



ISO/IEC 24739-1

Edition 1.0 2009-09

INTERNATIONAL STANDARD

**Information technology – AT attachment with packet interface-7 –
Part 1: Register delivered command set, logical register set (ATA/ATAPI-7 V1)**



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2009 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00



ISO/IEC 24739-1

Edition 1.0 2009-09

INTERNATIONAL STANDARD

**Information technology – AT attachment with packet interface-7 –
Part 1: Register delivered command set, logical register set (ATA/ATAPI-7 V1)**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XH**

ICS 35.200

ISBN 2-8318-1061-2

CONTENTS

FOREWORD.....	7
INTRODUCTION.....	9
1 Scope.....	11
2 Normative references	12
3 Definitions, abbreviations and conventions	13
3.1 Definitions and abbreviations	13
3.2 Abbreviations	21
3.3 Conventions	22
4 General operational requirements.....	28
4.1 Command delivery.....	28
4.2 Register delivered data transfer command sector addressing	28
4.3 General feature set	29
4.4 PACKET Command feature set	31
4.5 Power Management feature set.....	32
4.6 Advanced Power Management feature set.....	35
4.7 Security Mode feature set.....	35
4.8 SMART (self-monitoring, analysis and reporting technology) feature set.....	42
4.9 Host Protected Area feature set	43
4.10 CompactFlash™ Association (CFA) feature set.....	47
4.11 Removable Media Status Notification and Removable Media feature sets	48
4.12 Power-Up in Standby feature set.....	50
4.13 Automatic Acoustic Management (AAM) feature set	50
4.14 48-bit Address feature set	51
4.15 Device Configuration Overlay feature set	53
4.16 Media Card Pass Through Command feature set.....	56
4.17 Streaming feature set.....	57
4.18 General Purpose Logging feature set	59
4.19 Overlapped feature set.....	59
4.20 Queued feature set.....	60
4.21 Long physical sector feature set for non-packet devices	61
4.22 Long logical Sector feature set for non-packet devices	62
4.23 Devices implementing the Long Physical Sector Feature Set and the Long Logical Feature Sector Set	65
5 I/O register descriptions	65
5.1 Overview	65
5.2 Alternate Status register	65
5.3 Command register	66
5.4 Data port	66
5.5 Data register	67
5.6 Device register	67
5.7 Device control register	68
5.8 Error register	69
5.9 Features register	69
5.10 LBA High/Byte Count High register.....	70

5.11	LBA Low register	70
5.12	LBA Mid/Byte Count Low register	71
5.13	Sector Count/Interrupt Reason register	71
5.14	Status register	71
5.15	Signature and persistence	74
5.16	Single device configurations	75
6	Command descriptions	76
6.1	Overview	76
6.2	CFA ERASE SECTORS	78
6.3	CFA REQUEST EXTENDED ERROR CODE	79
6.4	CFA TRANSLATE SECTOR	82
6.5	CFA WRITE MULTIPLE WITHOUT ERASE	84
6.6	CFA WRITE SECTORS WITHOUT ERASE	86
6.7	CHECK MEDIA CARD TYPE	88
6.8	CHECK POWER MODE	90
6.9	CONFIGURE STREAM	91
6.10	DEVICE CONFIGURATION	94
6.11	DEVICE RESET	108
6.12	DOWNLOAD MICROCODE	109
6.13	EXECUTE DEVICE DIAGNOSTIC	111
6.14	FLUSH CACHE	113
6.15	FLUSH CACHE EXT	115
6.16	GET MEDIA STATUS	118
6.17	IDENTIFY DEVICE	119
6.18	IDENTIFY PACKET DEVICE	144
6.19	IDLE	158
6.20	IDLE IMMEDIATE	160
6.21	MEDIA EJECT	163
6.22	MEDIA LOCK	164
6.23	MEDIA UNLOCK	166
6.24	NOP	168
6.25	PACKET	169
6.26	READ BUFFER	175
6.27	READ DMA	176
6.28	READ DMA EXT	178
6.29	READ DMA QUEUED	181
6.30	READ DMA QUEUED EXT	185
6.31	READ LOG EXT	191
6.32	READ MULTIPLE	204
6.33	READ MULTIPLE EXT	207
6.34	READ NATIVE MAX ADDRESS	210
6.35	READ NATIVE MAX ADDRESS EXT	211
6.36	READ SECTOR(S)	213
6.37	READ SECTOR(S) EXT	216
6.38	READ STREAM DMA EXT	218
6.39	READ STREAM EXT	223
6.40	READ VERIFY SECTOR(S)	227
6.41	READ VERIFY SECTOR(S) EXT	229
6.42	SECURITY DISABLE PASSWORD	232

6.43	SECURITY ERASE PREPARE	233
6.44	SECURITY ERASE UNIT.....	235
6.45	SECURITY FREEZE LOCK	237
6.46	SECURITY SET PASSWORD.....	239
6.47	SECURITY UNLOCK.....	241
6.48	SERVICE	243
6.49	SET FEATURES.....	244
6.50	SET MAX	251
6.51	SET MAX ADDRESS EXT	259
6.52	SET MULTIPLE MODE.....	262
6.53	SLEEP	264
6.54	SMART	266
6.55	STANDBY	297
6.56	STANDBY IMMEDIATE	299
6.57	WRITE BUFFER.....	300
6.58	WRITE DMA.....	302
6.59	WRITE DMA EXT	304
6.60	WRITE DMA FUA EXT	308
6.61	WRITE DMA QUEUED	311
6.62	WRITE DMA QUEUED EXT.....	315
6.63	WRITE DMA QUEUED FUA EXT.....	320
6.64	WRITE LOG EXT.....	326
6.65	WRITE MULTIPLE.....	329
6.66	WRITE MULTIPLE EXT	331
6.67	WRITE MULTIPLE FUA EXT	334
6.68	WRITE SECTOR(S).....	338
6.69	WRITE SECTOR(S) EXT	340
6.70	WRITE STREAM DMA EXT	342
6.71	WRITE STREAM EXT.....	346
7	Parallel interface physical and electrical requirements (see ISO/IEC 24739-2)	351
8	Parallel interface signal assignments and descriptions (see ISO/IEC 24739-2).....	351
9	Parallel interface general operating requirements of the physical, data link, and transport layers (see ISO/IEC 24739-2).....	351
10	Parallel interface register addressing (see ISO/IEC 24739-2)	351
11	Parallel interface transport Protocols (see ISO/IEC 24739-2).....	351
12	Parallel interface timing (see ISO/IEC 24739-2).....	351
13	Serial interface overview (see ISO/IEC 24739-).....	351
14	Serial interface physical layer (see ISO/IEC 24739-3)	351
15	Serial interface link layer (see ISO/IEC 24739-3).....	351
16	Serial interface transport layer (see ISO/IEC 24739-3)	351
17	Serial interface device command layer (see ISO/IEC 24739-3).....	351
18	Host command layer (see ISO/IEC 24739-3)	351
19	Serial interface host adapter register interface (see ISO/IEC 24739-3)	351
20	Serial interface error handling (see ISO/IEC 24739-3).....	351
	Annex A (informative) Command Set summary	352
	Annex B (informative) Design and programming considerations for large physical sector devices	359

Annex C Device determination of cable type (informative) (see ISO/IEC 24739-2)	361
Annex D Signal integrity and UDMA guide (informative) (see ISO/IEC 24739-2)	361
Annex E Register selection address summary (informative) (see ISO/IEC 24739-2)	361
Annex F Sample code for CRC and scrambling (informative) (see ISO/IEC 24739-3)	361
Annex G FIS type field value selection (informative) (see ISO/IEC 24739-3)	361
Annex H Physical layer implementation examples (informative) (see ISO/IEC 24739-3)	361
Annex I Command processing Example (informative) (see ISO/IEC 24739-3)	361
Bibliography	362
Figure 1 – ATA document relationships	11
Figure 2 – State diagram convention	24
Figure 3 – Byte, word and DWORD relationships	28
Figure 4 – Power management state diagram	33
Figure 5 – Security mode state diagram	37
Figure 6 – SET MAX security state diagram	46
Figure 7 – Device configuration overlay state diagram	54
Figure 8 – Long Logical and long Physical Sector Example	62
Figure 9 – Selective self-test test span example	277
Figure B.1 – Unaligned Write Example	360
Table 1 – PACKET delivered command sets	12
Table 2 – Byte order	26
Table 3 – Byte order	27
Table 4 – Security mode command actions	40
Table 5 – 48-bit addresses	52
Table 6 – 28-bit addresses	52
Table 7 – Media Card type references	56
Table 8 – Long logical sector function	63
Table 9 – I/O registers	65
Table 10 – Extended error codes	81
Table 11 – CFA TRANSLATE SECTOR Information	83
Table 12 – Device Configuration Overlay Features register values	94
Table 13 – Device Configuration Identify data structure	100
Table 14 – Device Configuration Overlay data structure	105
Table 16 – IDENTIFY DEVICE data	122
Table 17 - Minor version number	135
Table 18 – IDENTIFY PACKET DEVICE data	146
Table 19 – Automatic Standby timer periods	158
Table 20 – Log address definition	192
Table 21 – General Purpose Log Directory	194
Table 22 – Extended Comprehensive SMART error log	195
Table 23 – Extended Error log data structure	196
Table 24 – Command data structure	197

Table 25 – Error data structure	198
Table 26 – State field values.....	198
Table 27 – Extended Self-test log data structure.....	199
Table 28 – Extended Self-test log descriptor entry	200
Table 29 – Read Stream Error log.....	201
Table 30 – Error Log Entry.....	201
Table 31 – Write Stream Error log.....	202
Table 32 – Streaming Performance Parameters log	203
Table 33 – Sector Time Array Entry (Linearly Interpolated)	203
Table 34 – Position Array Entry (Linearly Interpolated)	203
Table 35 – Access Time Array Entry (Linearly Interpolated)	203
Table 36 – Delayed LBA log.....	204
Table 37 – Security password content.....	233
Table 38 – SECURITY ERASE UNIT password.....	237
Table 39 – SECURITY SET PASSWORD data content.....	241
Table 40 – Identifier and security level bit interaction.....	241
Table 41 – SET FEATURES register definitions	246
Table 42 – Transfer mode values.....	247
Table 43 – Advanced power management levels.....	248
Table 44 – Automatic acoustic management levels	249
Table 45 – SET MAX Features register values	251
Table 46 – SET MAX SET PASSWORD data content.....	255
Table 47 – SMART Feature register values.....	267
Table 48 – SMART EXECUTE OFF-LINE IMMEDIATE LBA Low register values	275
Table 49 – Device SMART data structure	280
Table 50 – Off-line data collection status byte values.....	281
Table 51 – Self-test execution status values	281
Table 52 – Log address definition	284
Table 53 – SMART Log Directory.....	286
Table 54 – SMART summary error log sector.....	286
Table 55 – Error log data structure	287
Table 56 – Command data structure	288
Table 57 – Error data structure	288
Table 58 – State field values.....	289
Table 59 – Comprehensive error log	290
Table 60 – Self-test log data structure	291
Table 61 – Self-test log descriptor entry.....	291
Table 62 – Selective self-test log	292
Table 63 – Selective self-test feature flags	293
Table A.1 – Command matrix.....	352
Table A.2 – Command codes (sorted by command code).....	353
Table A.3 – Command codes (sorted by command)	356

INFORMATION TECHNOLOGY – AT ATTACHMENT WITH PACKET INTERFACE-7 –

Part 1: Register delivered command set, logical register set (ATA/ATAPI-7 V1)

FOREWORD

- 1) ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.
- 2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.
- 3) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.
- 4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 5) In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
- 6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.
- 7) All users should ensure that they have the latest edition of this publication.
- 8) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.
- 9) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 10) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 24739-1 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of the ISO/IEC 24739 series, under the general title *Information technology – AT attachment with packet interface-7*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

ISO/IEC 24739-1 is to be used in conjunction with ISO/IEC 24739-2 and ISO/IEC 24739-3.

INTRODUCTION

ISO/IEC 24739 defines the AT attachment with packet interface (ATAPI). The standard includes the command set and two transport protocols to support parallel and serial physical interconnects. ISO/IEC 24739 is partitioned into three parts:

Part 1: Register delivered command set, logical register set (ATA/ATAPI-7 V1)

Part 2: Parallel transport protocols and physical interconnect (ATA/ATAPI-7 V2)

Part 3: Serial transport protocols and physical interconnect (ATA/ATAPI-7 V3)

ISO/IEC 24739 is partitioned in this way to separate the command set (Part 1) for ease of reference and maintenance. The command set is the same for both the parallel transport (Part 2) and the serial transport (Part 3).

Parts 1 and Part 2 were substantially derived from the prior version of this standard (ATA/ATAPI-6, ANSI INCITS 361-2002). Part 3 is new material defining the serial transport of the ATA/ATAPI interface.

All three parts have a clause that includes introductory material, a common glossary and an index to the major clauses of the other two parts. After Clause 3 in each of the parts, the material is part specific. Within each part, references are made to other parts, given with the full reference of the publication and major clause number, e.g. ISO/IEC 24739-3, Clause 4.

In order to implement the standard for a parallel transport, it is necessary to comply with both ISO/IEC 24739-1 and ISO/IEC 24739-2. In order to implement the serial transport, it is necessary to comply with both ISO/IEC 24739-1 and ISO/IEC 24739-3. It should be recognized, however, that the serial transport as described in ISO/IEC 24739-3 relies heavily on logical interconnect and protocol concepts and requirements described in ISO/IEC 24739-2. These concepts are called "parallel emulation" in ISO/IEC 24739-3. In some cases, references are made to the parallel implementation of ATA, which refers to the parallel transport (ISO/IEC 24739-2). The reader is strongly advised to consult all three parts when implementing the serial transport.

This International Standard (ISO/IEC 24739-1) contains the command feature sets for ATA. It defines structures used by the parallel implementation of ATA and the serial implementation of ATA. The command descriptions are in alphabetical order, with a cross-reference by command codes in Annex A.

The ISO/IEC 24739 series of standards consists of the following parts and clauses:

Part 1

Clause 1 describes the scope.

Clause 2 provides normative references for the entire standard.

Clause 3 provides definitions, abbreviations and conventions used within the entire standard.

Clause 4 describes the general operating requirements of the command layer.

Clause 5 describes the I/O registers.

Clause 6 contains descriptions of the commands.

Clauses 7 through 12 point to the material in ISO/IEC 24739-2.

Clauses 13 through 19 point to material in ISO/IEC 24739-3.

Part 2

Clause 1 describes the scope.

Clause 2 provides normative references for the entire standard.

Clause 3 provides definitions, abbreviations and conventions used within the entire standard.

Clauses 4, 5 and 6 point to the material in ISO/IEC 24739-1.

Clause 7 contains the electrical and mechanical characteristics.

Clause 8 contains the signal descriptions.

Clause 9 describes the general operating requirements of the physical, data link and transport layers.

Clause 10 contains describes register addressing.

Clause 11 contains the transport protocols.

Clause 12 contains the interface timing diagrams.

Clauses 13 through 19 point to material in ISO/IEC 24739-3.

Part 3

Clause 1 describes the scope.

Clause 2 provides normative references for the entire standard.

Clause 3 provides definitions, abbreviations and conventions used within the entire standard.

Clauses 4, 5 and 6 point to the material in ISO/IEC 24739-1.

Clauses 7 through 12 point to the material in ISO/IEC 24739-2.

Clause 13 contains a general overview of the serial interface.

Clause 14 describes the serial physical layer.

Clause 15 describes the serial link layer.

Clause 16 describes the serial transport layer.

Clause 17 describes the device command layer protocol for the serial interface.

Clause 18 describes the host command layer protocol for the serial interface.

Clause 19 describes the serial interface host adapter register interface.

Clause 20 describes the serial interface error handling.

INFORMATION TECHNOLOGY – AT ATTACHMENT WITH PACKET INTERFACE-7 –

Part 1: Register delivered command set, logical register set (ATA/ATAPI-7 V1)

1 Scope

This part of ISO/IEC 24739 specifies the AT Attachment Interface between host systems and storage devices. It provides a common attachment interface for systems manufacturers, system integrators, software suppliers and suppliers of intelligent storage devices.

ISO/IEC 24739-1 defines the register delivered commands used by devices implementing the standard. ISO/IEC 24739-2 defines the connectors and cables for physical interconnection between host and storage device, the electrical and logical characteristics of the interconnecting signals and the protocols for the transporting of commands, data and status over the interface for the parallel interface. ISO/IEC 24739-3 defines the connectors and cables for physical interconnection between host and storage device, the electrical and logical characteristics of the interconnecting signals and the protocols for the transporting of commands, data and status over the interface for the serial interface. Figure 1 shows the relationship of these documents. For devices implementing the PACKET command feature set, additional command layer standards are listed in Table 1 and described in Clause 2.

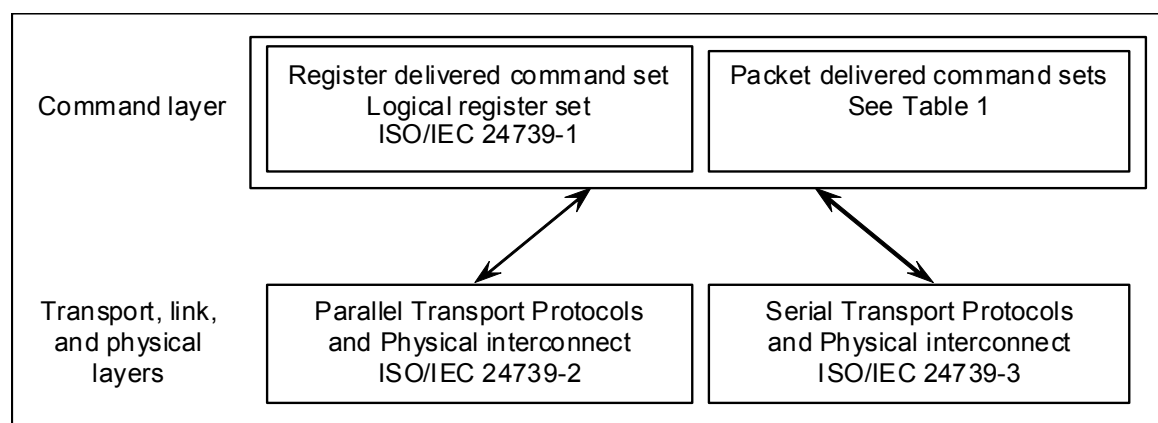


Figure 1 – ATA document relationships

Table 1 – PACKET delivered command sets

Standard
SCSI Primary Commands (SPC)
ISO/IEC 14776-452, SCSI Primary Commands 2 (SPC-2)
ISO/IEC 14776-453, SCSI Primary Commands-3 (SPC-3)
ISO/IEC 14776-322, SCSI Block Commands (SBC-2)
ISO/IEC 14776-331, SCSI Stream Commands (SSC)
Multimedia Commands (MMC)
ISO/IEC 14776-362, Multimedia Commands-2 (MMC-2)
ISO/IEC 14776-363, Multimedia Commands-3 (MMC-3)
ISO/IEC 14776-364: Multimedia Commands-4 (MMC-4)
ATAPI for Removable Media (SFF8070I)
ATA Packet Interface (ATAPI) for Streaming Tape QIC-157 revision D

This standard maintains compatibility with the AT Attachment with packet interface-6 standard (ATA/ATAPI-6), ANSI INCITS 361-2002, and while providing additional functions, is not intended to require changes to presently installed devices or existing software.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references only the edition cited applies. For undated references the latest edition (including any amendments) applies.

ISO/IEC 14776-321, *Information technology – Small computer system interface (SCSI-3) – Part 321: Block commands (SBC)* [ANSI INCITS 306-1998 (R2003)]

ISO/IEC 14776-322, *Information technology – Small computer system interface (SCSI) – Part 322: Block commands-2 (SBC-2)* [T10/1417-D]

ISO/IEC 14776-331, *Information technology – Small computer system interface (SCSI) – Part 331: Stream commands (SSC)* [ANSI INCITS 335-2000]

ISO/IEC 14776-362, *Information technology – Small computer system interface (SCSI) – Part 362: Multimedia commands-2 (MMC-2)* [ANSI INCITS 333-2000]

ISO/IEC 14776-363, *Information technology – Small computer system interface (SCSI) – Part 363: Multimedia commands-3 (MMC-3)* [ANSI INCITS 360-2002]
(under consideration)

ISO/IEC 14776-364, *Information technology – Small computer system interface (SCSI) – Part 364: Multimedia commands-4 (MMC-4)* [T10/1545D]
(under consideration)

ISO/IEC 14776-452, *Information technology – Small computer system interface (SCSI) – Part 452: Primary commands-2 (SPC-2)* [ANSI INCITS 351-2001]

ISO/IEC 14776-453, *Information technology – Small computer system interface (SCSI) – Part 453: Primary commands-3 (SPC-3)* [T10/1416-D]
(under consideration)

ISO/IEC 13213:1994, *Information technology – Microprocessor systems – Control and Status Register (CSR) Architecture for microprocessor buses*

ISO 7779:1999, *Acoustics – Measurement of airborne noise emitted by information technology and telecommunications equipment*

AT Attachment with Packet Interface Extension (ATA/ATAPI-4) [ANSI INCITS 317-1998] (R2003)

SCSI-3 Primary Commands (SPC) [ANSI INCITS 301-1997 (R2002)]

Multimedia Commands (MMC) [ANSI INCITS 304-1997 (R2002)]

Protected Area Run Time Interface Extensions (PARTIES) [ANSI INCITS 346-2001]

ATAPI for Rewritable Media (under development) [SFF8070i]

3 Definitions, abbreviations and conventions

3.1 Definitions and abbreviations

For the purposes of this standard, the following definitions apply.

3.1.1

ASCII Character

designates 8-bit value that is encoded using the ASCII character set

3.1.2

acoustics

measurement of airborne noise emitted by information technology and telecommunications equipment [see ISO 7779:1999(E)]

3.1.3

ATA (AT Attachment)

ATA defines the physical, electrical, transport and command protocols for the internal attachment of storage devices to host systems

3.1.4

ATA-1 device

device that complied with ANSI X3.221-1994, the AT Attachment interface for disk drives

NOTE ANSI X3.221-1994 has been withdrawn.

3.1.5

ATA-2 device

device that complied with ANSI X3.279-1996, the AT Attachment interface with extensions

NOTE ANSI X3.279-1996 has been withdrawn.

3.1.6

ATA-3 device

device that complies with ANSI INCITS 298-1997, the AT Attachment-3 Interface

NOTE ANSI INCITS 298-1997 has been withdrawn.

3.1.7

ATA/ATAPI-4 device

device that complies with ANSI INCITS 317-1998

NOTE For reference, see bibliography.

3.1.8

ATA/ATAPI-5 device

device that complies with ANSI INCITS 340-2000

NOTE For reference, see bibliography.

3.1.9

ATA/ATAPI-6 device

device that complies with ANSI INCITS 361-2002

NOTE For reference, see bibliography.

3.1.10

ATA/ATAPI-7 device

device that complies with this standard

3.1.11

ATAPI (AT Attachment Packet Interface) device

device implementing the Packet Command feature set

3.1.12

AU (Allocation Unit)

minimum number of logically contiguous sectors on the media as used in the Streaming feature set

NOTE An Allocation Unit may be accessed with one or more requests.

3.1.13

AV (Audio-Video)

Audio-Video applications use data that is related to video images and/or audio; the distinguishing characteristic of this type of data is that accuracy is of lower priority than timely transfer of the data

3.1.14

backchannel

when transmitting a FIS, the backchannel is the receive channel

3.1.15

BER (bit error rate)

the statistical probability of a transmitted encoded bit being erroneously received in a communication system

3.1.16

bus release

for devices implementing overlap, the term bus release is the act of clearing both DRQ and BSY to zero before the action requested by the command is completed; this allows the host to select the other device or deliver another queued command

3.1.17

byte count

value placed in the Byte Count register by the device to indicate the number of bytes to be transferred during this DRQ assertion when executing a PACKET PIO data transfer command

3.1.18

byte count limit

value placed in the Byte Count register by the host as input to a PACKET PIO data transfer command to specify the maximum byte count that may be transferred during a single DRQ assertion

3.1.19**CFA (CompactFlash™ Association)**

the CompactFlash™ Association which created the specification for compact flash memory that uses the ATA interface

(CompactFlash™ is a registered trade mark of the CompactFlash™ Association)

3.1.20**check condition**

for devices implementing the PACKET Command feature set, this indicates an error or exception condition has occurred

3.1.21**CHS (cylinder-head-sector)**

obsolete method of addressing the data on the device by cylinder number, head number and sector number

3.1.22**code violation**

in a serial interface implementation, a code violation is an error that occurs in the decoding of an encoded character (see ISO/IEC 24739-3, Clause 15)

3.1.23**command aborted**

command completion with ABRT set to one in the Error register and ERR set to one in the Status register

3.1.24**command acceptance**

a command is considered accepted whenever the currently selected device has the BSY bit cleared to zero in the Status register and the host writes to the Command register

NOTE An exception exists for the DEVICE RESET command (see Clause 6). In a serial implementation, command acceptance is a positive acknowledgment of a host to device register FIS.

3.1.25**Command Block registers**

interface registers used for delivering commands to the device or posting status from the device; in a serial implementation, the command block registers are FIS payload fields

3.1.26**command completion**

completion by the device of the action requested by the command or the termination of the command with an error, the placing of the appropriate error bits in the Error register, the placing of the appropriate status bits in the Status register, the clearing of both BSY and DRQ to zero, and Interrupt Pending

3.1.27**command packet**

data structure transmitted to the device during the execution of a PACKET command that includes the command and command parameters

3.1.28**command released**

when a device supports overlap or queuing, a command is considered released when a bus release occurs before command completion

3.1.29

Control Block registers

in a parallel implementation, interface registers used for device control and to post alternate status

in a serial interface implementation, the logical field of a FIS corresponding to the Device Register bits of a parallel implementation

3.1.30

control character

in a serial interface implementation, an encoded character that represents a non-data byte (see ISO/IEC 24739-3, Clause 15)

3.1.31

CRC (Cyclical Redundancy Check)

a means used to check the validity of certain data transfers

3.1.32

Cylinder High register

name used for the LBA High register in previous ATA/ATAPI standards

3.1.33

Cylinder Low register

name used for the LBA Mid register in previous ATA/ATAPI standards

3.1.34

data character

in a serial interface implementation, an encoded character that represents a data byte. (See ISO/IEC 24739-3, Clause 15)

3.1.35

data-in

protocol that moves data from the device to the host; such transfers are initiated by READ commands

3.1.36

data-out

protocol that moves data from the host to the device; such transfers are initiated by WRITE commands

3.1.37

Delayed LBA

any sector for which the performance specified by the Streaming Performance Parameters log is not valid

3.1.38

device

a storage peripheral

NOTE Traditionally, a device on the interface has been a hard disk drive, but any form of storage device may be placed on the interface provided the device adheres to this standard.

3.1.39

device selection

in a parallel implementation, a device is selected when the DEV bit of the Device register is equal to the device number assigned to the device by means of a Device 0/Device 1 jumper or switch, or use of the CSEL signal

in a serial implementation the device ignores the DEV bit, the host adapter may use this bit to emulate device selection

3.1.40**disparity**

difference between the number of ones and the number of zeroes in an encoded character (see ISO/IEC 24739-3, Clause 15)

3.1.41**DMA (direct memory access) data transfer**

a means of data transfer between device and host memory without host processor intervention

3.1.42**don't care**

indicates that a value is irrelevant for the particular function described

3.1.43**driver**

active circuit inside a device or host that sources or sinks current to assert or negate a signal on the bus

3.1.44**DRQ data block**

a unit of data words transferred during a single assertion of DRQ when using PIO data transfer

3.1.45**elasticity buffer**

in a serial interface implementation, a portion of the receiver where character slipping and/or character alignment is performed

3.1.46**encoded character**

in a serial interface implementation, the output of the 8b/10b encoder (see ISO/IEC 24739-3, Clause 15)

3.1.47**First party DMA access**

method by which a device accesses host memory

NOTE First party DMA differs from DMA in that the device sends a DMA Setup FIS to select host memory regions; whereas for DMA the host configures the DMA controller.

3.1.48**FIS (Frame Information Structure)**

data structure that is the payload of a frame and does not include the SOF primitive, CRC and EOF primitive

3.1.49**frame**

unit of information exchanged between the host adapter and a device

NOTE A frame consists of an SOF primitive, a Frame Information Structure, a CRC calculated over the contents of the FIS and an EOF primitive.

3.1.50**FUA (Forced Unit Access)**

requires that user data be transferred to or from the device media before command completion even if caching is enabled

3.1.51

Gen1 DWORD Time

the time it takes to transmit a 40 bit encoded value at 1,5 Gbit/s

3.1.52

host

the computer system executing the software BIOS and/or operating system device driver controlling the device and the adapter hardware for the ATA interface to the device

3.1.53

host adapter

the implementation of the host transport, link and physical layers

3.1.54

Interrupt Pending

in a parallel implementation, an internal state of a device; in this state, the device asserts INTRQ if nIEN is cleared to zero and the device is selected (see Clause 8)

in a serial implementation, the Interrupt Pending state is an internal state of the host adapter; this state is entered by reception of a FIS with the I field set to one (see ISO/IEC 24739-3, Clause 16)

3.1.55

LBA (logical block address)

the addressing of data on the device by the linear mapping of sectors

3.1.56

LFSR (Linear Feedback Shift Register)

(See ISO/IEC 24739-3, Clause 15)

3.1.57

link

the link layer manages the phy layer to achieve the delivery and reception of frames (see ISO/IEC 24739-3, Clause 15)

3.1.58

logical sector

a uniquely addressable set of 256 words (512 bytes)

3.1.59

native max address

the highest address a device accepts in the factory default condition, that is, the highest address that is accepted by the SET MAX ADDRESS command

3.1.60

overlap

a protocol that allows devices that require extended command time to perform a bus release so that commands may be executed by the other device (if present) on the bus

3.1.61

packet delivered command

a command that is delivered to the device using the PACKET command via a command packet that contains the command and the command parameters

NOTE See also register delivered command.

3.1.62

phy

physical layer electronics (see ISO/IEC 24739-3, Clause 14)

3.1.63**physical sector**

a group of contiguous logical sectors that are read from or written to the device media in a single operation

3.1.64**PIO (programmed input/output) data transfer**

PIO data transfers are performed by the host processor utilizing accesses to the Data register

3.1.65**primitive**

in a serial interface implementation, a single DWORD of information that consists of a control character in byte 0 followed by three additional data characters in byte 1 through 3

3.1.66**queued**

command queuing allows the host to issue concurrent commands to the same device

NOTE Only commands included in the Overlapped feature set may be queued. In this standard, the queue contains all commands for which command acceptance has occurred but command completion has not occurred.

3.1.67**read command**

a command that causes the device to transfer data from the device to the host (e.g., READ SECTOR(S), READ DMA, etc.)

3.1.68**register**

a register may be a physical hardware register or a logical field

3.1.69**register delivered command**

command that is delivered to the device by placing the command and all of the parameters for the command in the device Command Block registers

NOTE See also packet delivered command.

3.1.70**register transfers**

host reading and writing any device register except the Data register; register transfers are 8 bits wide

3.1.71**released**

in a parallel interface implementation, indicates that a signal is not being driven

NOTE For drivers capable of assuming a high-impedance state, this means that the driver is in the high-impedance state. For open-collector drivers, the driver is not asserted.

3.1.72**sector**

uniquely addressable set of 256 words (512 bytes)

3.1.73**Sector Number register**

LBA Low register in previous ATA/ATAPI standards

3.1.74

Shadow Command Block

in a serial interface implementation, a set of virtual fields in the host adapter that map the Command Block registers defined at the command layer to the fields within the FIS content

3.1.75

Shadow Control Block

in a serial interface implementation, a set of virtual fields in the host adapter that map the Control Block registers defined at the command layer to the fields within the FIS content

3.1.76

signature

unique set of values placed in the Command Block registers by the device to allow the host to distinguish devices implementing the PACKET Command feature set from those devices not implementing the PACKET Command feature set

3.1.77

SMART (Self-Monitoring, Analysis and Reporting Technology)

for prediction of device degradation and/or faults

3.1.78

transport

the transport layer manages the lower layers (link and phy) as well as constructing and parsing FISs (see ISO/IEC 24739-3, Clause 13)

3.1.79

Ultra DMA burst

the period from an assertion of DMACK[−] to the subsequent negation of DMACK[−] when an Ultra DMA transfer mode has been enabled by the host

3.1.80

unaligned write

write command that does not start at the first logical sector of a physical sector or does not end at the last logical sector of a physical sector

3.1.81

unit attention condition

state that a device implementing the PACKET Command feature set maintains while the device has asynchronous status information to report to the host

3.1.82

unrecoverable error

when the device sets either the ERR bit or the DF bit to one in the Status register at command completion

3.1.83

VS (Vendor Specific)

bits, bytes, fields and code values that are reserved for vendor specific purposes

NOTE 1 These bits, bytes, fields, and code values are not described in this standard, and may vary among vendors. This term is also applied to levels of functionality whose definition is left to the vendor.

NOTE 2 Industry practice could result in conversion of a Vendor Specific bit, byte, field or code value into a defined standard value in a future standard.

3.1.84

write command

command that causes the device to transfer data from the host to the device (e.g., WRITE SECTOR(S), WRITE DMA, etc.)

3.1.85**WWN (world wide name)**

a 64-bit worldwide unique name based upon a company's IEEE identifier (see IDENTIFY DEVICE Words 108 to 111 in ISO/IEC 24739-1, Clause 6)

3.2 Abbreviations

ABRT	Abort
a/r	As Required
BSY	Busy
CCTL	Command Completion Time Limit
C/D	Command/Data
CFA	Compact Flash Association
DASP	Drive Active / Slave Present
DD	Device Data
DEV	Device
DF	Device fault
DF/SE	Device Fault / Stream Error
DIOW	Device Input Output Write
DMA	Direct Memory Access
DMACK	DMA acknowledge
DMARQ	DMA request
DRDY	Device ready
DRQ	Data Request
ECC	Error Correcting Code
ENB	Enable
ERR	Error
ERR/CHK	Error check
FIFO	First in / First Out
HOB	High Order Bit
ID	Identification
IEEE OUI	Institute of Electrical and Electronics Engineers Organization Unique Identifier
INTRQ	Interrupt Request
I/O	Input / Output
LBA	Logical Block Address
na	Not Applicable
NAA	Network Address Authority
nIEN	Negative Interrupt Enable
NM	No media
NOP	No Operation
obs	Obsolete
OVL	Overlap
PDIAG	Passed Diagnostics
PIO	programmed input/output
REL	Release
R/W	Read / Write
SERV	Service

SRST Soft Reset

3.3 Conventions

3.3.1 General

Lowercase is used for words having the normal English meaning. Certain words and terms used in this standard have a specific meaning beyond the normal English meaning. These words and terms are defined either in Clause 3 or in the text where they first appear.

The names of abbreviations, commands, fields, and acronyms used as signal names are in all uppercase (e.g., IDENTIFY DEVICE). Fields containing only one bit are usually referred to as the "name" bit instead of the "name" field. (See 3.3.7 for the naming convention used for naming bits.)

Names of device registers begin with a capital letter (e.g., LBA Mid register).

The expression "word n" or "bit n" shall be interpreted as indicating the content of word n or bit n.

3.3.2 Precedence

If there is a conflict between text, figures and tables, the precedence shall be tables, figures and then text.

3.3.3 Lists

Ordered lists, those lists describing a sequence, are of the form:

- a)
- b)
- c)

Unordered list are of the form:

- 1)
- 2)
- 3)

3.3.4 Keywords

Several keywords are used to differentiate between different levels of requirements and optionality.

3.2.4.1

expected

A keyword used to describe the behavior of the hardware or software in the design models assumed by this standard. Other hardware and software design models may also be implemented.

3.2.4.2

mandatory

A keyword indicating items to be implemented as defined by this standard.

3.2.4.3

may

A keyword that indicates flexibility of choice with no implied preference.

3.2.4.4

obsolete

A keyword indicating that the designated bits, bytes, words, fields and code values that may have been defined in previous standards are not defined in this standard and shall not be reclaimed for other uses in future standards. However, some degree of functionality may be required for items designated as "obsolete" to provide for backward compatibility.

Obsolete commands should not be used by the host. Commands defined as obsolete may be command aborted by devices conforming to this standard. However, if a device does not command abort an obsolete command, the minimum that is required by the device in response to the command is command completion.

3.2.4.5 optional

A keyword that describes features that are not required by this standard. However, if any optional feature defined by the standard is implemented, the feature shall be implemented in the way defined by the standard.

3.2.4.6 prohibited

A keyword indicating that an item shall not be implemented by an implementation.

3.2.4.7 reserved

A keyword indicating reserved bits, bytes, words, fields and code values that are set aside for future standardization. Their use and interpretation may be specified by future extensions to this or other standards. A reserved bit, byte, word or field shall be cleared to zero, or in accordance with a future extension to this standard. The recipient shall not check reserved bits, bytes, words or fields. Receipt of reserved code values in defined fields shall be treated as a command parameter error and reported by returning command aborted.

3.2.4.8 retired

A keyword indicating that the designated bits, bytes, words, fields and code values that had been defined in previous standards are not defined in this standard and may be reclaimed for other uses in future standards. If retired bits, bytes, words, fields or code values are used before they are reclaimed, they shall have the meaning or functionality as described in previous standards.

3.2.4.9 shall

A keyword indicating a mandatory requirement. Designers are required to implement all such mandatory requirements to ensure interoperability with other products that conform to this standard.

3.2.4.10 should

A keyword indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase "it is recommended".

3.3.5 Numbering

Numbers that are not immediately followed by a lowercase "b" or "h" are decimal values. Numbers that are immediately followed by a lowercase "b" (e.g., 01b) are binary values. Numbers that are immediately followed by a lowercase "h" (e.g., 3Ah) are hexadecimal values.

3.3.6 Signal conventions

Signal names are shown in all uppercase letters.

All signals are either high active or low active signals. A dash character (-) at the end of a signal name indicates the signal is a low active signal. A low active signal is true when the signal is below V_{IL} , and is false when the signal is above V_{IH} . No dash at the end of a signal name indicates the signal is a high active signal. A high active signal is true when the signal is above V_{IH} , and is false when the signal is below V_{IL} .

"Asserted" means that the signal is driven by an active circuit to the true state. Negated means that the signal is driven by an active circuit to the false state. "Released" means that

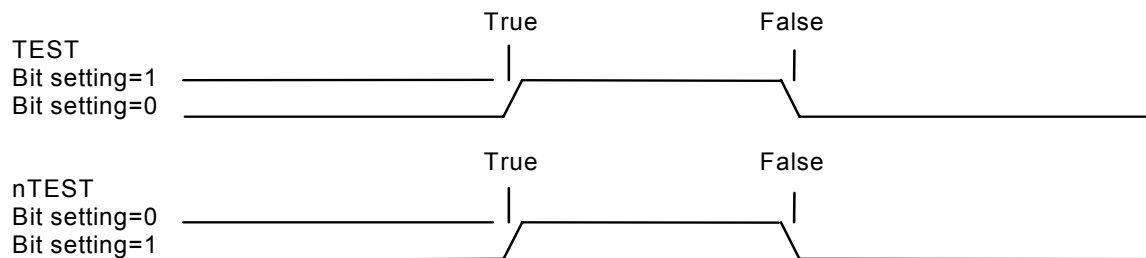
the signal is not actively driven to any state (see clause 6). Some signals have bias circuitry that pull the signal to either a true state or false state when no signal driver is actively asserting or negating the signal.

Control signals that may be used for more than one mutually exclusive functions are identified with their function names separated by a colon (e.g., DIOW:-STOP).

SIGNAL(n:m) denotes a set of signals, for example, DD(15:0).

3.3.7 Bit conventions

Bit names are shown in all uppercase letters except where a lowercase n precedes a bit name. If there is no preceding n, then when BIT is set to one the meaning of the bit is true, and when BIT is cleared to zero the meaning of the bit is false. If there is a preceding n, then when nBIT is cleared to zero the meaning of the bit is true and when nBIT is set to one the meaning of the bit is false.



Bit (n:m) denotes a set of bits, for example, bits (7:0).

3.3.8 State diagram conventions

State diagrams shall be as shown in Figure 2.

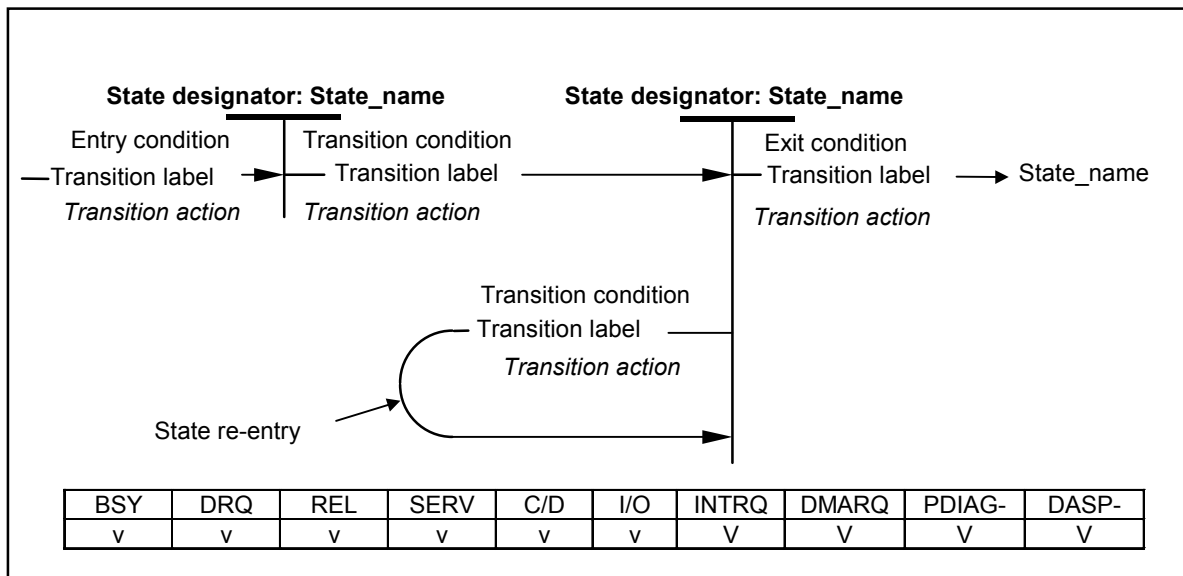


Figure 2 – State diagram convention

Each state is identified by a state designator and a state name. The state designator is unique among all states in all state diagrams in this document. The state designator consists of a set of letters that are capitalized in the title of the figure containing the state diagram followed by a unique number. The state name is a brief description of the primary action taken during the state, and the same state name may appear in other state diagrams. If the same primary function occurs in other states in the same state diagram, they are designated with a unique

letter at the end of the name. Additional actions may be taken while in a state and these actions are described in the state description text.

In device command protocol state diagrams, the state of bits and signals that change state during the execution of this state diagram are shown under the state designator:state_name, and a table is included that shows the state of all bits and signals throughout the state diagram as follows:

v = bit value changes
 1 = bit set to one
 0 = bit cleared to zero
 x = bit is don't care
 V = signal changes
 A = signal is asserted
 N = signal is negated
 R = signal is released
 X = signal is don't care.

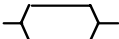
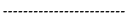
Each transition is identified by a transition label and a transition condition. The transition label consists of the state designator of the state from which the transition is being made followed by the state designator of the state to which the transition is being made. In some cases, the transition to enter or exit a state diagram may come from or go to a number of state diagrams, depending on the command being executed. In this case, the state designator is labeled xx. The transition condition is a brief description of the event or condition that causes the transition to occur and may include a transition action, indicated in italics, that is taken when the transition occurs. This action is described fully in the transition description text.

Upon entry to a state, all actions to be executed in that state are executed. If a state is re-entered from itself, all actions to be executed in the state are executed again.

Transitions from state to state shall be instantaneous.

3.3.9 Timing conventions

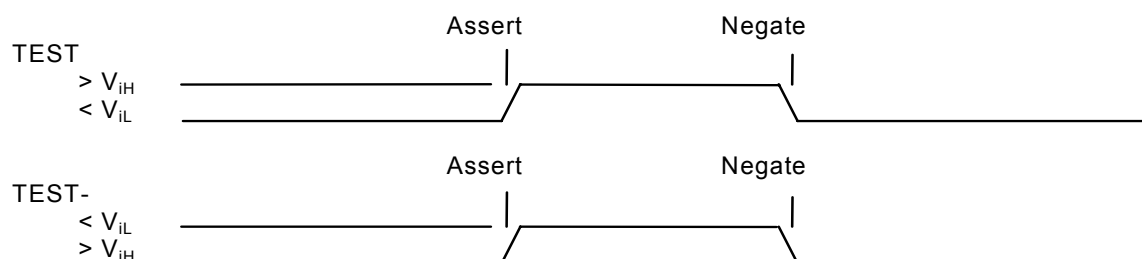
Certain symbols are used in the timing diagrams. These symbols and their respective definitions are listed below.

 or 	- signal transition (asserted or negated)
 or 	- data transition (asserted or negated)
	- data valid
	- undefined but not necessarily released
	- asserted, negated or released
	- released
	- the "other" condition if a signal is shown with no change

All signals are shown with the asserted condition facing to the top of the page. The negated condition is shown towards the bottom of the page relative to the asserted condition.

The interface uses a mixture of negative and positive signals for control and data. The terms asserted and negated are used for consistency and are independent on electrical characteristics.

In all timing diagrams, the lower line indicates negated, and the upper line indicates asserted. The following illustrates the representation of a signal named TEST going from negated to asserted and back to negated, based on the polarity of the signal.



3.3.10 Byte ordering for data transfers

Data is transferred in blocks using either PIO or DMA protocols. PIO data transfers occur when the BSY bit is cleared to zero and the DRQ bit is set to one. These transfers are usually 16-bit but CFA devices may implement 8-bit PIO transfers. Data is transferred in blocks of one or more bytes known as a DRQ block. DMA data transfers occur when the host asserts DMACK- in response to the device asserting DMARQ. DMA transfers are always 16-bit. Each assertion of DMACK- by the host defines a DMA data burst. A DMA data burst is two or more bytes.

Assuming a DRQ block or a DMA burst of data contains "n" bytes of information, the bytes are labeled Byte(0) through Byte(n-1), where Byte(0) is first byte of the block, and Byte(n-1) is the last byte of the block. Table 2 shows the order the bytes shall be presented in when such a block of data is transferred on the interface using 16-bit PIO and DMA transfers. Table 3 shows the order the bytes shall be presented in when such a block or burst of data is transferred on the interface using 8-bit PIO.

Table 2 – Byte order

	DD 15	DD 14	DD 13	DD 12	DD 11	DD 10	DD 9	DD 8	DD 7	DD 6	DD 5	DD 4	DD 3	DD 2	DD 1	DD 0
First transfer	Byte (1)								Byte (0)							
Second transfer	Byte (3)								Byte (2)							
.....																
Last transfer	Byte (n-1)								Byte (n-2)							

Table 3 – Byte order

	DD 7	DD 6	DD 5	DD 4	DD 3	DD 2	DD 1	DD 0
First transfer	Byte (0)							
Second transfer	Byte (1)							
.....								
Last transfer	Byte (n-1)							

NOTE The above description is for data on the interface. Host systems and/or host adapters may cause the order of data as seen in the memory of the host to be different.

Some parameters are defined as a string of ASCII characters. ASCII data fields shall contain only code values 20h through 7Eh. For the string "Copyright", the character "C" is the first byte, the character "o" is the second byte, etc. When such fields are transferred, the order of transmission is:

the 1st character ("C") is on DD(15:8) of the first word,
the 2nd character ("o") is on DD(7:0) of the first word,
the 3rd character ("p") is on DD(15:8) of the second word,
the 4th character ("y") is on DD(7:0) of the second word,
the 5th character ("r") is on DD(15:8) of the third word,
the 6th character ("i") is on DD(7:0) of the third word,
the 7th character ("g") is on DD(15:8) of the fourth word,
the 8th character ("h") is on DD(7:0) of the fourth word,
the 9th character ("t") is on DD(15:8) of the fifth word,
the 10th character ("space") is on DD(7:0) of the fifth word,
etc.

Word (n:m) denotes a set of words, for example, words 100 to 103.

3.3.11 Byte, word and DWORD relationships

Figure 3 illustrates the relationship between bytes, words and DWORDs for serial interface implementations.

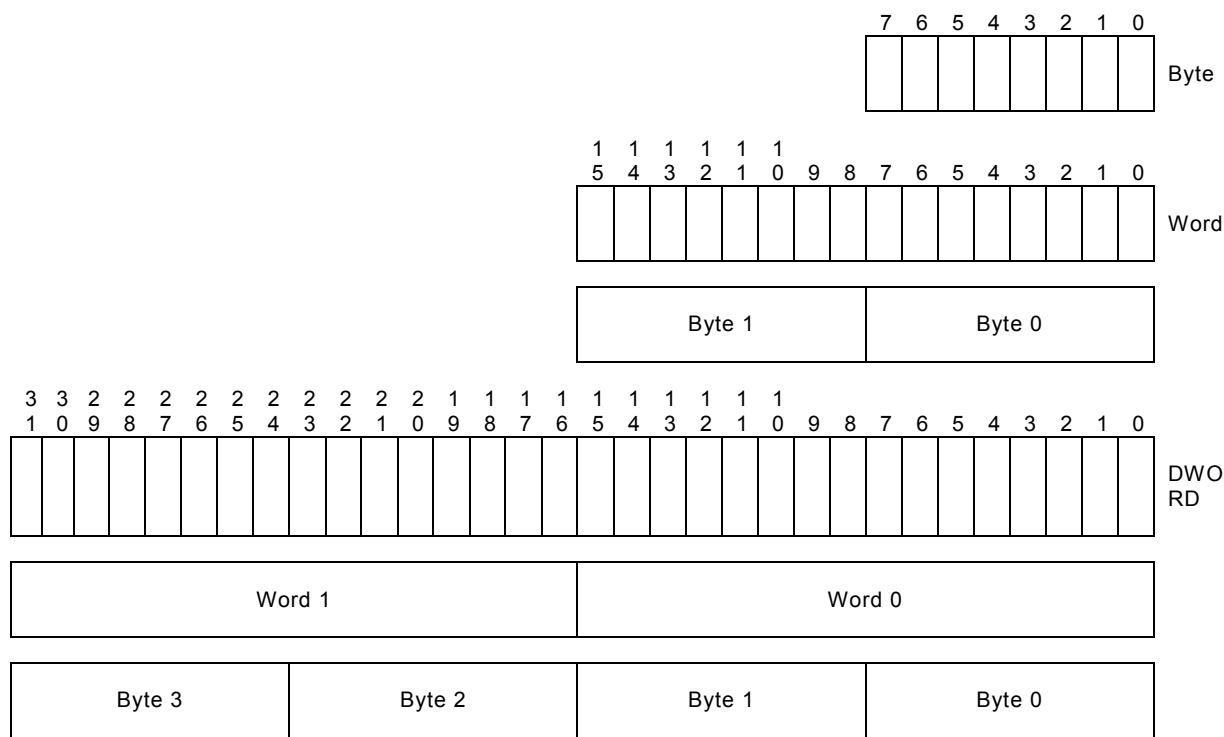


Figure 3 – Byte, word and DWORD relationships

4 General operational requirements

4.1 Command delivery

Commands may be delivered in two forms. For devices that do not implement the PACKET Command feature set, all commands and command parameters are delivered by writing the device Command Block registers. Such commands are defined as register delivered commands.

Devices that implement the PACKET Command feature set use packet delivered commands as well as some register delivered commands.

All register delivered commands and the PACKET command are described in Clause 5.

NOTE The content of command packets delivered during execution of the PACKET command are not described in this standard. See Clause 2 for standards and specifications that define command packet content.

4.2 Register delivered data transfer command sector addressing

4.2.1 General

For register delivered data transfer commands all addressing of data sectors recorded on the device's media is by a logical sector address. There is no implied relationship between logical sector addresses and the actual physical location of the data sector on the media. All devices shall support LBA translation.

In standards ATA/ATAPI-5 and earlier, a CHS translation was defined. This translation is obsolete but if implemented it shall be implemented as defined in ATA/ATAPI-5.

4.2.2 Definitions and value ranges of IDENTIFY DEVICE data words

(Also see 6.17)

- 1) Words 60 to 61 shall contain the value one greater than the total number of user-addressable sectors in 28-bit addressing and shall not exceed 0FFFFFFFh. The content of words 60 to 61 shall be greater than or equal to one and less than or equal to 268,435,455.
- 2) Words 100 to 103 shall contain the value one greater than the total number of user-addressable sectors in 48-bit addressing and shall not exceed 0000FFFFFFFFFh.
- 3) The contents of words 60 to 61 and 100 to 103 may be affected by the host issuing a SET MAX ADDRESS or SET MAX ADDRESS EXT command.
- 4) The contents of words 60 to 61 and 100 to 103 shall not be used to determine if 48-bit addressing is supported. IDENTIFY DEVICE bit 10 word 83 indicates support for 48-bit addressing.

4.2.3 Addressing constraints and error reporting

Devices shall set IDNF to one or ABRT to one in the Error register and ERR to one in the Status register in response to any command where the requested LBA number is greater than or equal to the content of words 60 to 61 for a 28-bit addressing command or greater or equal to the contents of words 100 to 103 for a 48-bit addressing command.

4.3 General feature set

4.3.1 General

The General feature set defines the common commands implemented by devices.

4.3.2 General feature set for devices not implementing the PACKET command feature set

The following General feature set commands are mandatory for all devices that are capable of both reading and writing their media and do not implement the PACKET command feature set:

- EXECUTE DEVICE DIAGNOSTIC
- FLUSH CACHE
- IDENTIFY DEVICE
- READ DMA
- READ MULTIPLE
- READ SECTOR(S)
- READ VERIFY SECTOR(S)
- SET FEATURES
- SET MULTIPLE MODE
- WRITE DMA
- WRITE MULTIPLE
- WRITE SECTOR(S)

The following General feature set commands are mandatory for all devices that are capable of only reading their media and do not implement the PACKET command feature set:

- EXECUTE DEVICE DIAGNOSTIC
- IDENTIFY DEVICE
- READ DMA
- READ MULTIPLE
- READ SECTOR(S)
- READ VERIFY SECTOR(S)

- SET FEATURES
- SET MULTIPLE MODE

The following General feature set commands are optional for devices not implementing the PACKET command feature set:

- DOWNLOAD MICROCODE
- NOP
- READ BUFFER
- WRITE BUFFER

The following General feature set command is prohibited for use by devices not implementing the PACKET command feature set:

- DEVICE RESET

The following resets are mandatory for devices not implementing the PACKET command feature set:

- Power-on reset: Executed at power-on, the device may execute a series of diagnostics and shall set default values (see Clauses 11 and 17)
- Hardware reset: Executed in response to the assertion of the RESET- signal the device may execute a series of diagnostics and shall set default values (see Clauses 11 and 17).
- Software reset: Executed in response to the setting of the SRST bit in the Device Control register the device resets the interface circuitry (see Clauses 11 and 17).

4.3.3 General feature set for devices implementing the PACKET command feature set

The following General feature set commands are mandatory for all devices implementing the PACKET command feature set:

- EXECUTE DEVICE DIAGNOSTIC
- IDENTIFY DEVICE
- NOP
- READ SECTOR(S)
- SET FEATURES

The following General feature set commands are optional for all devices implementing the PACKET command feature set:

- FLUSH CACHE

The following General command set commands are prohibited for use by devices implementing the PACKET command feature set. These functions are supported by Packet commands.

- DOWNLOAD MICROCODE
- READ BUFFER
- READ DMA
- READ MULTIPLE
- READ VERIFY
- SET MULTIPLE MODE
- WRITE BUFFER
- WRITE DMA
- WRITE MULTIPLE
- WRITE SECTOR(S)

The following resets are mandatory for devices implementing the PACKET command feature set:

- Power-on reset: Executed at power-on, the device may execute a series of diagnostics and shall set default values (see clause 11).
- Hardware reset: Executed in response to the assertion of the RESET- signal the device may execute a series of and shall set default values (see clause 11).
- Software reset: Executed in response to the setting of the SRST bit in the Device Control register the device resets the interface circuitry (see clause 11).
- DEVICE RESET: Executed in response to the DEVICE RESET command the device resets the interface circuitry (see 6.11).

4.4 PACKET Command feature set

4.4.1 General

The optional PACKET Command feature set provides for devices that require command parameters that are too extensive to be expressed in the Command Block registers. Devices implementing the PACKET Command feature set exhibit responses different from those exhibited by devices not implementing this feature set.

The commands unique to the PACKET Command feature set are:

- PACKET
- DEVICE RESET
- IDENTIFY PACKET DEVICE

4.4.2 Identification of PACKET Command feature set devices

When executing a power-on, hardware, DEVICE RESET or software reset, a device implementing the PACKET Command feature set shall perform the same reset protocol as other devices, but leaves the registers with a signature unique to PACKET Command feature set devices (see 5.15).

In addition, the IDENTIFY DEVICE command shall not be executed but shall be command aborted and shall return a signature unique to devices implementing the PACKET Command feature set. The IDENTIFY PACKET DEVICE command is used by the host to get identifying parameter information for a device implementing the PACKET Command feature set (see 6.17.5.2 and 6.18).

4.4.3 PACKET Command feature set resets

Devices implementing the PACKET Command feature set respond to power-on, hardware, and software resets as any other device except for the resulting contents in the device registers as described above. However, software reset should not be issued while a PACKET command is in progress. PACKET commands used by some devices do not terminate if a software reset is issued.

The DEVICE RESET command is provided to allow the device to be reset without affecting the other device on the bus.

4.4.4 The PACKET command

The PACKET command allows a host to send a command to the device via a command packet. The command packet contains the command and command parameters that the device is to execute.

Upon receipt of the PACKET command the device sets BSY to one and prepares to receive the command packet. When ready, the device sets DRQ to one and clears BSY to zero. The command packet is then transferred to the device by PIO transfer. When the last word of the command packet is transferred, the device sets BSY to one, and clears DRQ to zero (see 6.25 and clause 10 in ISO/IEC 24739-2).

4.5 Power Management feature set

4.5.1 General

A device shall implement power management. A device implementing the PACKET Command feature set may implement the power management as defined by the PACKET command set implemented by the device. Otherwise, the device shall implement the Power Management feature set as described in this standard.

The Power Management feature set permits a host to modify the behavior of a device in a manner that reduces the power required to operate. The Power Management feature set provides a set of commands and a timer that enable a device to implement low power consumption modes. A register delivered command device that implements the Power Management feature set shall implement the following minimum set of functions: See also 4.6 and 4.12.

- A Standby timer
- CHECK POWER MODE command
- IDLE command
- IDLE IMMEDIATE command
- SLEEP command
- STANDBY command
- STANDBY IMMEDIATE command

A device that implements the PACKET Command feature set and implements the Power Management feature set shall implement the following minimum set of functions:

- CHECK POWER MODE command
- IDLE IMMEDIATE command
- SLEEP command
- STANDBY IMMEDIATE command

4.5.2 Power management commands

The CHECK POWER MODE command allows a host to determine if a device is currently in, going to or leaving Standby or Idle mode. The CHECK POWER MODE command shall not change the power mode or affect the operation of the Standby timer.

The IDLE and IDLE IMMEDIATE commands move a device to Idle mode immediately from the Active or Standby modes. The IDLE command also sets the Standby timer count and enables or disables the Standby timer.

The STANDBY and STANDBY IMMEDIATE commands move a device to Standby mode immediately from the Active or Idle modes. The STANDBY command also sets the Standby timer count and enables or disables the Standby timer.

The SLEEP command moves a device to Sleep mode. The device's interface becomes inactive at command completion of the SLEEP command. A hardware or software reset or DEVICE RESET command is required to move a device out of Sleep mode.

4.5.3 Standby timer

The Standby timer provides a method for the device to automatically enter Standby mode from either Active or Idle mode following a host programmed period of inactivity. If the Standby timer is enabled and if the device is in the Active or Idle mode, the device waits for the specified time period and if no command is received, the device automatically enters the Standby mode.

If the Standby timer is disabled, the device may automatically enter Standby mode.

4.5.4 Power modes

Figure 4 shows the set of mode transitions that shall be implemented.

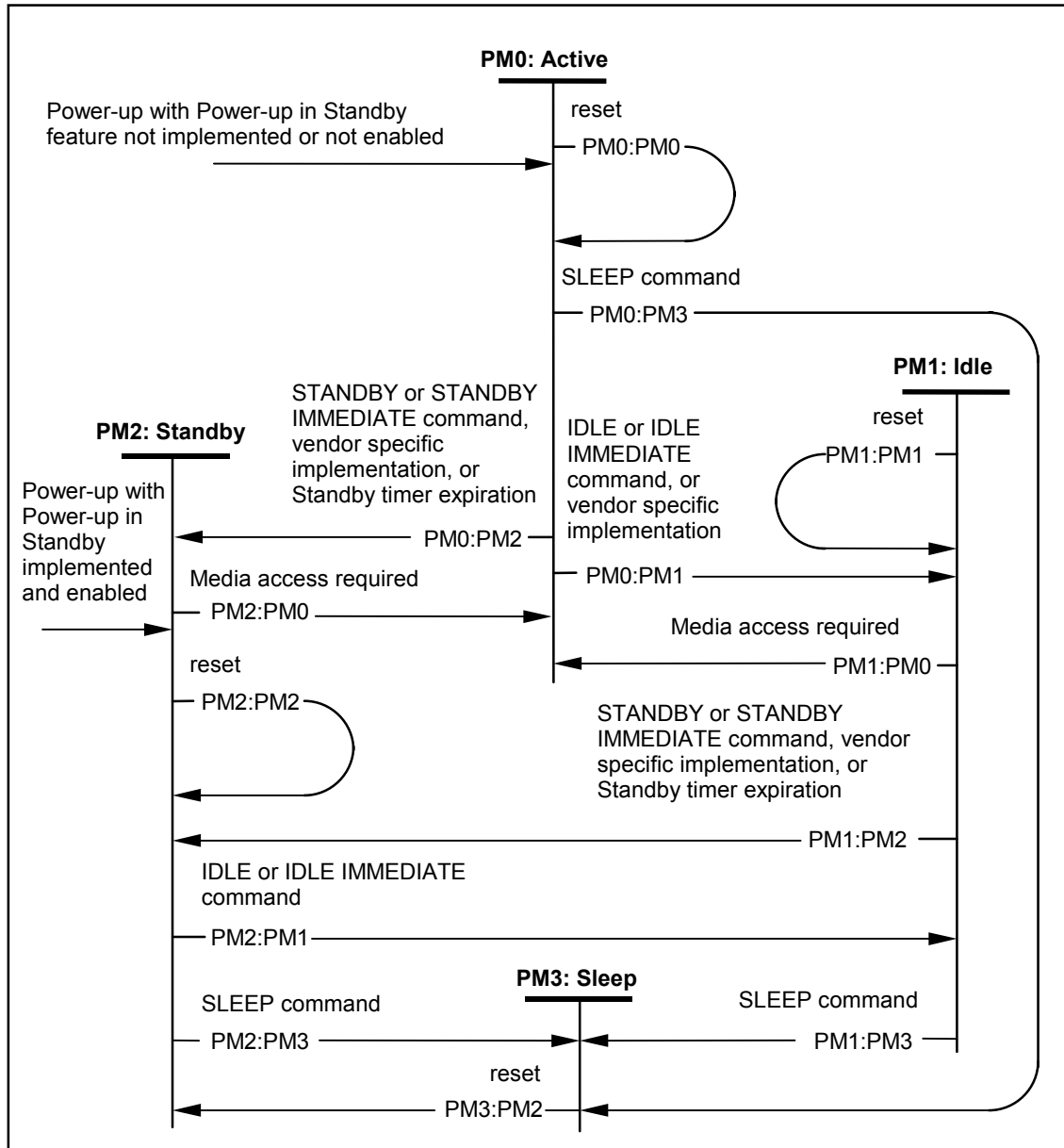


Figure 4 – Power management state diagram

PM0: Active: This mode shall be entered when the device receives a media access command while in Idle or Standby mode. This mode shall also be entered when the device is powered-up with the Power-Up In Standby feature not implemented or not enabled (see 4.12).

In Active mode the device is capable of responding to commands. During the execution of a media access command a device shall be in Active mode. Power consumption is greatest in this mode.

Transition PM0:PM0: When hardware reset, software reset or DEVICE RESET command is received, the device shall make a transition to the PM0: Active mode when the reset protocol is completed.

Transition PM0:PM1: When an IDLE or IDLE IMMEDIATE command is received or when a vendor specific implementation determines a transition is required, then the device shall make a transition to the PM1:Idle mode.

Transition PM0:PM2: When a STANDBY or STANDBY IMMEDIATE command is received, the Standby timer expires, or a vendor specific implementation determines a transition is required, then the device shall make a transition to the PM2:Standby mode.

Transition PM0:PM3: When a SLEEP command is received, the device shall make a transition to the PM3:Sleep mode.

PM1: Idle: This mode shall be entered when the device receives an IDLE or IDLE IMMEDIATE command. Some devices may perform vendor specific internal power management and make a transition to the Idle mode without host intervention.

In Idle mode the device is capable of responding to commands but the device may take longer to complete commands than when in the Active mode. Power consumption may be reduced from that of Active mode.

Transition PM1:PM0: When a media access is required, the device shall make a transition to the PM0:Active mode.

Transition PM1:PM1: When hardware reset, software reset, or DEVICE RESET command is received, the device shall make a transition to the PM1:Idle mode when the reset protocol is completed.

Transition PM1:PM2: When a STANDBY or STANDBY IMMEDIATE command is received, the Standby timer expires, or a vendor specific implementation determines a transition is required, then the device shall make a transition to the PM2:Standby mode.

Transition PM1:PM3: When a SLEEP command is received, the device shall make a transition to the PM3:Sleep mode.

PM2: Standby: This mode shall be entered when the device receives a STANDBY command, a STANDBY IMMEDIATE command or the Standby timer expires. Some devices may perform vendor specific internal power management and make a transition to the Standby mode without host intervention. This mode shall also be entered when the device is powered-up with the Power-Up In Standby feature implemented and enabled.

In Standby mode the device is capable of responding to commands but the device may take longer to complete commands than in the Idle mode. The time to respond could be as long as 30 s. Power consumption may be reduced from that of Idle mode.

Transition PM2:PM0: When a media access is required, the device shall make a transition to the PM0:Active mode.

Transition PM2:PM1: When an IDLE or IDLE IMMEDIATE command is received, or a vendor specific implementation determines a transition is required, then the device shall make a transition to the PM1:Idle mode.

Transition PM2:PM2: When hardware reset, software reset, or DEVICE RESET command is received, the device shall make a transition to the PM2:Standby mode when the reset protocol is completed.

Transition PM2:PM3: When a SLEEP command is received, the device shall make a transition to the PM3:Sleep mode.

PM3: Sleep: This mode shall be entered when the device receives a SLEEP command.

In Sleep mode the device requires a hardware or software reset or a DEVICE RESET command to be activated. The time to respond could be as long as 30 s. Sleep mode provides the lowest power consumption of any mode.

In Sleep mode, the device's interface is not active. The content of the Status register is invalid in this mode.

Transition PM3:PM2: When hardware reset, software reset or DEVICE RESET command is received the device shall make a transition to the PM2:Standby mode.

4.6 Advanced Power Management feature set

The Advanced Power Management feature set is an optional feature set that allows the host to select a power management level. The power management level is specified using a scale from the lowest power consumption setting of 01h to the maximum performance level of FEh. Device performance may increase with increasing power management levels. Device power consumption may increase with increasing power management levels. A device may implement one power management method for two or more contiguous power management levels. For example, a device may implement one power management method from level 80h to A0h and a higher performance, higher power consumption method from level A1h to FEh. Advanced power management levels 80h and higher do not permit the device to spin down to save power.

The Advanced Power Management feature set uses the following functions:

- A SET FEATURES subcommand to enable Advanced Power Management
- A SET FEATURES subcommand to disable Advanced Power Management

Advanced Power Management is independent of the Standby timer setting. If both Advanced Power Management and the Standby timer are set, the device will go to the Standby state when the timer times out or the device's Advanced Power Management algorithm indicates that the Standby state should be entered.

The device shall indicate:

- a) feature set support in IDENTIFY DEVICE data and IDENTIFY PACKET DEVICE data word 83 bit 3;
- b) feature set enabled in IDENTIFY DEVICE data and IDENTIFY PACKET DEVICE data word 86 bit 3; and
- c) APM Level in IDENTIFY DEVICE data and IDENTIFY PACKET DEVICE data word 91.

4.7 Security Mode feature set

4.7.1 General

The optional Security Mode feature set is a password system that restricts access to user data stored on a device. The system has two passwords, User and Master, and two security levels, High and Maximum. The security system is enabled by sending a user password to the device with the SECURITY SET PASSWORD command. When the security system is enabled, access to user data on the device is denied after a power cycle until the User password is sent to the device with the SECURITY UNLOCK command.

A Master password may be set in addition to the User password. The purpose of the Master password is to allow an administrator to establish a password that is kept secret from the user, and which may be used to unlock the device if the User password is lost. Setting the Master password does not enable the password system.

The security level is set to High or Maximum with the SECURITY SET PASSWORD command. The security level determines device behavior when the Master password is used to unlock

the device. When the security level is set to High the device requires the SECURITY UNLOCK command and the Master password to unlock. When the security level is set to Maximum the device requires a SECURITY ERASE PREPARE command and a SECURITY ERASE UNIT command with the Master password to unlock. Execution of the SECURITY ERASE UNIT command erases all user data on the device.

The SECURITY FREEZE LOCK command prevents changes to passwords until a following power cycle. The purpose of the SECURITY FREEZE LOCK command is to prevent password setting attacks on the security system.

A device that implements the Security Mode feature set shall implement the following minimum set of commands:

- SECURITY SET PASSWORD
- SECURITY UNLOCK
- SECURITY ERASE PREPARE
- SECURITY ERASE UNIT
- SECURITY FREEZE LOCK
- SECURITY DISABLE PASSWORD

Support of the Security Mode feature set is indicated in IDENTIFY DEVICE data word 82 and data word 128.

4.7.2 Security mode initial setting

When the device is shipped by the manufacturer, the state of the Security Mode feature shall be disabled. The initial Master password value is not defined by this standard.

If the Master Password Revision Code feature is supported, the Master Password Revision Code shall be set to FFFEh by the manufacturer.

4.7.3 User password lost

If the User password sent to the device with the SECURITY UNLOCK command does not match the user password previously set with the SECURITY SET PASSWORD command, the device shall not allow the user to access data.

If the Security Level was set to High during the last SECURITY SET PASSWORD command, the device shall unlock if the Master password is received.

If the Security Level was set to Maximum during the last SECURITY SET PASSWORD command, the device shall not unlock if the Master password is received. The SECURITY ERASE UNIT command shall erase all user data and unlock the device if the Master password matches the last Master password previously set with the SECURITY SET PASSWORD command.

4.7.4 Attempt limit for SECURITY UNLOCK command

The device shall have an attempt limit counter. The purpose of this counter is to defeat repeated trial attacks. After each failed User or Master password SECURITY UNLOCK command, the counter is decremented. When the counter value reaches zero the EXPIRE bit (bit 4) of IDENTIFY DEVICE data word 128 is set to one, and the SECURITY UNLOCK and SECURITY UNIT ERASE commands are command aborted until the device is powered off or hardware reset. The EXPIRE bit shall be cleared to zero after power-on or hardware reset. The counter shall be set to five after a power-on or hardware reset.

4.7.5 Security mode states

Figure 5 describes security mode states and state transitions.

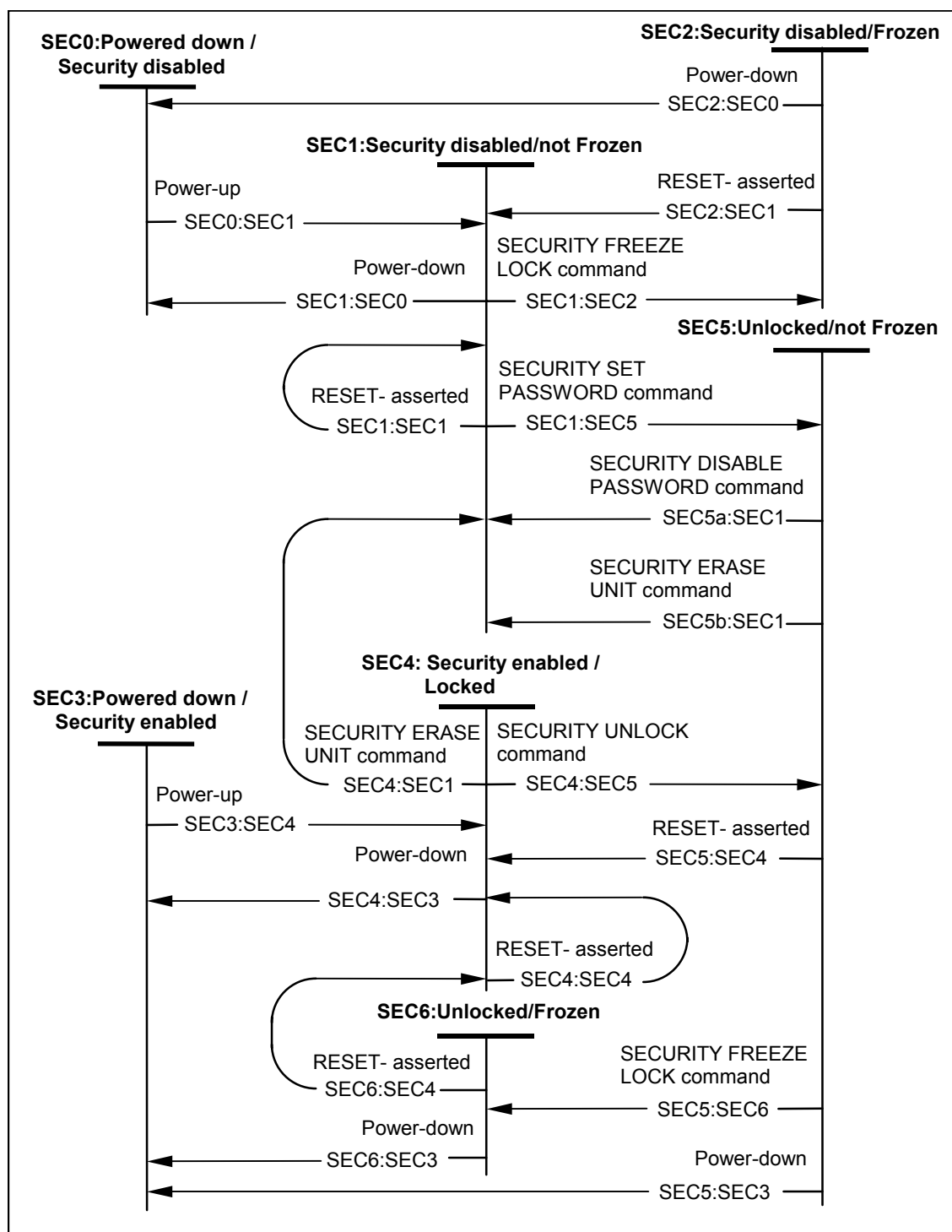


Figure 5 – Security mode state diagram

SEC0: Powered down/Security disabled: This mode shall be entered when the device is powered-down with the Security Mode feature set disabled.

Transition SEC0:SEC1: When the device is powered-up, the device shall make a transition to the SEC1: Security disabled/not Frozen state.

SEC1: Security disabled/not Frozen: This mode shall be entered when the device is powered-up or a hardware reset is received with the Security Mode feature set disabled or when the Security Mode feature set is disabled by a SECURITY DISABLE PASSWORD or SECURITY ERASE UNIT command.

In this state, the device is capable of responding to all commands (see Table 4 Unlocked column).

Transition SEC1:SEC0: When the device is powered-down, the device shall make a transition to the SEC0: Powered down/Security disabled state.

Transition SEC1:SEC1: When the device receives a hardware reset, the device shall make a transition to the SEC1: Security disabled/not Frozen state.

Transition SEC1:SEC2: When a SECURITY FREEZE LOCK command is received, the device shall make a transition to the SEC2: Security disabled/Frozen state.

Transition SEC1:SEC5: When a SECURITY SET PASSWORD command is received, the device shall make a transition to the SEC5: Unlocked/not frozen state

SEC2: Security disabled/Frozen: This mode shall be entered when the device receives a SECURITY FREEZE LOCK command while in Security disabled/not Frozen state.

In this state, the device is capable of responding to all commands except those indicated in Table 4, Frozen column.

Transition SEC2:SEC0: When the device is powered-down, the device shall make a transition to the SEC0: Powered down/Security disabled state.

Transition SEC2:SEC1: When the device receives a hardware reset, the device shall make a transition to the SEC1: Security disabled/not Frozen state.

SEC3: Powered down/Security enabled: This mode shall be entered when the device is powered-down with the Security Mode feature set enabled.

Transition SEC3:SEC4: When the device is powered-up, the device shall make a transition to the SEC4: Security enabled/locked state.

SEC4: Security enabled/Locked: This mode shall be entered when the device is powered-up or a hardware reset is received with the Security Mode feature set enabled.

In this state, the device shall only respond to commands that do not access data in the user data area of the media (see Table 4 Locked column).

Transition SEC4:SEC3: When the device is powered-down, the device shall make a transition to the SEC3: Powered down/Security enabled state.

Transition SEC4:SEC4: When the device receives a hardware reset, the device shall make a transition to the SEC4: Security enabled/locked state.

Transition SEC4:SEC5: When a valid SECURITY UNLOCK command is received, the device shall make a transition to the SEC5: Unlocked/not Frozen state.

Transition SEC4:SEC1: When a SECURITY ERASE PREPARE command is received and is followed by a SECURITY ERASE UNIT command, the device shall make a transition to the SEC1: Security disabled/not Frozen state.

SEC5: Unlocked/not Frozen: This mode shall be entered when the device receives a SECURITY SET PASSWORD command to enable the lock or a SECURITY UNLOCK command.

In this state, the device shall respond to all commands (see Table 4, Unlocked column).

Transition SEC5a:SEC1: When a valid SECURITY DISABLE PASSWORD command is received, the device shall make a transition to the SEC1: Security disabled/not Frozen state.

Transition SEC5b:SEC1: When a SECURITY ERASE PREPARE command is received and is followed by a SECURITY ERASE UNIT command, the device shall make a transition to the SEC1: Security disabled/not Frozen state.

Transition SEC5:SEC6: When a SECURITY FREEZE LOCK command is received, the device shall make a transition to the SEC6: Unlocked/Frozen state.

Transition SEC5:SEC3: When the device is powered-down, the device shall make a transition to the SEC3: Powered down/Security enabled state.

Transition SEC5:SEC4: When the device receives a hardware reset, the device shall make a transition to the SEC4: Security enabled/Locked state.

SEC6: Unlocked/ Frozen: This mode shall be entered when the device receives a SECURITY FREEZE LOCK command while in Unlocked/Locked state.

In this state, the device is capable of responding to all commands except those indicated in Table 4, Frozen column.

Transition SEC6:SEC3: When the device is powered-down, the device shall make a transition to the SEC3: Powered down/Security enabled state.

Transition SEC6:SEC4: When the device receives a hardware reset, the device shall make a transition to the SEC4: Security enabled/Locked state.

Table 4 – Security mode command actions

Command	Locked	Unlocked	Frozen
CFA ERASE SECTORS	Command aborted	Executable	Executable
CFA REQUEST EXTENDED ERROR CODE	Executable	Executable	Executable
CFA TRANSLATE SECTOR	Executable	Executable	Executable
CFA WRITE MULTIPLE WITHOUT ERASE	Command aborted	Executable	Executable
CFA WRITE SECTORS WITHOUT ERASE	Command aborted	Executable	Executable
CHECK MEDIA CARD TYPE	Command aborted	Executable	Executable
CHECK POWER MODE	Executable	Executable	Executable
CONFIGURE STREAM	Command aborted	Executable	Executable
DEVICE CONFIGURATION	Command aborted	Executable	Executable
DEVICE RESET	Executable	Executable	Executable
DOWNLOAD MICROCODE	Vendor Specific	Vendor Specific	Vendor Specific
EXECUTE DEVICE DIAGNOSTIC	Executable	Executable	Executable
FLUSH CACHE	Command aborted	Executable	Executable
FLUSH CACHE EXT	Command aborted	Executable	Executable
GET MEDIA STATUS	Command aborted	Executable	Executable
IDENTIFY DEVICE	Executable	Executable	Executable
IDENTIFY PACKET DEVICE	Executable	Executable	Executable
IDLE	Executable	Executable	Executable
IDLE IMMEDIATE	Executable	Executable	Executable
MEDIA EJECT	Command aborted	Executable	Executable
MEDIA LOCK	Command aborted	Executable	Executable
MEDIA UNLOCK	Command aborted	Executable	Executable
NOP	Executable	Executable	Executable
PACKET	Command aborted	Executable	Executable
READ BUFFER	Executable	Executable	Executable
READ DMA	Command aborted	Executable	Executable
READ DMA EXT	Command aborted	Executable	Executable
READ DMA QUEUED	Command aborted	Executable	Executable
READ DMA QUEUED EXT	Command aborted	Executable	Executable
READ LOG EXT	Command aborted	Executable	Executable
READ MULTIPLE	Command aborted	Executable	Executable
READ MULTIPLE EXT	Command aborted	Executable	Executable
READ NATIVE MAX ADDRESS	Executable	Executable	Executable
READ NATIVE MAX ADDRESS EXT	Executable	Executable	Executable
READ SECTOR(S)	Command aborted	Executable	Executable
READ SECTOR(S) EXT	Command aborted	Executable	Executable
READ STREAM DMA EXT	Command aborted	Executable	Executable
READ STREAM EXT	Command aborted	Executable	Executable
READ VERIFY SECTOR(S)	Command aborted	Executable	Executable
READ VERIFY SECTOR(S) EXT	Command aborted	Executable	Executable
SECURITY DISABLE PASSWORD	Command aborted	Executable	Command aborted
SECURITY ERASE PREPARE	Executable	Executable	Command aborted

Command	Locked	Unlocked	Frozen
SECURITY ERASE UNIT	Executable	Executable	Command aborted
SECURITY FREEZE LOCK	Command aborted	Executable	Executable
SECURITY SET PASSWORD	Command aborted	Executable	Command aborted
SECURITY UNLOCK	Executable	Executable	Command aborted
SERVICE	Command aborted	Executable	Executable
SET FEATURES	Executable	Executable	Executable
SET MAX ADDRESS	Command aborted	Executable	Executable
SET MAX ADDRESS EXT	Command aborted	Executable	Executable
SET MAX SET PASSWORD	Command aborted	Executable	Executable
SET MAX LOCK	Command aborted	Executable	Executable
SET MAX FREEZE LOCK	Command aborted	Executable	Executable
SET MAX UNLOCK	Command aborted	Executable	Executable
SET MULTIPLE MODE	Executable	Executable	Executable
SLEEP	Executable	Executable	Executable
SMART DISABLE OPERATIONS	Executable	Executable	Executable
SMART ENABLE/DISABLE AUTOSAVE	Executable	Executable	Executable
SMART ENABLE OPERATIONS	Executable	Executable	Executable
SMART EXECUTE OFF-LINE IMMEDIATE	Executable	Executable	Executable
SMART READ DATA	Executable	Executable	Executable
SMART READ LOG	Executable	Executable	Executable
SMART RETURN STATUS	Executable	Executable	Executable
SMART WRITE LOG	Executable	Executable	Executable
STANDBY	Executable	Executable	Executable
STANDBY IMMEDIATE	Executable	Executable	Executable
WRITE BUFFER	Executable	Executable	Executable
WRITE DMA	Command aborted	Executable	Executable
WRITE DMA EXT	Command aborted	Executable	Executable
WRITE DMA FUA EXT	Command aborted	Executable	Executable
WRITE DMA QUEUED	Command aborted	Executable	Executable
WRITE DMA QUEUED EXT	Command aborted	Executable	Executable
WRITE DMA QUEUED FUA EXT	Command aborted	Executable	Executable
WRITE LOG EXT	Command aborted	Executable	Executable
WRITE MULTIPLE	Command aborted	Executable	Executable
WRITE MULTIPLE EXT	Command aborted	Executable	Executable
WRITE MULTIPLE FUA EXT	Command aborted	Executable	Executable
WRITE SECTOR(S)	Command aborted	Executable	Executable
WRITE SECTOR(S) EXT	Command aborted	Executable	Executable
WRITE STREAM DMA EXT	Command aborted	Executable	Executable
WRITE STREAM EXT	Command aborted	Executable	Executable

4.8 SMART (self-monitoring, analysis and reporting technology) feature set

4.8.1 General

The intent of self-monitoring, analysis and reporting technology (the SMART feature set) is to protect user data and minimize the likelihood of unscheduled system downtime that may be caused by predictable degradation and/or fault of the device. By monitoring and storing critical performance and calibration parameters, SMART feature set devices attempt to predict the likelihood of near-term degradation or fault condition. Providing the host system the knowledge of a negative reliability condition allows the host system to warn the user of the impending risk of a data loss and advise the user of appropriate action. Support of this feature set is indicated in the IDENTIFY DEVICE data.

Devices that implement the PACKET Command feature set shall not implement the SMART feature set as described in this standard. Devices that implement the PACKET Command feature set and SMART shall implement SMART as defined by the command packet set implemented by the device. This feature set is optional if the PACKET Command feature set is not supported.

4.8.2 Device SMART data structure

SMART feature set capability and status information for the device are stored in the device SMART data structure. The off-line data collection capability and status data stored herein may be useful to the host if the SMART EXECUTE OFF-LINE IMMEDIATE command is implemented (see 6.54.5).

4.8.3 On-line data collection

Collection of SMART data in an “on-line” mode shall have no impact on device performance. The SMART data that is collected or the methods by which data is collected in this mode may be different from those in the off-line data collection mode for any particular device and may vary from one device to another.

4.8.4 Off-line data collection

The device shall use off-line mode for data collection and self-test routines that have an impact on performance if the device is required to respond to commands from the host while performing that data collection. This impact on performance may vary from device to device. The data that is collected or the methods by which the data is collected in this mode may be different from those in the on-line data collection mode for any particular device and may vary from one device to another.

4.8.5 Threshold exceeded condition

This condition occurs when the device's SMART reliability status indicates an impending degrading or fault condition.

4.8.6 SMART feature set commands

These commands use a single command code and are differentiated from one another by the value placed in the Features register (see 6.54).

If the SMART feature set is implemented, the following commands shall be implemented.

- SMART DISABLE OPERATIONS
- SMART ENABLE/DISABLE AUTOSAVE
- SMART ENABLE OPERATIONS
- SMART RETURN STATUS

If the SMART feature set is implemented, the following commands may be implemented.

- SMART EXECUTE OFF-LINE IMMEDIATE
- SMART READ DATA
- SMART READ LOG
- SMART WRITE LOG
- READ LOG EXT
- WRITE LOG EXT

4.8.7 SMART operation with power management modes

When used with a host that has implemented the Power Management feature set, a SMART enabled device should automatically save the device accumulated SMART data upon receipt of an IDLE IMMEDIATE, STANDBY IMMEDIATE, or SLEEP command or upon return to an Active or Idle mode from a Standby mode (see 6.54.6).

If a SMART feature set enabled device has been set to use the Standby timer, the device should automatically save the device accumulated SMART data prior to going from an Idle mode to the Standby mode or upon return to an Active or Idle mode from a Standby mode.

A device shall not execute any routine to automatically save the device accumulated SMART data while the device is in a Standby or Sleep mode.

4.8.8 SMART device error log reporting

Logging of reported errors is an optional SMART feature. If error logging is supported by a device, it is indicated in byte 370 of the SMART READ DATA command response and bit 0 of word 84 of the IDENTIFY DEVICE response. If error logging is supported, the device shall provide information on the last five errors that the device reported as described in the SMART READ LOG command (see 6.54.7). The device may also provide additional vendor specific information on these reported errors.

If error logging is supported, it shall not be disabled when SMART is disabled. Error log information shall be gathered when the device is powered-on except that logging of errors when in a reduced power mode is optional. If errors are logged when in a reduced power mode, the reduced power mode shall not change. Disabling SMART shall disable the delivering of error log information via the SMART READ LOG command.

If a device receives a firmware modification, all error log data shall be discarded and the device error count for the life of the device shall be reset to zero.

4.9 Host Protected Area feature set

4.9.1 General

A reserved area for data storage outside the normal operating system file system is required for several specialized applications. Systems may wish to store configuration data or save memory to the device in a location that the operating systems cannot change. The optional Host Protected Area feature set allows a portion of the device to be reserved for such an area when the device is initially configured. A device that implements the Host Protected Area feature set shall implement the following minimum set of commands:

- READ NATIVE MAX ADDRESS
- SET MAX ADDRESS

A device that implements the Host Protected Area feature set and supports the 48-bit Address feature set shall implement the following additional set of commands:

- READ NATIVE MAX ADDRESS EXT
- SET MAX ADDRESS EXT

Devices supporting this feature set shall set bit 10 of word 82 to one in the data returned by the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE command.

In addition, a device supporting the Host Protected Area feature set may optionally include the security extensions. The Host Protected Area security commands use a single command code and are differentiated from one another by the value placed in the Features register.

- SET MAX SET PASSWORD
- SET MAX LOCK
- SET MAX FREEZE LOCK
- SET MAX UNLOCK

Devices supporting these extensions shall set bit 10 of word 82 and bit 8 of word 83 of the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data to one.

The READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command allows the host to determine the maximum native address space of the device even when a protected area has been allocated.

The SET MAX ADDRESS or SET MAX ADDRESS EXT command allows the host to redefine the maximum address of the user accessible address space. That is, when the SET MAX ADDRESS or SET MAX ADDRESS EXT command is issued with a maximum address less than the native maximum address, the device reduces the user accessible address space to the maximum specified by the command, providing a protected area above that maximum address. The SET MAX ADDRESS or SET MAX ADDRESS EXT command shall be immediately preceded by a READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command. After the SET MAX ADDRESS or SET MAX ADDRESS EXT command has been issued, the device shall report only the reduced user address space in response to an IDENTIFY DEVICE command in words 60, 61, 100, 101, 102 and 103. Any read or write command to an address above the maximum address specified by the SET MAX ADDRESS or SET MAX ADDRESS EXT command shall cause command completion with the IDNF bit set to one and ERR set to one, or command aborted. A volatility bit in the Sector Count register allows the host to specify if the maximum address set is preserved across power-on or hardware reset cycles. On power-on or hardware reset the device maximum address returns to the last non-volatile address setting regardless of subsequent volatile SET MAX ADDRESS or SET MAX ADDRESS EXT commands. If the SET MAX ADDRESS or SET MAX ADDRESS EXT command is issued with a value that exceeds the native maximum address command aborted shall be returned.

Typical use of these commands would be

- on reset
 - a) BIOS receives control after a system reset;
 - b) BIOS issues a READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command to find the max capacity of the device;
 - c) BIOS issues a SET MAX ADDRESS or SET MAX ADDRESS EXT command to the values returned by READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT;
 - d) BIOS reads configuration data from the highest area on the disk;
 - e) BIOS issues a READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command followed by a SET MAX ADDRESS or SET MAX ADDRESS EXT command to reset the device to the size of the file system.
- on save to disk
 - a) BIOS receives control prior to shut down;
 - b) BIOS issues a READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT command to find the max capacity of the device;

- c) BIOS issues a volatile SET MAX ADDRESS or SET MAX ADDRESS EXT command to the values returned by READ NATIVE MAX ADDRESS or READ NATIVE MAX ADDRESS EXT;
- d) Memory is copied to the reserved area;
- e) Shut down completes;
- f) On power-on or hardware reset the device max address returns to the last non-volatile setting.

These commands are intended for use only by system BIOS or other low-level boot time process. Using these commands outside BIOS controlled boot or shutdown may result in damage to file systems on the device. Devices should return command aborted if a subsequent non-volatile SET MAX ADDRESS or SET MAX ADDRESS EXT command is received after a power-on or hardware reset.

The SET MAX SET PASSWORD command allows the host to define the password to be used during the current power-on cycle. The password does not persist over a power cycle but does persist over a hardware or software reset. This password is not related to the password used for the Security Mode Feature set. When the password is set the device is in the Set_Max_Unlocked mode.

The SET MAX LOCK command allows the host to disable the SET MAX commands (except SET MAX UNLOCK) until the next power cycle or the issuance and acceptance of the SET MAX UNLOCK command. When this command is accepted the device is in the Set_Max_Locked mode.

The SET MAX UNLOCK command changes the device from the Set_Max_Locked mode to the Set_Max_Unlocked mode.

The SET MAX FREEZE LOCK command allows the host to disable the SET MAX commands (including SET MAX UNLOCK) until the next power cycle. When this command is accepted the device is in the Set_Max_Frozen mode.

4.9.2 BIOS determination of SET MAX security extension status

When the device is locked bit 8 of word 86 of the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data shall be set to one.

4.9.3 BIOS locking SET MAX

To allow for multiple BIOSs to gain access to the protected area the host BIOS should only lock the protected area immediately prior to booting the operating system.

Figure 6 is the SET MAX state diagram.

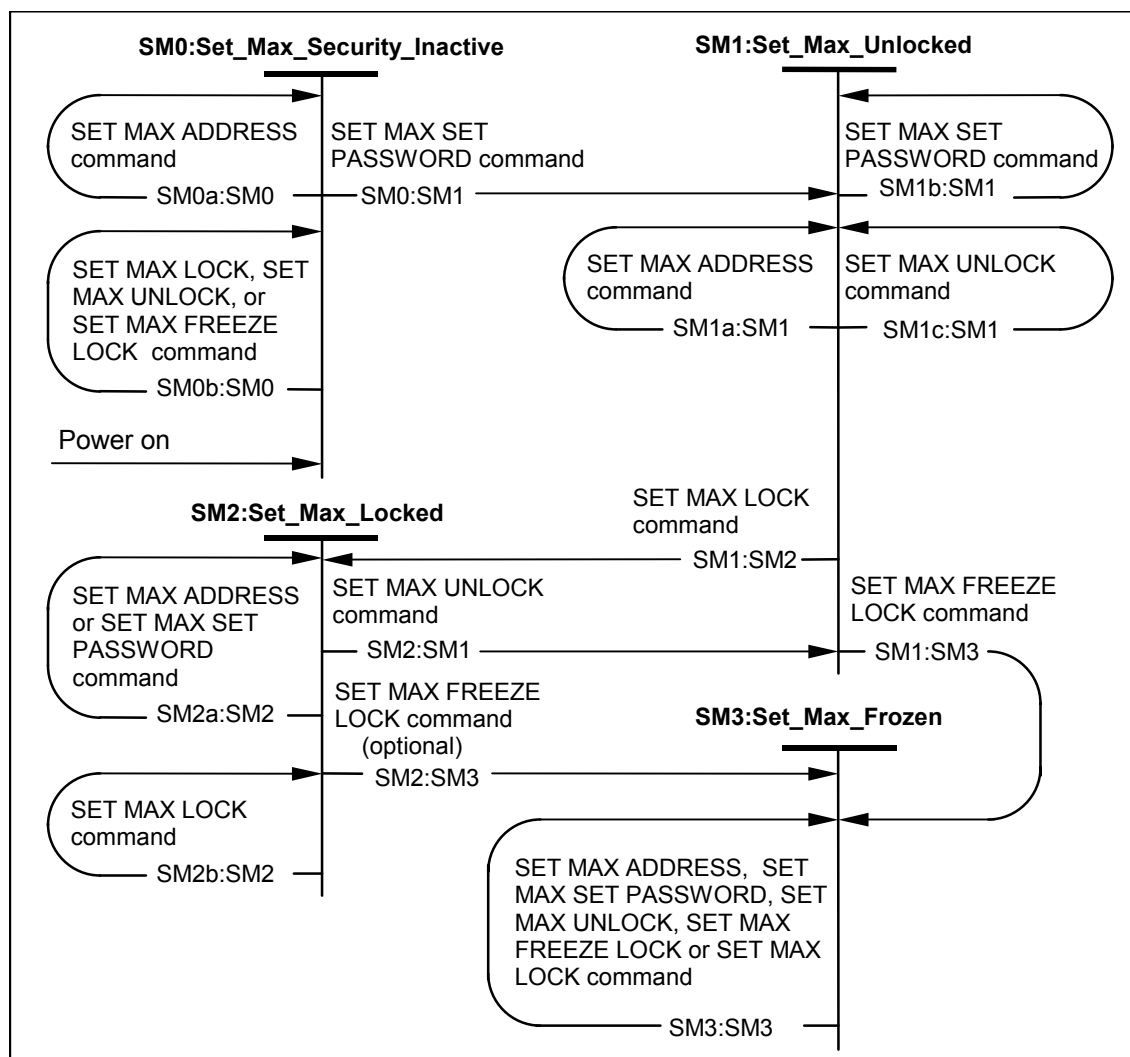


Figure 6 – SET MAX security state diagram

SM0: Set_Max_Security_Inactive: This state shall be entered when the device is powered-on.

When in this state, SET MAX security is disabled.

Transition SM0a:SM0: When a SET MAX ADDRESS command is received, the command shall be executed and the device shall make a transition to the SM0: Set_Max_Security_Inactive state.

Transition SM0b:SM0: When a SET MAX LOCK, SET MAX UNLOCK, or SET MAX FREEZE LOCK command is received, the device shall abort the command and make a transition to the SM0: Set_Max_Security_Inactive state.

Transition SM0:SM1: When a SET MAX SET PASSWORD command is received, the device shall make a transition to the SM1: Set_Max_Unlocked state.

SM1: Set_Max_Unlocked: This state is entered when a SET MAX SET PASSWORD or a SET MAX UNLOCK command is received.

When in this state, a SET MAX security password has been established and the SET MAX security is unlocked. Bit 8 of word 86 of the IDENTIFY DEVICE data shall be set to one.

Transition SM1a:SM1: When a SET MAX ADDRESS command is received, the command shall be executed and the device shall make a transition to the SM1: Set_MAX_Unlocked state.

Transition SM1b:SM1: When a SET MAX SET PASSWORD is received, the password stored by the device shall be changed to the new value and the device shall make a transition to the SM1: Set_MAX_Unlocked state.

Transition SM1c:SM1: When a SET MAX UNLOCK command is received, the command shall not be executed and the device shall make a transition to the SM1: Set_MAX_Unlocked state.

Transition SM1:SM2: When a SET MAX LOCK command is received, the device shall make a transition to the SM2: Set_Max_Locked state.

Transition SM1:SM3: When a SET MAX FREEZE LOCK command is received, the device shall make a transition to the SM3: Set_Max_Frozen state.

SM2: Set_Max_Locked: This state is entered when a SET MAX LOCK command is received.

When in this state, a SET MAX security password has been established and the SET MAX security is locked. Bit 8 of word 86 of the IDENTIFY DEVICE data shall be set to one.

Transition SM2a:SM2: When a SET MAX ADDRESS or SET MAX SET PASSWORD command is received, the command shall be aborted and the device shall make a transition to the SM2: Set_Max_Locked state.

Transition SM2b:SM2: When a SET MAX LOCK command is received, the command shall be executed and the device shall make a transition to the SM2: Set_Max_Locked state.

Transition SM2:SM1: When a SET MAX UNLOCK command is received, the device shall make a transition to the SM1: Set Max Unlocked state.

Transition SM2:SM3: When a SET MAX FREEZE LOCK command is received, the device may make a transition to the SM3: Set_Max_Frozen state. Hosts should not issue the SET MAX FREEZE LOCK command when in this state.

SM3: Set_Max_Frozen: This state is entered when a SET MAX FREEZE LOCK command is received.

In this state, the device may not transition to any other state except by a power cycling. When in this mode bit 8 of word 86 of the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE data shall be set to one.

Transition SM3:SM3: When a SET MAX ADDRESS, SET MAX SET PASSWORD, SET MAX UNLOCK, SET MAX FREEZE LOCK or SET MAX LOCK command is received, the command shall be aborted and the device shall make a transition to the SM3: Set_Max_Frozen state.

4.10 CompactFlash™ Association (CFA) feature set

The optional CompactFlash™ Association (CFA) feature set provides support for solid state memory devices. A device that implements the CFA feature set shall implement the following minimum set of commands:

- CFA REQUEST EXTENDED ERROR CODE
- CFA WRITE SECTORS WITHOUT ERASE
- CFA ERASE SECTORS
- CFA WRITE MULTIPLE WITHOUT ERASE

- CFA TRANSLATE SECTOR
- SET FEATURES Enable/Disable 8-bit transfer

Devices reporting the value 848Ah in IDENTIFY DEVICE data word 0 or devices having bit 2 of IDENTIFY DEVICE data word 83 set to one shall support the CFA feature Set. If the CFA feature set is implemented, all five commands shall be implemented.

Support of DMA commands is optional for devices that support the CFA feature set.

The CFA ERASE SECTORS command preconditions the sector for a subsequent CFA WRITE SECTORS WITHOUT ERASE or CFA WRITE MULTIPLE WITHOUT ERASE command to achieve higher performance during the write operation. The CFA TRANSLATE SECTOR command provides information about a sector such as the number of write cycles performed on that sector and an indication of the sector's erased precondition. The CFA REQUEST EXTENDED ERROR CODE command provides more detailed error information.

Command codes B8h through BFh are reserved for assignment by the CompactFlash™ Association.

4.11 Removable Media Status Notification and Removable Media feature sets

4.11.1 General

This subclause describes two feature sets that secure the media in removable media storage devices using the ATA/ATAPI interface protocols. The Removable Media Status Notification feature set is intended for use in both devices implementing the PACKET Command feature set and those not implementing the PACKET Command feature set. The Removable Media feature set is intended for use only in devices not implementing the PACKET Command feature set. Only one of these feature sets shall be enabled at any time. If the Removable Media Status Notification feature set is in use then the Removable Media feature set is disabled and vice versa.

The reasons for implementing the Removable Media Status Notification feature set or the Removable Media feature set are

- to prevent data loss caused by writing to new media while still referencing the previous media's information,
- to prevent data loss by locking the media until completion of a cached write,
- to prevent removal of the media by unauthorized persons.

4.11.2 Removable Media Status Notification feature set

The Removable Media Status Notification feature set is the preferred feature set for securing the media in removable media storage devices. This feature set uses the SET FEATURES command to enable Removable Media Status Notification. Removable Media Status Notification gives the host system maximum control of the media. The host system determines media status by issuing the GET MEDIA STATUS command and controls the device eject mechanism via the MEDIA EJECT command (for devices not implementing the PACKET Command feature set). While Removable Media Status Notification is enabled devices not implementing the PACKET Command feature set execute MEDIA LOCK and MEDIA UNLOCK commands without changing the media lock state (no-operation). While Removable Media Status Notification is enabled the eject button does not eject the media.

Removable Media Status Notification is persistent through medium removal and insertion and is only disabled via the SET FEATURES command, hardware reset, software reset, the DEVICE RESET command, the EXECUTE DEVICE DIAGNOSTIC command, or power-on reset. Removable Media Status Notification shall be re-enabled after any of the previous reset conditions occur. All media status is reset when Removable Media Status Notification is disabled because a reset condition occurred. Any pending media change or media change request is cleared when the Removable Media Status Notification reset condition occurs.