in figure D.1. The values for each measurement are to be averaged between 2 ns and 4 ns from the test fixture/cable interface.

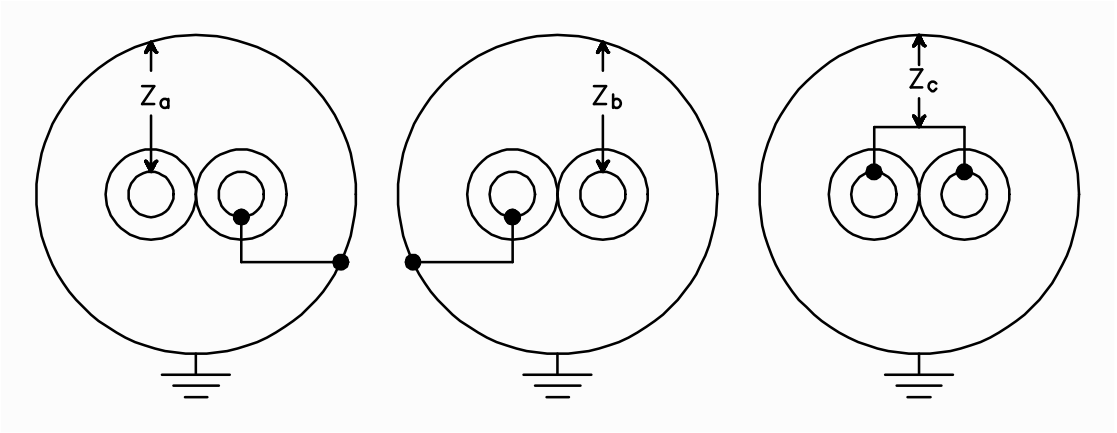

Figure D.1— Differential impedance measurement

Calculate the differential impedance of the cable using the following equation:

$$\frac{4Z_c(Z_z + Z_b)}{8Z_c - (Z_a + Z_b)}$$

Differential impedance measurements may also be performed using single and dual step differential time domain reflectometers.

D.1.3 Attenuation, differential

Measured in accordance with ASTM D-4566 at a test frequency of 5 Mhz.

D.1.4 Velocity (propagation delay) and skew

Propagation delay is the time it takes a signal to traverse a length of cable. Using a pulse generator with a 1 ns maximum rise time and an oscilloscope or a time domain reflectometer, on a 6 m (20 ft), cable sample length, select the pair to be evaluated. The shield and other pairs are unterminated. Measure the difference between the input and output signal corresponding to the 50% level.

Propagation delay skew is the difference between the maximum and minimum measured propagation delay.

D.1.5 D.C. resistance

Measured in accordance with ASTM D-4566.