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
Digital Equipment Corporation
CXO 1-2 / N26
301 Rockrimmon Blvd., South
Colorado Springs, CO 80919-2398

voice: (719) 548-2247
FAX: (719) 548-3364
email: gardner@ssag.enet.dec.com

Changes from revision 2 to revision 3:

1. Explicit description of different implementation levels. A SCAM compatible device is a current device (e.g., one that is already shipping) that responds to selection quickly enough that SCAM masters can reliably detect its presence. Level 1 SCAM is what might plausibly be implemented with some (but not all) existing interface hardware. Level 2 SCAM will typically require new hardware, and incorporates such features as multiple hosts and "hot plugging".

2. Using data bus bits 5 to 7 for the transfer cycle control lines instead of MSG, C/D, and I/O. This signal reassignment appears to substantially increase the number of existing chip designs that can implement Level 1 SCAM. The rationale for this change was discussed in more detail in a recent SCSI reflector message.

3. Additional detail and editorial improvements.

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 must use a hard ID. 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 compatible** device is a non-SCAM device that satisfies certain requirements on responding to selection. These requirements ensure that SCAM compatible devices will be detected by SCAM masters, allowing SCAM compatible devices to be freely intermixed with SCAM devices. SCAM incompatible devices cannot be reliably detected by SCAM masters. If a SCAM incompatible 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 incompatible device's ID is not assigned to a SCAM device.

2. SCAM Timing and Interface Requirements

2.1. SCAM Compatible Devices

A SCAM compatible device shall enable its response to selection within a SCAM compatible power-on to selection time after the device powers-on. It shall re-enable its response to selection within a SCAM compatible 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 compatible selection response time following the appearance on the bus of a valid SELECTION phase containing its ID.

Notes:

1. The above are requirements to be characterized as a SCAM compatible device, not simply recommendations as in SCSI.

2. I wish to require that SCAM compatible devices respond to both SCSI-2 selection and SCSI-1 single initiator selection, where the target's ID is asserted without an initiator ID. I'm not certain of the appropriate wording, thus this note. This allows a substantial simplification of configuration rules for SCAM masters with soft IDs, and I believe almost all devices today still support SCSI-1 single initiator selection. The remainder of this proposal is written on the assumption that requiring response to SCSI-1 single initiator selection is acceptable.

3. This characterization of SCAM compatible 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 compatible 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 compatible 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 incompatible device. The means for doing so are outside the scope of SCAM.

4. 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 compatible power-on to selection time exists to ensure that SCAM compatible devices respond when the SCAM master scans the bus. Making this parameter larger allows more devices to be characterized as SCAM compatible. 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 compatible" characterization being useless.

   I am recommending that the SCAM compatible 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.

5. After completing its power-on initialization, a SCAM compatible device is required to respond to selection (assert BSY) quickly. I am recommending that this value, the SCAM compatible 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 compatible devices (old devices) and SCAM devices with default IDs. SCAM compatible 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 compatible 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 within the SCAM configuration selection time-out delay range during initial configuration.
5. shall not assert RST upon a selection time-out.

Level 1 SCAM slave devices:

6. shall recognize reset conditions, regardless of whether they are using the bus or processing commands at the time the reset occurs.
7. 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. SCAM slave devices do not recognize or respond to SCAM selection in normal operation, that is, once they have their ID. Level 1 SCAM slave devices do not perform SCAM selection.

8. 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.
9. shall not assert RST upon a selection time-out.
10. 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 within the SCAM configuration selection time-out delay range during initial configuration.
5. shall not assert RST upon a selection time-out.

Level 2 SCAM slave devices:

6. shall recognize reset conditions, regardless of whether they are using the bus or processing commands at the time the reset occurs.
7. 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. SCAM slave devices do not recognize or respond to SCAM selection in normal operation, that is, once they have their ID.
8. 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.
9. shall not assert RST upon a selection time-out.
10. shall implement the hard reset alternative.
11. after completing initialization and 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.

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 is somewhat arbitrary.

2.5. SCAM Timing Parameters

SCAM compatible power-on to selection time	5s	
SCAM compatible reset to selection time	250ms	
SCAM compatible selection response time	500us	
SCAM configuration selection time-out delay	750us	minimum
	1,5ms	maximum
SCAM default ID selection response time	2ms	
SCAM power-on to SCAM selection time	1s	
SCAM reset to SCAM selection time	250ms	
Long SCAM selection response time	250ms	
Short SCAM selection response time	1ms	

2.5.1.SCAM compatible power-on to selection time

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

2.5.2.SCAM compatible reset to selection time

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

2.5.3.SCAM compatible selection response time

The maximum time in which a SCAM compatible device may respond to selection of its ID, provided that the SCAM compatible power-on to selection time and SCAM compatible reset to selection time have both elapsed.

2.5.4.SCAM configuration selection time-out delay

The range of selection time-out delay values that a SCAM master shall use when examining the bus for SCAM compatible devices.

2.5.5. SCAM default ID selection response time

The minimum time in which a SCAM slave device may respond to selection of its unconfirmed default ID.

2.5.6. SCAM power-on to SCAM selection time

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

2.5.7. SCAM reset to SCAM selection time

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

2.5.8. 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.

2.5.9. 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 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.

Note: The SCAM protocol could be extended to allow a hardware response of asserting BSY, the same as with ordinary selection or reselection, followed by firmware asserting SEL and MSG, releasing BSY, and later releasing MSG. SCAM's reveiwers have not felt that the additional complexity was warranted.

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 compatible devices shall respond to selection or reselection of the device's ID within a SCAM compatible selection response time. That is, SCAM and SCAM compatible devices shall assert BSY no later than a SCAM compatible selection response time after the device's ID and SEL are asserted with BSY released. This requirement applies whenever at least a SCAM compatible power-on to selection time has elapsed since the device most recently powered-on and at least a SCAM compatible 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 compatible selection response time (preceeding paragraph) after they have been assigned a soft ID or have confirmed their default ID.

SCAM master devices shall use a selection time-out delay within the SCAM configuration selection time-out delay range following each power-on or reset condition. They shall continue using a selection time-out delay in that range until they have completed examining the bus for SCAM compatible devices.

3.5. Hard reset alternative

All SCAM and SCAM compatible 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.

4. SCAM Protocol

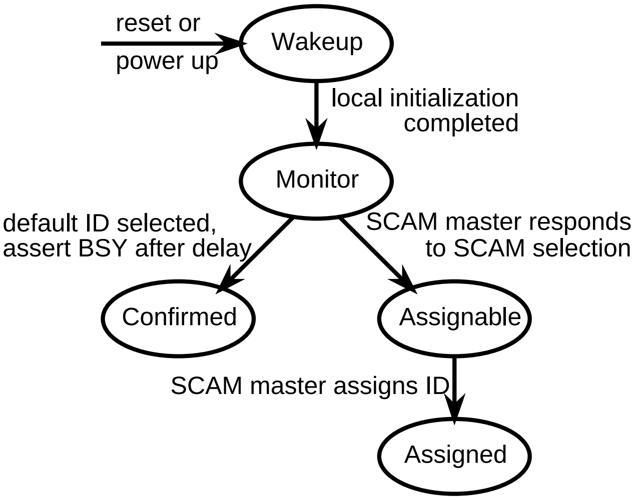
4.1. SCAM Slave Device Operation

A SCAM slave device shall cease responding to its previous ID whenever it powers up or detects a reset condition. After completing its local initialization, the SCAM slave device shall monitor the bus for SCAM selection. Upon detecting or performing a SCAM selection, the SCAM slave device shall determine whether a SCAM master responds to the SCAM selection. If a SCAM master responds, the SCAM slave device shall request ID assignment and continue doing so for subsequent SCAM selections until it is assigned a soft ID. After being assigned a soft ID the SCAM slave device need not recognize or respond to SCAM selection until after a subsequent power up or reset condition.

If a SCAM slave device has a default ID, it should concurrently monitor the bus for selection or reselection of its default ID as well as SCAM selection. If its default ID is selected or reselected prior to the device detecting a SCAM master's response to SCAM selection, the device shall wait a minimum of a /tbd/ selection time-out delay [probably 2ms] before asserting BSY. If the selection or reselection phase for its default ID persists for longer than the /tbd/ selection time-out delay [probably 2ms], the device should assert BSY, provided it does so within the usual rules for responding to selection or reselection. The device shall confirm its default ID if and only if it asserts BSY in response to selection or reselection of its default ID. Its default ID shall remain confirmed until a subsequent power up or reset condition. After confirming its default ID, a SCAM slave device need not recognize or respond to SCAM selection, and should respond to subsequent selection or reselection of its default ID as rapidly as it is capable. A SCAM slave device shall not respond to selection or reselection of its default ID if a SCAM master responds to a SCAM selection prior to the first selection or reselection of the slave device's default ID since the most recent power up or reset condition.

Whenever a SCAM slave device has neither been assigned a soft ID nor confirmed its default ID, it may solicit ID assignment. It does so by arbitrating without an ID, then performing SCAM selection if it wins arbitration. If a SCAM master responds to SCAM selection the SCAM slave shall request ID assignment. The SCAM slave device shall continue to monitor the bus for SCAM selection or selection of its default ID while attempting to arbitrate without an ID. Typically a SCAM slave should only solicit ID assignment if there has not been a bus reset condition since it last powered up. After power up, a slave device should solicit ID assignment several times using a short SCAM selection time-out delay, then solicit once or twice using a long SCAM selection time-out delay, 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.

The above behavior is illustrated in the accompanying figure. Following a reset condition or power up a SCAM slave device enters the Wakeup state, in which state the device does not use the bus or respond to selection. After completing local initialization it transitions to the Monitor state. In the Monitor state the device monitors the bus for both SCAM selection and selection (or reselection) of its default ID. If its default ID is selected, the device waits at least a /tbd/ selection time-out delay [probably 2ms], then (if its selection is still valid) asserts BSY and enters the



SCAM Slave Device Operation

Confirmed state. In the Confirmed state the device operates using its default ID. It will typically respond rapidly to selection of its default ID and ignore SCAM selection.

Alternately, while in the Monitor state the device may detect or itself perform a SCAM selection and thence detect a SCAM master's response to SCAM selection. Upon detecting a SCAM master's response to SCAM selection the slave device transitions to the Assignable state. It remains in the Assignable state until it is assigned a soft ID through the SCAM protocol, then transitions to the Assigned state. The soft ID assignment may occur during the same or a subsequent SCAM protocol invocation as the invocation that caused the device's transition to the Assignable state. While in the Assignable state, the slave device shall detect and respond to SCAM selection, and shall not respond to selection or reselection of any ID. While in the Assigned state, the slave device shall respond to selection of its assigned ID, and will typically ignore SCAM selection. A SCAM slave device may solicit ID assignment while in either the Monitor or Assignable states.

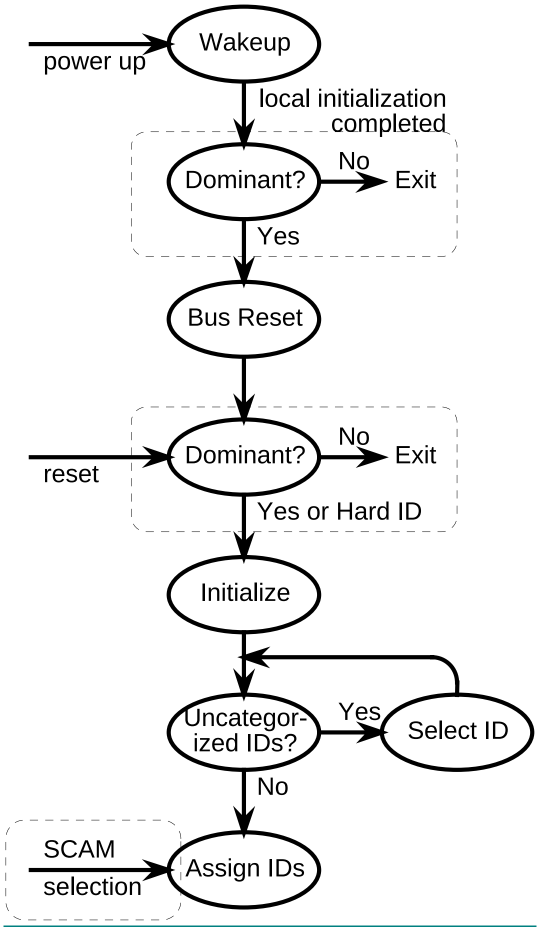
4.2. SCAM Master Device Operation

SCAM master device operation is illustrated in the accompanying figure. Portions enclosed in dashed boxes only 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 accompanying 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 shall 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.

Following power-on, a Level 1 SCAM master device shall complete its local initialization (Wakeup state), then generate a reset condition (Bus Reset state). A level 1 SCAM master assumes it is the only master on the bus and is therefore the dominant master.

Following a reset condition, whether generated by itself or another device, a Level 2 SCAM master shall again initiate the SCAM protocol and attempt to dominate other masters (second Dominant decision). It shall proceed to categorize IDs if it succeeds in becoming the dominant master. It shall exit and wait for ID assignment if it fails to become dominant and uses a soft ID. If it fails to become dominent and has a hard ID, the master may either categorize IDs or exit.



SCAM Master Device Operation

Level 1 SCAM masters shall always categorize IDs following a reset condition.

When a SCAM master categorizes IDs, it first initializes all IDs except its own as uncategorized (Initialize state). The SCAM master wins arbitration and selects an uncategorized ID using a selection time-out delay within the SCAM configuration selection time-out delay range (Select ID state). If a target device responds and enters command phase, the master should issue an INQUIRY or similar command.

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, and the SELECTION phase began later than both a SCAM compatible power-on to selection time following the master's most recent power-on and a SCAM compatible 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 compatible power-on to selection time and SCAM compatible 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 shall initiate the SCAM protocol (Assign IDs state). A level 2 SCAM master shall first attempt to dominate other masters, then proceed with ID assignment if and only if it succeeds in becoming dominant. A level 1 SCAM master shall proceed directly with ID assignment, unless it detects a level 2 SCAM master's attempt to become dominant. A level 1 SCAM master that detects a level 2 master's attempt to become dominant 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. They then wait a minimum of a SCAM selection time, release MSG, and wait until MSG has been released by all devices, using wired-or glitch filtering.

Note: This ensures that SCAM selection is maintained for the longest SCAM selection time parameter of the participating devices. While many slave devices will use a short SCAM selection time, a master device might choose to use a longer SCAM selection time due to knowledge of the configuration.

After detecting that MSG has been released by all devices, each SCAM device asserts several other signals. SCAM master devices assert BSY, I/O, C/D, and DB6. SCAM devices that need a soft ID assigned assert BSY, I/O, and DB7. After asserting the signals each device waits at least two 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 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 DB7 is released, then there are no devices requiring ID assignment.

After a SCAM master device detects that SEL has been released by all devices and DB7 is asserted, it asserts DB7, releases DB6 and waits for DB6 to be released by all devices, using wired-or glitch filtering. After a SCAM slave device detects that SEL has been released by all devices and C/D is asserted, it waits for DB6 to be released by all devices, using wired-or glitch detection. Initiation of the SCAM protocol is complete once all devices release DB6.

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

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

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.

The second transfer cycle in each iteration contains a function code. Master devices assert a 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 (if any) are determined by the resultant function code.

Slave devices shall ignore any iterations whose resultant function 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 requests are anticipated:

- contend to be a unique master
- set priority flag in all devices that do not yet have an ID
- assign an ID to a device

4.6. ID Assignment Function

Following an ID assignment function code, devices that do not yet have an ID assigned send their device identification strings one bit per transfer cycle. The device identification string is variable length and sent most significant bit first.

Initially all devices that do not yet have an ID assigned are contending devices. During each transfer cycle the contending devices assert DB 0 if the next bit of their identification string is zero, DB 1 if the next bit is one, or no data bits if they have reached the end of their identification string. Master devices may assert DB 4 to terminate the contention prematurely. Each contending device reads the data transferred during each cycle and takes the following actions:

Bit device sent	Bit(s) device receives	Action
DB 0	DB 0 DB 0 and DB 1	Continue Defer
DB 1	DB 1 with or without DB 0	Continue
none	DB 0 or DB 1 or both none	Defer Terminate
any	DB 4 with any combination of DB 0 and DB 1	Terminate

The Continue action means the device shall continue sending its device identification string in the next transfer cycle. The Defer action means the device shall stop sending its device identification string and ignore the remainder of the current iteration. The Terminate action either means the device has the numerically largest device identification string and is the sole remaining contending device, or a master has chosen to prematurely terminate the contention for some reason. In either case the next transfer cycle is a command instructing the remaining devices what to do. Anticipated commands are:

- assign a specified ID to the device
- clear the device's priority flag
- do nothing

The first byte of a device's identification string is a type code. It contains the following information:

- the device's current priority flag setting in the most significant bit
- the bus width implemented by the device
- a code representing the peripheral device type

Following the type code is the eight byte Vendor Identification from the device's INQUIRY data. After the Vendor Identification is a vendor unique Model Identification and serial number or other unique identifying number. The total length of the Model Identification and serial number should be less than or equal to 23 bytes so that the device's identification string will fit in 32 bytes.