**To:** X3T9.2 Committee Membership

**From:** Edward A. Gardner, Digital Equipment Corporation

**Subject:** SCSI Configured AutoMagically

This proposal describes a protocol for ID assignment in parallel SCSI without the use of jumpers or similar configuration settings. It addresses the issues that came up in discussion of Jim McGrath's "Son of SPASTIC" proposal at the Santa Fe meeting. In particular, it allows systems with multiple devices that assign IDs (e.g., multiple hosts assigning IDs for disks) and devices that power up after the system has performed ID assignment. The proposal name has been changed in accordance with John Lohmeyer's comments on the SCSI reflector.

Please send comments to the SCSI reflector or to:

Edward A. Gardner voice: (719) 548-2247
Digital Equipment Corporation FAX: (719) 548-3364
CXO 1-2 / N26 email: gardner@ssag.enet.dec.com
301 Rockrimmon Blvd., South
Colorado Springs, CO 80919-2398

## 1. Terminology

The **SCAM protocol** is defined by this document. A **SCAM device** is any SCSI device that implements the SCAM protocol. A **non-SCAM device** is any SCSI device that does not implement the SCAM protocol. All existing SCSI devices are non-SCAM devices.

A SCSI device may use either a **hard ID** or a **soft ID**. Hard IDs are selected with jumpers or equivalent configuration settings. Soft IDs are assigned with the SCAM protocol. Non-SCAM devices always use hard IDs.

SCAM devices implement either Level 1 or Level 2 of the SCAM protocol. Each SCAM device acts as either a SCAM master or a SCAM slave**.**

**SCAM master devices** control the assignment of soft IDs, in particular which device gets what ID. Level 1 SCAM master devices use hard IDs. Level 2 SCAM master devices may use either hard IDs or a soft IDs. There may be several level 2 SCAM master devices on a SCAM capable bus.

**SCAM slave devices** receive soft ID assignments through the SCAM protocol. A slave device may have an optional **default ID**. If the slave device is on a SCAM capable bus it uses a soft ID, if it is on a non-SCAM bus it uses its default ID.

A SCSI bus is **SCAM capable** if it has one or more SCAM master devices attached to it. A SCSI bus is a **non-SCAM bus** if it has no SCAM master devices attached to it.

**Level 1 SCAM** is expected to be implementable with many (but not all) existing interface chips, but requires certain configuration restrictions. **Level 2 SCAM** alleviates those configuration restrictions, but uses additional functions that are likely to require hardware interface changes. The configuration differences between level 1 and level 2 SCAM are:

1. Level 1 SCAM master devices use hard IDs. Level 2 SCAM masters may have hard or soft IDs.
2. Level 1 SCAM master devices must be the only SCAM master on their bus. There may be multiple level 2 SCAM masters on the same bus.
3. If either the master or a slave device is level 1, then either the slave must power up before the master, or both master and slave must power up concurrently. If the master device(s) and the slave device are level 2, then they may power up independently.

Note that these configuration restrictions might also be overcome by means outside the scope of SCAM. For example, support for SCAM slave devices that power up independently of the system as a whole might be incorporated if user actions (e.g., a reference to a previously unknown device) are used to trigger the SCAM protocol.

A **SCAM tolerant** device is a non-SCAM device that satisfies certain requirements on responding to selection. These requirements ensure that SCAM tolerant devices will be detected by SCAM masters, allowing SCAM tolerant devices to be freely intermixed with SCAM devices. SCAM intolerant devices cannot be reliably detected by SCAM masters. If a SCAM intolerant device is present in a SCAM system, some means outside the scope of SCAM (e.g., a manual configuration setting) must be used to ensure that the intolerant device's ID is not assigned to a SCAM device.

# 2. SCAM Timing and Interface Requirements

## 2.1. SCAM Tolerant Devices

A SCAM tolerant device shall enable its response to selection within a SCAM tolerant power-on to selection time after the device powers-on. It shall re-enable its response to selection within a SCAM tolerant reset to selection time after a reset condition. Once its response to selection is enabled, the device shall assert BSY no later than a SCAM tolerant selection response time following the appearance on the bus of a valid SELECTION phase containing its ID.

SCAM tolerant devices shall respond to single initiator selection as defined in SCSI-1 as well as normal SCSI-2 selection. That is, SCAM tolerant devices shall respond when just their own ID is asserted during a selection phase, without an initiator ID present, as well as when an initiator's ID is asserted along with their own. When selected without an initiator ID, SCAM tolerant devices should accept and process simple commands (e.g., INQUIRY) without disconnecting. Note that selection without a detectable initiator ID may occur in non-SCAM systems when a wide device selects a narrow device.

**Notes:**

1. The above are requirements to be characterized as a SCAM tolerant device, not simply recommendations as in SCSI. This characterization of SCAM tolerant devices is not intended to apply to all existing SCSI devices. Rather, it is intended to characterize devices that can be conveniently supported in a SCAM environment. The convenience I am discussing is that of the end user, such as a technically naive PC owner and user. Convenient support requires that non-SCAM devices be detected automatically. The rules for SCAM tolerant devices are simply the rules necessary to ensure that SCAM masters can reliably detect non-SCAM devices. Of necessity these rules assume that the user will be told to always power-on external boxes before powering-on his or her PC, and actually adheres to this stricture.

   Devices that do not satisfy the requirements for SCAM tolerant devices can still be used on a SCAM system. However, doing so will require special effort by the user or his system administrator. The SCAM master (typically the host adapter) will need to be informed of the ID used by the SCAM intolerant device. The means for doing so are outside the scope of SCAM.

2. Given that all other devices are powered-on before or concurrently with the SCAM master (typically the host adapter), the SCAM master can scan the bus to determine which IDs are in use by non-SCAM devices. However, this only works if the non-SCAM devices are responding to selection by the time the SCAM master scans the bus.

   The SCAM tolerant power-on to selection time exists to ensure that SCAM tolerant devices respond when the SCAM master scans the bus. Making this parameter larger allows more devices to be characterized as SCAM tolerant. However, nearly all systems will need to delay this much time before they can begin booting after power-on. Increasing this parameter risks exceeding human patience, resulting in system vendors using a shorter limit and the "SCAM tolerant" characterization being useless.

   I am recommending that the SCAM tolerant power-on to selection time be 5 seconds. I believe this is the maximum acceptable value, that anything larger would exceed human patience and make this exercise useless. I would personally prefer a shorter time, but am concerned that that may be placing aesthetics and architectural purity over practicality. After checking the characteristics of many devices, the following led to my recommending 5 seconds:

   a. I know of several disk drives that do not respond to selection until 3 to 5 seconds after power-on. These disk drives are commonly used in PCs today without difficulty.

   b. In a discussion of this with a manufacturer of PC SCSI adapters, 5 seconds was characterized as reasonable. The events between power-on and scanning the SCSI bus (BIOS diagnostics, memory scan, adapter diagnostics, SCSI reset and delay) typically take about this long.

3. After completing its power-on initialization, a SCAM tolerant device is required to respond to selection (assert BSY) quickly. I am recommending that this value, the SCAM tolerant selection response time, be 500 microseconds. I chose this value because I know of no significant benefit to making it any smaller. The belief is that response to selection

is performed by hardware that, once enabled, responds within a few microseconds at most. Note that SCAM merely requires that BSY be asserted. However, while SCAM does not require that any commands be processed, other host software might expect to issue commands such as INQUIRY.

The purpose of requiring rapid response to selection is to allow SCAM masters (host adapters) to distinguish between SCAM tolerant devices (old devices) and SCAM devices with default IDs. SCAM tolerant devices respond to selection quickly; SCAM devices with default IDs respond slowly the first time they are selected. Thus a SCAM master can use a relatively short selection time-out delay (the SCAM configuration selection time-out delay) to locate SCAM tolerant devices.

## 2.2. SCAM Level 1 Devices

Level 1 SCAM master devices:

1. shall recognize reset conditions, regardless of whether they are using the bus or any SCSI devices at the time the reset occurs.
2. shall be able to perform SCAM selection. Level 1 SCAM master devices need not recognize or respond to SCAM selection.
3. shall have a hard ID.
4. shall be able to use a selection time-out, during initial configuration, within the range from a SCAM tolerant selection response time (minimum) through a SCAM default ID selection response time (maximum).
5. shall not assert RST upon a selection time-out.
6. shall satisfy the requirements for SCAM tolerant devices.

Level 1 SCAM slave devices:

7. shall recognize reset conditions, regardless of whether they are using the bus or processing commands at the time the reset occurs.
8. shall recognize and respond to SCAM selection within a long SCAM selection time, provided that the device has not been assigned a soft ID, has not confirmed its default ID, and that both a SCAM power-on to SCAM selection time has elapsed since the device most recently powered-on and a SCAM reset to SCAM selection time has elapsed since the most recent reset condition. Level 1 SCAM slave devices do not perform SCAM selection.
9. shall satisfy the requirements for SCAM tolerant devices during normal operation, that is, from being assigned a soft ID or confirming a default ID until the device subsequently loses power or detects a reset condition. Note that SCAM slave devices do not recognize or respond to SCAM selection during normal operation.
10. may have a default ID. If a SCAM slave device has a default ID, it shall not respond (assert BSY) to selection or reselection of its unconfirmed default ID unless the SELECTION phase has remained valid for at least a SCAM default ID selection response time.
11. shall not assert RST upon a selection time-out.

12. shall implement the hard reset alternative.

## 2.3. SCAM Level 2 Devices

Level 2 SCAM master devices:

1. shall recognize reset conditions, regardless of whether they are using the bus or any SCSI devices at the time the reset occurs.
2. shall be able to perform SCAM selection. Level 2 SCAM master devices shall also recognize and respond to SCAM selection within a long SCAM selection time during normal operation.
3. shall either have a hard ID or be able to arbitrate without an ID.
4. shall be able to use a selection time-out, during initial configuration, within the range from a SCAM tolerant selection response time (minimum) through a SCAM default ID selection response time (maximum).
5. shall not assert RST upon a selection time-out.
6. shall satisfy the requirements for SCAM tolerant devices whenever they have an ID. That is, at all times if they have a hard ID, or after assigning themselves or being assigned an ID if they use soft IDs.

Level 2 SCAM slave devices:

7. shall recognize reset conditions, regardless of whether they are using the bus or processing commands at the time the reset occurs.
8. shall recognize and respond to SCAM selection within a long SCAM selection time, provided that the device has not been assigned a soft ID, has not confirmed its default ID, and that both a SCAM power-on to SCAM selection time has elapsed since the device most recently powered-on and a SCAM reset to SCAM selection time has elapsed since the most recent reset condition.
9. shall satisfy the requirements for SCAM tolerant devices during normal operation, that is, from having been assigned a soft ID or confirming a default ID until a subsequent power loss or reset condition. Note that SCAM slave devices do not recognize or respond to SCAM selection during normal operation.
10. may have a default ID. If a SCAM slave device has a default ID, it shall not respond (assert BSY) to selection or reselection of its unconfirmed default ID unless the SELECTION phase has remained valid for at least a SCAM default ID selection response time.
11. shall not assert RST upon a selection time-out.
12. shall implement the hard reset alternative.
13. after completing initialization and before beginning normal operation (before they have their ID), shall be able to arbitrate without an ID and perform SCAM selection. SCAM slave devices do not arbitrate without an ID or perform SCAM selection once they have their ID and begin normal operation..

## 2.4. Wide Device Arbitration

As specified in SCSI-2, SCSI devices wait at least an arbitration delay after asserting BSY before examining the DATA BUS to determine whether they have won or lost arbitration. SCSI-2 places no upper limit on how long a device may take to determine it has won arbitration and assert SEL.

Devices whose ID is 8 or higher (that is, devices whose ID is outside the first data byte) that might be present in SCAM systems shall conclude their examination of the DATA BUS and assert SEL if they have won arbitration no later than three arbitration delays after the time they asserted BSY to begin arbitration.

**Note:** This requirement is necessary for arbitration without an ID to work in mixed width systems. It seems reasonable to assume that all wide SCSI devices will use hardware to perform arbitration and assert SEL quickly. The three arbitration delays was confirmed by the committee at the September 1993 meeting.

## 2.5. SCAM Timing Parameters

| | |
|---|---|
| 5s | SCAM tolerant power-on to selection time |
| 250ms | SCAM tolerant reset to selection time |
| 1ms | SCAM tolerant selection response time |
| 4ms | SCAM default ID selection response time |
| 1s | SCAM power-on to SCAM selection time |
| 250ms | SCAM reset to SCAM selection time |
| 250ms | Long SCAM selection response time |
| 1ms | Short SCAM selection response time |

### 2.5.1.SCAM tolerant power-on to selection time

The maximum time a SCAM tolerant device may delay after power-on before enabling its response to selection.

### 2.5.2.SCAM tolerant reset to selection time

The maximum time a SCAM tolerant device may delay after a reset condition before enabling its response to selection.

### 2.5.3.SCAM tolerant selection response time

The maximum time in which a SCAM tolerant device may respond to selection of its ID, provided that the SCAM tolerant power-on to selection time and SCAM tolerant reset to selection time have both elapsed. Also, the minimum selection time-out delay a SCAM master should use when examining the bus for SCAM tolerant devices.

### 2.5.4.SCAM default ID selection response time

The minimum time in which a SCAM slave device may respond to selection of its unconfirmed default ID. Also, the maximum selection time-out delay a SCAM master shall use when examining the bus for SCAM tolerant devices.

### 2.5.5.SCAM power-on to SCAM selection time

The minimum time a SCAM device should delay after power on before initiating the SCAM protocol.

### 2.5.6.SCAM reset to SCAM selection time

The minimum time a SCAM device should delay after a reset condition before initiating the SCAM protocol.

### 2.5.7.Long SCAM selection response time

The minimum time a SCAM device should maintain SCAM selection in situations where a slow response is anticipated. Also the maximum time a SCAM device shall require to detect and respond to SCAM selection.

**Note:** This corresponds to the time necessary to detect and respond to SCAM selection with firmware polling.

### 2.5.8.Short SCAM selection response time

The minimum time a SCAM device should maintain SCAM selection in situations where a rapid response is anticipated. Also the recommended maximum time a SCAM device should require to detect and respond to SCAM selection.

**Note:** This corresponds to the time necessary to detect and respond to SCAM selection with hardware.

## 3. Bus Interface Requirements

The principal requirement is for interface chips to allow firmware to disable active negation and toggle individual signal lines. The underlying assumption is that the protocol will be operated by firmware, perhaps using an interface chip diagnostic mode that allows firmware control of individual signal lines. Some but not all existing interface chips provide this capability. The protocol proper is totally asynchronous and independent of firmware timing.

## 3.1. Reset Condition Recognition

SCAM master devices shall recognize when a reset condition occurs, regardless of whether they are using the bus or any SCSI devices at the time. Following a reset SCAM master devices initiate the SCAM protocol to assign soft IDs.

SCAM slave devices shall recognize when a reset condition occurs and discard their ID. Following a reset condition all SCSI devices that use soft IDs shall have their ID reassigned.

## 3.2. SCAM Selection

Certain SCAM devices perform and recognize SCAM selection. SCAM selection is a "selection phase" where MSG is asserted rather than any data bus signals. Specifically, SEL and MSG are asserted while BSY is released. Upon recognizing SCAM selection a SCAM device's SCSI interface should respond by asserting SEL and MSG itself, then interrupting the device's processor.

SCAM master devices shall be able to perform SCAM selection. This will often be implemented by direct firmware control of the individual signals, as SCAM selection is performed infrequently.

Level 1 SCAM master devices need not recognize SCAM selection. Only the master device performs SCAM selection in a level 1 SCAM system.

Level 2 SCAM master devices shall recognize and respond to SCAM selection during normal conditions. The master devices shall respond within a SCAM selection time following the appearance of SCAM selection on the bus. They shall respond within a long SCAM selection time during all normal conditions. They should respond within a short SCAM selection time whenever another device might power-on independently.

Level 2 SCAM master devices need not recognize or respond to SCAM selection during abnormal conditions. Periods of internal initialization after power-on or a bus reset condition are common examples of abnormal conditions. Following any period of abnormal conditions, each level 2 SCAM master shall first enable its recognition of and response to SCAM selection, then itself initiate the SCAM protocol. A level 2 SCAM master should spend a substantial majority of its time in normal conditions or it may appear broken.

SCAM slave devices shall recognize and respond to SCAM selection whenever the device has neither been assigned a soft ID nor confirmed its default ID since power-on or a reset condition. The slave devices shall respond within a long SCAM selection time following the appearance of SCAM selection on the bus, provided that at least a SCAM power-on to SCAM selection time has elapsed since the device most recently powered-on and at least a SCAM reset to SCAM selection time has elapsed since the most recent reset condition. SCAM slave devices need not recognize or respond to SCAM selection after they have been assigned an ID or confirmed their default ID.

Level 2 SCAM slave devices shall be able to arbitrate without an ID and perform SCAM selection when the device has neither been assigned a soft ID nor confirmed its default ID.

**Note:** SCAM slave devices only participate in the SCAM protocol when they do not yet have an ID. They do not recognize, respond to, or perform SCAM selection while they have an ID, which includes all periods of normal operation.

## 3.3. Arbitration Without an ID

Level 2 SCAM devices that use soft IDs shall be able to arbitrate without an ID. Arbitration without an ID allows devices that have not yet been assigned an ID to obtain control of the bus for initiating the SCAM protocol.

A device arbitrates without an ID by simply arbitrating for the bus without asserting any DATA BUS signals. That is, the device waits for BUS FREE, then asserts BSY without asserting any line of the DATA BUS. After waiting a minimum of four arbitration delays, the device has won arbitration if neither any DATA BUS lines nor SEL have been asserted. Note that the four arbitration delays is longer than normal SCSI arbitration; all other arbitration timing remains the same.

### 3.4. Response to Normal Selection

All SCAM and SCAM tolerant devices shall respond to selection or reselection of the device's ID within a SCAM tolerant selection response time. That is, SCAM and SCAM tolerant devices shall assert BSY no later than a SCAM tolerant selection response time after the device's ID and SEL are asserted with BSY released. This requirement applies whenever at least a SCAM tolerant power-on to selection time has elapsed since the device most recently powered-on and at least a SCAM tolerant reset to selection time has elapsed since the most recent reset condition.

SCAM slave devices shall not respond to selection or reselection of the device's unconfirmed default ID unless the Selection Phase has remained valid for at least a SCAM default ID selection response time. SCAM slave devices respond within a SCAM tolerant selection response time (preceeding paragraph) after they have been assigned a soft ID or have confirmed their default ID.

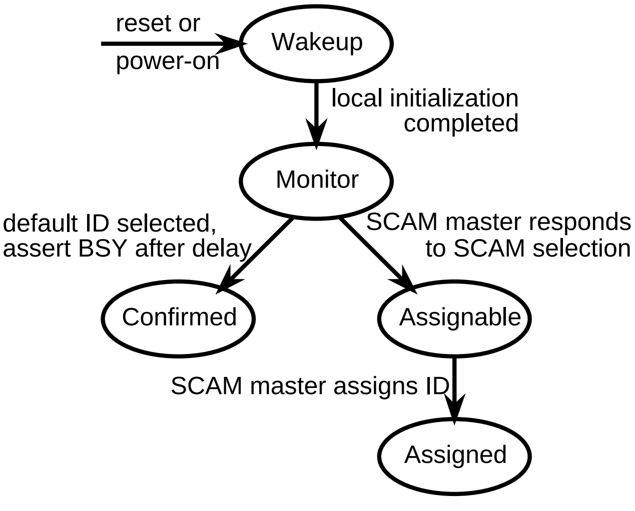
Following each power-on or reset condition, SCAM master devices shall use a selection time-out delay within the range from a SCAM tolerant selection response time (minimum) through a SCAM default ID selection response time (maximum). They shall continue using a selection time-out delay in that range until they have completed examining the bus for SCAM tolerant devices.

### 3.5. Hard reset alternative

All SCAM and SCAM tolerant devices shall implement the hard reset alternative.

### 3.6. SELECTION time-out procedure

SCAM master devices shall implement option b as specified in clause 6.1.3.1, SELECTION time-out procedure, of SCSI-2 (X3T9.2/375R revision 10k). That is, SCAM master devices shall not assert RST upon a selection time-out.


reset or
power-on
Wakeup
local initialization completed
Monitor
default ID selected, assert BSY after delay
SCAM master responds to SCAM selection
Confirmed
Assignable
SCAM master assigns ID
Assigned

SCAM Slave Device Operation

## 4. SCAM Protocol

### 4.1. SCAM Slave Device Operation

SCAM slave device operation is illustrated in the accompanying figure. State names from the figure are referenced parenthetically in the following description.

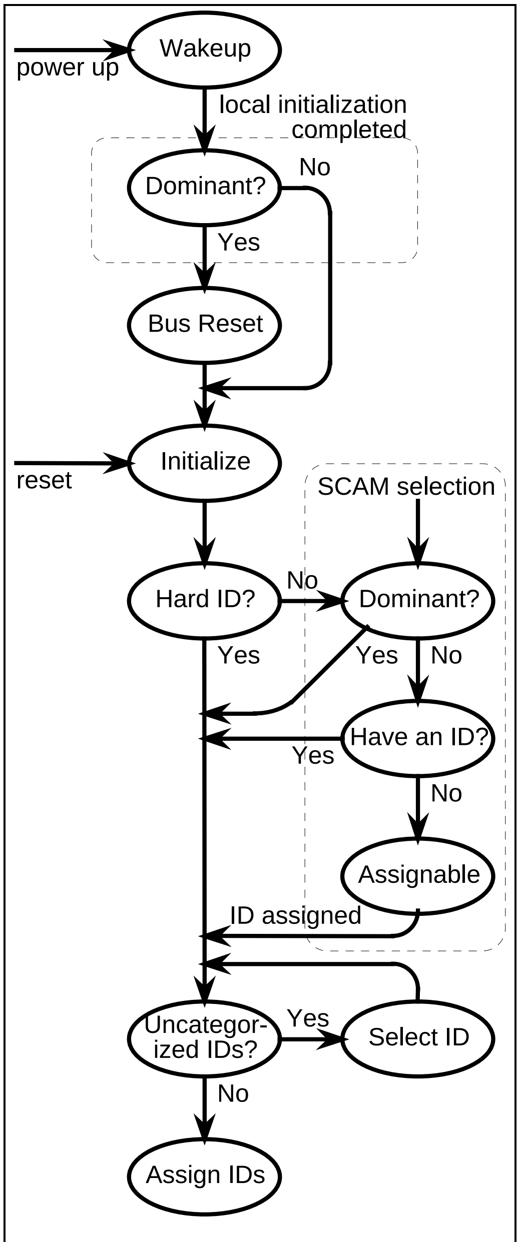
Following a reset condition or power-on, a SCAM slave device shall cease responding to its former ID and perform local initialization (Wakeup state). After completing its local initialization, the SCAM slave device shall monitor the bus for selection or reselection of its default ID (if any) or for SCAM selection (Monitor state). A SCAM slave device shall enter the Monitor state no later than a SCAM power-on to SCAM selection time following power-on or a SCAM reset to SCAM selection time following a reset condition.

If a SCAM slave device detects selection or reselection of its default ID while in the Monitor state, the device shall wait a minimum of a SCAM default ID selection response time before asserting BSY. If the selection or reselection phase persists for longer than that time, the SCAM slave device should assert BSY, provided it does so within the usual rules for responding to selection or reselection. The SCAM slave device shall confirm its default ID (Confirmed state) if and only if it asserts BSY in response to selection or reselection of its default ID. A device that has confirmed its default ID (is in the Confirmed state) should ignore SCAM selection and shall respond to subsequent selection or reselection of its default ID within a SCAM tolerant selection response time. The device's default ID remains confirmed until the next reset condition or loss of power.

If a SCAM slave device detects or initiates SCAM selection while in the Monitor state, the device shall itself respond to SCAM selection, then determine whether a SCAM master has responded as well (i.e., whether C/D is asserted). Upon detecting that a SCAM master has responded the slave device shall cease monitoring the bus for selection or reselection of its default ID and wait for an ID assignment (Assignable state). The device may receive an ID assignment during the same SCAM protocol invocation (Monitor state to Assignable state to Assigned state all in a single invocation) or in a subsequent SCAM protocol invocation (Monitor state to Assignable state in one invocation and Assignable state to Assigned state in a later invocation). While in the Assignable state the device shall continue to monitor the bus for SCAM selection, but shall not respond to selection or reselection of any ID.

Upon receiving a soft ID assignment (Assigned state) a SCAM slave device should ignore SCAM selection and shall respond to subsequent selection or reselection of its soft ID within a SCAM tolerant selection response time. The device continues to use its soft ID until the next reset condition or loss of power.

A Level 2 SCAM slave device may solicit ID assignment while in the Monitor state, by first arbitrating without an ID then performing SCAM selection after winning arbitration. The Level 2 SCAM slave device shall continue to monitor the bus for selection or reselection of its default ID or for SCAM Selection while attempting to arbitrate without an ID. Typically a SCAM slave device should only solicit ID assignment if there has been no bus reset condition since it last powered-on. After power-on, a SCAM slave device should wait both a SCAM power-on to SCAM selection time and until the device has its serial number available before its first solicitation. The SCAM slave device should solicit ID assignment several times using a Short SCAM selection response time, then solicit once or twice using a Long SCAM selection response time, then cease soliciting. Successive solicitations should be a minimum of one second apart. A SCAM slave device may generate a bus reset condition if there is no response to its solicitations, but only if there has been no other bus reset condition since it last powered up.



SCAM Master Device Operation

## 4.2. SCAM Master Device Operation

SCAM master device operation is illustrated in the accompanying figure. Portions enclosed in dashed boxes apply to Level 2 SCAM master devices. All other portions apply to both Level 1 and Level 2 SCAM master devices. State names from the figure are referenced parenthetically in the following description.

Following power-on, a Level 2 SCAM master device shall complete its local initialization (Wakeup state), then initiate the SCAM protocol and attempt to dominate other masters (first Dominant decision). The master should generate a reset condition (Bus Reset state) if and only if it succeeds in becoming the dominant master. Note that this implies that either it is the only master present or that all masters have powered-on concurrently.

A Level 1 SCAM master device, or any other SCAM master that can determine (through means outside the scope of SCAM) that it is the only master present on a bus, should generate a reset condition whenever it powers-on. Since it is the only master present, it is always the dominant master.

After power-on or following a reset condition a SCAM master shall initialize its internal table of IDs to indicate that all IDs are uncategorized (Initialize state). If it has a hard ID (Hard ID decision), it should proceed immediately with categorizing IDs (Uncategorized IDs decision). Note that Level 1 SCAM master devices always have hard IDs and therefore always take this path. If the SCAM master does not have a hard ID, it shall initiate the SCAM protocol and contend for dominance (second Dominant decision).

After determining that it must contend for dominance due to not having a hard ID, or upon detecting SCAM selection, a SCAM master shall contend for dominance (second Dominant decision). It should proceed with categorizing IDs (Uncategorized ID decision) if it achieves dominance or if it has either a hard ID or a previously assigned soft ID (Have an ID decision). If the SCAM master neither achieves dominance nor has an ID, it should adopt the role of a slave until an ID is assigned to it (Assignable state).

A SCAM master may categorize IDs when it is either dominant or has an ID. SCAM masters categorize IDs by winning arbitration and selecting an uncategorized ID using a selection time-out delay less than the SCAM default ID selection response time (Select ID state). If a target device responds and enters command phase, the master should issue an INQUIRY or similar command. A dominant master may arbitrate without an ID to categorize IDs. A master the has an ID may arbitrate using that ID to categorize IDs.

The SCAM master shall repeat this process until it has categorized all IDs (Uncategorized ID decision). It categorizes IDs in four ways:

1. The SCAM master shall categorize it's own ID (if any) as in use.
2. If a target device responds to selection of an uncategorized ID by asserting BSY, the master shall categorize that ID as in use.
3. If no device responds to selection of an uncategorized ID within a SCAM tolerant selection response time, and the SELECTION phase began later than both a SCAM tolerant power-on to selection time following the master's most recent power-on and a SCAM tolerant reset to selection time following the most recent reset condition, then the master may categorize that ID as not in use.
4. The master may categorize IDs through non-SCAM means such as configuration parameters.

Typically the master will wait until the SCAM tolerant power-on to selection time and SCAM tolerant reset to selection time have both elapsed, then select every ID other than its own. However, the master may skip any IDs categorized by configuration parameters, and may skip this entire step if all IDs are categorized by configuration parameters.

After categorizing IDs, the SCAM master device should initiate the SCAM protocol and assign IDs (Assign IDs state). Typically the master should contend for dominance, then proceed with ID assignment if and only if it achieves dominance. A level 1 SCAM master that fails to achieve dominance shall cease all SCAM activity until a subsequent reset condition or power-on. Once a master begins ID assignment it should continue assigning IDs until all devices that request an ID have been assigned an ID or all IDs are in use.

A SCAM master may initiate the SCAM protocol as often as it wishes. A level 1 master or a dominant level 2 master shall initiate the SCAM protocol (starting with SCAM selection) at least once after both the SCAM power-on to SCAM selection time and SCAM reset to SCAM selection time have elapsed. Typically those delays elapse before the first SCAM protocol initiation, but if not the SCAM protocol shall be initiated again after they elapse. The master should subsequently initiate the SCAM protocol if it can determine (via non-SCAM means) that a SCAM slave device may have powered-on or been reset.

### 4.3. SCAM Protocol Initiation

A device initiates the SCAM protocol by first winning bus arbitration, then performing SCAM selection. The device may arbitrate using a hard or soft ID if it has one, otherwise it may arbitrate without an ID. After winning arbitration the device has BSY and SEL asserted. It shall release the DATA BUS and assert MSG, then wait at least two deskew delays and release BSY. It shall maintain this pattern of SEL and MSG asserted with BSY released for a minimum of a SCAM selection time, then release MSG. After releasing MSG the device shall wait until MSG has been released by all other devices, using wired-or glitch filtering.

Level 2 SCAM master devices and SCAM slave devices that have not yet been assigned an ID recognize SCAM selection and assert SEL and MSG. After a variable delay (see below) they release MSG, then wait until MSG has been released by all devices, using wired-or glitch filtering. SCAM slave devices should release MSG quickly, perhaps never asserting it at all. SCAM master devices should wait a SCAM selection time before releasing MSG. This ensures that SCAM selection is maintained for the master's SCAM selection time parameter, regardless of the parameter setting in the device that initiates the SCAM protocol.

After detecting that MSG has been released by all devices, each SCAM device asserts BSY, waits at least two deskew delays, then asserts several other signals. SCAM master devices assert BSY followed by I/O, C/D, DB6 and DB7. SCAM slave devices assert BSY followed by I/O, DB6 and DB7. After asserting its signals each device waits at least two more deskew delays, then releases SEL and waits until SEL has been released by all devices, using wired-or glitch filtering.

After detecting that SEL has been released by all devices, the SCAM devices release DB6 and examine the bus signals. If C/D is released, then there are no SCAM master devices participating. The slave devices shall release all signals. If C/D is asserted, each SCAM device waits for DB6 to be released by all devices, using wired-or glitch filtering, then asserts SEL. Initiation of the SCAM protocol is complete after SEL has been asserted.

## 4.4. Transfer Cycles

The SCAM protocol functions through a sequence of transfer cycles. During each cycle certain devices send data to all participating SCAM devices. The actual data received is the logical-or of the data sent 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 nodes involved.

Transfer cycles use DB5-7 as handshake lines and DB0-4 as data lines. At the beginning and end of each cycle DB7 is asserted while DB6 and DB5 are released. Each device sequences through the following steps for each transfer cycle (see figure):

1. Place data on DB0-4, if the device is sending data, and assert DB5.
2. Release DB7.
3. Wait until DB7 is released by all other devices, using wired-or glitch filtering.
4. Read and latch data from DB0-4 and assert DB6.
5. Release DB5.
6. Wait until DB5 is released by all other devices, using wired-or glitch filtering.
7. Release or change DB0-4 and assert DB7.
8. Release DB6.
9. Wait until DB6 is released by all other devices, using wired-or glitch filtering.

The SCAM protocol continues through successive transfer cycles until the master device(s) choose to terminate it by releasing C/D and all other signals. Slave devices shall note the release of C/D and release all signals.

## 4.5. Iterations

Successive transfer cycles are grouped into iterations. Each iteration performs a distinct functional purpose, such as assigning an ID to a single device.

The first transfer cycle in each iteration transfers a synchronization pattern, which is all five data bits asserted. Master devices assert the synchronization pattern to begin a new iteration. Slave devices shall recognize the synchronization pattern and begin a new interation regardless of whether the previous iteration has been completed. Note that master devices may assert the synchronization pattern at any time to abort an interation and begin a new one.

The second transfer cycle in each iteration contains a function code. Master devices assert a

```
Step  |1 |2   3|  4  |5   6|7 |8   9|
      |  ___________________  |     |
-DB0-4///|     |latch|     |\\\\\\\\\
      \\\___________________/////////
      _  |     |     |     __________
 -DB5 |\ |     |     | ////|  |     |
      | \_____________//// |  |     |
      |  |     |     |     |  |     |
      ____________   |     |  |     _
 -DB6 |  |     |  \  |     |  | ////|
      |  |     |   \___________//// |
      |  |     |     |     |  |     |
      |  |     _____________  |     |
 -DB7 |  | ////|     |     |\ |     |
      ____//// |     |     | \_______
      |  |     |     |     |  |     |
```

Note: Signals are shown asserted low.

Transfer Cycles

function request. The inclusive-or of all function requests is the resultant function code, which determines the function that will be performed by the iteration. The contents of subsequent transfer cycles within the iteration (if any) are determined by the resultant function code.

Slave devices shall ignore any iterations whose resultant function codes are reserved or are codes they do not recognize. A slave device ignores an iteration by continuing the transfer cycle handshake sequence, but asserting no data bits and ignoring the data received. This continues until the slave receives the next iteration synchronization pattern.

The following function codes are defined:

| Function Code | Description |
|---|---|
| 00000b | Assign ID. |
| 00001b | Set Priority Flag. |
| 00010b to 01110b | reserved |
| 01111b | Dominant Master Contention |
| 10000b to 11110b | reserved |
| 11111b | synchronization pattern |

## 4.6. Isolation Stages

Many function codes are followed by an isolation stage, which is used to isolate or identify an individual device to perform some action. During an isolation stage each partipating device sends an identification string bit serially. As it sends its identification string, each participating device compares its own identification string against the strings of other devices. If a device observes a numerically higher string, it stops participating in the iteration. After the isolation stage completes, only the device with the numerically highest identification string is still participating, and that device performs whatever action is implied by the function 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 cycle of an isolation stage, the devices that are still participating assert DB0 if the next bit of their identification string is zero, DB1 if the next bit of their identification string is one, or no data bits if they have reached the end of their identification string. Master devices may assert DB4 to terminate the isolation stage prematurely. Each participating device reads the data transferred during each cycle and acts on the following conditions:

| Bit Value | Sent on DB4-0 | Received on DB4-0 | 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 combination | Error |

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

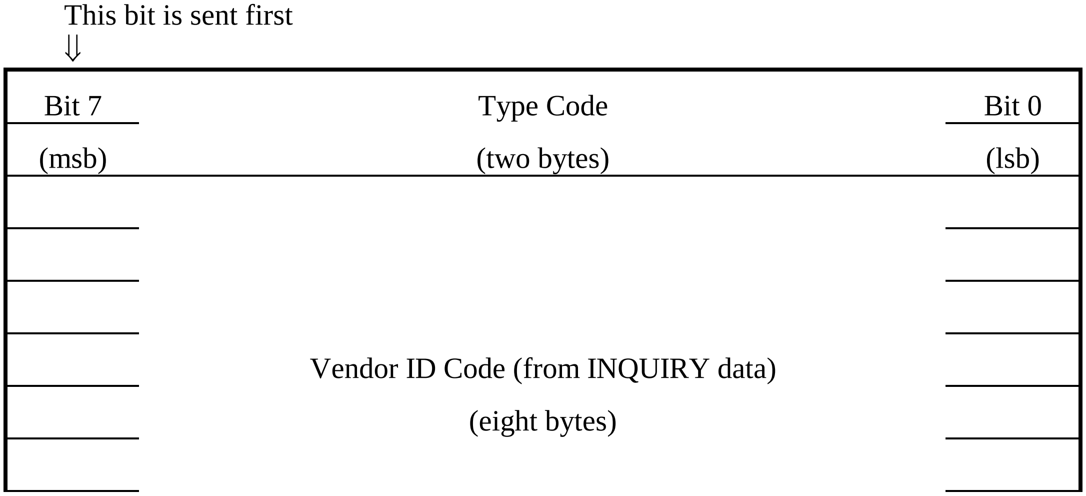
The Defer condition means that the device has "lost" to a device with a higher identification string. The device shall continue to handshake data without asserting DB4-0 and wait for the next synchronization pattern.

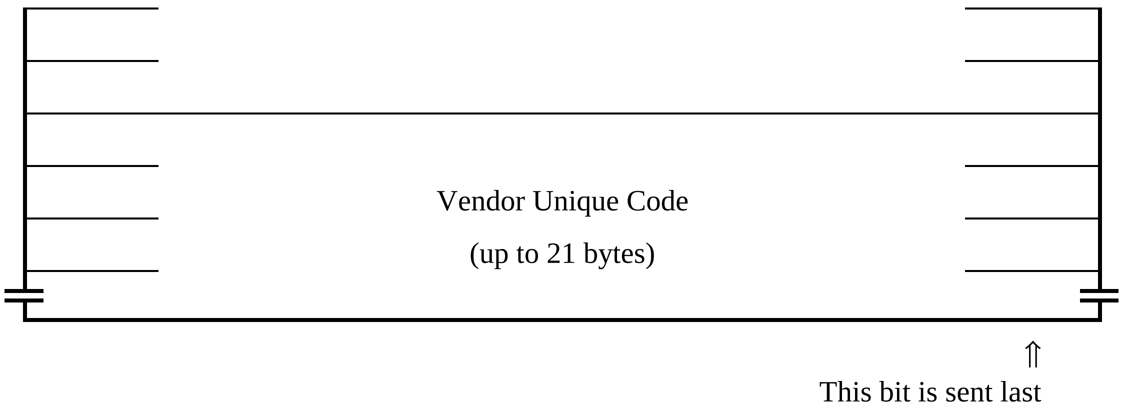
The Terminate condition means that the isolation stage has terminated. The action to be performed by the remaining device(s) is either implicit in the function code or specified by subsequent transfer cycles in the iteration. Usually only one SCAM device will still be participating and perform the action. However, if a SCAM master terminates the isolation phase by asserting DB4, multiple devices may perform the action. SCAM slave devices shall not check for this case, they shall act regardless of how the isolation stage was terminated. It is the responsibility of the master device(s) to determine whether multiple devices remain (perhaps using configuration knowledge outside the scope of SCAM) and ensure 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. Its exact treatment is described in the individual function code descriptions.

Master devices typically examine the identification strings for use in determining what action should be performed. The identification string of the "winning" device is obtained from DB1. The end of the identification string is recognized by DB0 and DB1 both released.

Identification strings consist of a two byte type code (most significant), the 8-byte Vendor ID Code (from INQUIRY data), followed by a vendor unique code (least significant). The vendor unique code may be up to 21 bytes in length. The device vendor shall select the vendor unique code to ensure that no two devices from the same vendor on the same bus contain the same code value. The recommended means is to concatenate the vendor's model identification (in ASCII) with the device's serial number (also in ASCII). However, other means are also permitted. The overall structure of identification strings is shown in the accompanying figure.





**Note:** This results in 31 bytes as the maximum identification string. However, to allow for future protocol extensions, SCAM masters shall support identification strings up to 32 bytes total length.

The first (most significant) two bytes of a device identification string contain a type code. The contents of the type code bytes are as follows:

| Bit 7<br>(msb) | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0<br>(lsb) |
|---|---|---|---|---|---|---|---|
| Priority Code | | Maximum ID Code | | reserved | ID Valid | | SNA |
| reserved | | | ID | | | | |

**Priority Code:** A code indicating the priority for a device winning an isolation stage. The values in this field depend upon the function code and are specified in the individual function code descriptions.

**Maximum ID Code:** Encodes the maximum SCSI ID that the device can accept:

| | |
|---|---|
| 00b | device can accept SCSI IDs up to 1Fh |
| 01b | device can accept SCSI IDs up to 0Fh |
| 10b | device can accept SCSI IDs up to 07h |
| 11b | reserved |

**reserved:** This bit shall be sent as 0. A device that receives a 1 in this bit shall defer for the iteration.

**ID Valid:** Indicates the validity and contents of the ID field:

| | |
|---|---|
| 00b | ID not valid. The ID field shall be sent containing zero. A device that receives a non-zero ID field shall defer for the iteration. |
| 01b | ID field contains a default ID or a soft ID. |
| 10b | ID field contains a hard ID. |
| 11b | reserved. A device that receives this ID Valid code shall defer for the iteration. |

If it has one, the device shall report its hard ID, its assigned soft ID, or its confirmed default ID. Note that these three conditions are mutually exclusive. If the device does not yet have an ID (none of these three conditions apply), it shall report its unconfirmed default ID if it has one. Otherwise it shall report ID not valid.

**SNA:** Serial Number Available. Sent as 1 if the device's full identification string is available. Sent as 0 if the full identification string will not be available until a lengthy delay has elapsed, such as for a mechanical device access. The entire type code byte and the first bit of the Vendor ID Code shall be available at all times, regardless of the setting of this bit. 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 handshake until its identification information is available.

**Note:** Upon seeing this bit clear, some masters may assert DB4 to terminate the isolation stage and retry the function after a delay. For this reason devices should obtain their full identification string in anticipation of future functions.

**reserved:** These bits shall be sent as 0. A device that receives a 1 in any reserved bit shall defer for the iteration.

**ID:** The device's default ID, assigned soft ID, hard ID, or reserved, as specified by the value in ID Valid.

## 4.7. Assign ID and Set Priority Flag Functions

These two functions both assign IDs to SCAM devices. Following the function code, SCAM devices that need to have an ID assigned participate in an isolation stage. The isolation stage normally terminates with a single remaining participating device. Then a master (usually the dominant master) may assign it an ID or instruct it to perform some other action.

Each SCAM device maintains a priority flag while the SCAM protocol is active. The priority flag's value determines the contents of the Priority Code field sent during the isolation stage for these functions. The Priority Code field shall be sent as p0b, where p is the current value of the device's priority flag. As a consequence low priority devices (p=0) will defer to high priority devices (p=1).

Each SCAM device shall set its priority flag to 1 (high priority) during SCAM selection. The Clear Priority Flag action code defined later in this section sets the priority flag to 0 (low priority). The Assign ID function leaves the priority flag unaltered, while the Set Priority Flag function sets the flag to 1. The two functions are otherwise identical.

After the isolation stage terminates, the master device(s) send an action code to the remaining participating device(s). Usually only a single device will remain. However, multiple devices may remain if a master device asserts DB4 to terminate the isolation stage, and all shall receive and act on the action code.

Action codes are two quintets sent on DB4-0. In each quintet DB2-0 contain a three bit code value and DB4-3 contain two check bits. The value in DB4-3 is the count of the number of zero bits in DB2-0. This encoding ensures detection if multiple master devices should erroneously present conflicting action codes.

The possible action codes are:

| First Quintet | Second Quintet | Description |
|---|---|---|
| 11000b | ccnnnb | Assign SCSI ID 00nnnb |
| 10001b | ccnnnb | Assign SCSI ID 01nnnb |
| 10010b | ccnnnb | Assign SCSI ID 10nnnb |
| 01011b | ccnnnb | Assign SCSI ID 11nnnb |
| 10100b | 11000b | Clear Priority Bit |
|  | 10001b | reserved |
|  | 10010b | Locate On |
|  | 01011b | Locate Off |
|  | others | reserved |
| 01101b | ccnnnb | reserved |
| 01110b | ccnnnb | reserved |
| 00111b | ccnnnb | reserved |

The Clear Priority Bit action code instructs the remaining device(s) to clear their priority flag. This function is typically used when the master(s) wish to defer assigning an ID to the device(s) until a later iteration.

The Locate On and Off action codes instruct the remaining device(s) to provide assistance for users or service personnel attempting to physically locate the device. Upon receiving a Locate On action code, the recommended action is for the remaining device(s) to flash their fault indicator or some similar indication. The indication should be cleared upon receiving a Locate Off action code, a reset condition, after a time delay, or upon other vendor unique actions.

An ction code is valid if the check bits are correct and both quintets are received. ID assignment action codes must also identify an ID that the device can support. The remaining device(s) perform a valid action code as soon as they receive it. Transfer cycles after a valid action code and preceeding the next synchronization pattern shall be ignored.

A SCAM slave device that receives a valid ID assignment should release all bus signals and cease participating in the SCAM protocol until the next reset condition or power-on. SCAM slave devices 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. Not receiving an action code is typically caused by a master device choosing to abort a function by asserting the synchronization pattern.

## 4.8. Dominant Master Contention Function

The Dominant Master Contention function selects one master device, called the dominant master, from possibly multiple masters that may be present. Level 2 SCAM master devices shall specify the Dominant Master Contention function for the first iteration following each SCAM protocol invocation. Level 1 SCAM master devices should also specify the Dominant Master Contention function unless they can guarantee through non-SCAM means that they are the only master present. SCAM slave devices shall ignore Dominant Master Contention functions, just as they ignore reserved function codes.

Following a Dominant Master Contention function code, SCAM master devices participate in a dominant master isolation stage. After the isolation stage completes the single remaining master is the dominant master. It remains the dominant master until the next invocation of the SCAM protocol (occurence of SCAM selection).

SCAM devices shall not prematurely terminate a Dominant Master Contention isolation stage. If a SCAM master detects DB4 asserted or detects an Error condition during the isolation stage, it may attempt recovery by releasing all signals and waiting for BUS FREE phase, or by generating a reset condition.

The Preference Code a SCAM master sends during the isolation stage encodes the preference for that master being dominant:

00b A Level 1 master device.

01b A Level 2 master device for which code 11b does not apply.

10b reserved

11b A Level 2 master device that knows it was dominant in the previous invocation of the SCAM protocol or has non-SCAM knowledge that it should become the dominant master.

*End of document SCSI Configured AutoMagically, X3T9.2/93-109r5.*