

CHAPTER 10



Digital Recording Standard

Acronyms 10-v

Chapter 10. Digital Recording Standard 10-1

10.1 General..... 10-1

 10.1.1 Digital Recorder Requirements..... 10-1

 10.1.2 Interface Levels..... 10-3

10.2 Definitions..... 10-3

10.3 Operational Requirements..... 10-3

 10.3.1 Recorder Compliance Requirements 10-3

 10.3.2 Required Configuration 10-5

 10.3.3 Exclusions to Standard..... 10-5

 10.3.4 Internal System Management 10-5

 10.3.5 Data Download 10-5

 10.3.6 Host Platform Interface to Recorder Media..... 10-5

 10.3.7 Required File Table Entries 10-6

 10.3.8 Recorder Setup Configuration File 10-6

 10.3.9 Recorder Data Streaming Transport 10-7

 10.3.10 Commercial Off-the-Shelf Media..... 10-13

10.4 Data Download and Electrical Interface..... 10-13

 10.4.1 Fibre Channel Recorder Download Interface 10-13

 10.4.2 IEEE 1394b Recorder Interface 10-16

 10.4.3 Ethernet Recorder Interface 10-16

10.5 Interface File Structure Definitions 10-17

 10.5.1 Data Organization 10-17

 10.5.2 Directory Definition..... 10-19

 10.5.3 Data Definitions 10-22

10.6 Data Format Definition 10-24

 10.6.1 IRIG 106 Chapter 11..... 10-24

 10.6.2 Time Data Packets 10-26

10.7 Recorder Control 10-27

 10.7.1 Recorder Control and Status 10-27

 10.7.2 Communication Ports..... 10-27

 10.7.3 RS-232/422 Port..... 10-27

 10.7.4 Commands 10-27

 10.7.5 Status Requests 10-27

 10.7.6 Serial Status 10-27

 10.7.7 Default Interface 10-28

| | | |
|-----------------------|---|--------------|
| 10.7.8 | Serial Commands | 10-28 |
| 10.7.9 | Required Discrete Control Functions..... | 10-28 |
| 10.8 | Declassification | 10-28 |
| 10.9 | Host Platform Interface to Recorder Media | 10-28 |
| 10.9.1 | Media Time Synchronization..... | 10-28 |
| 10.9.2 | Physical and Signaling..... | 10-28 |
| 10.9.3 | Removable Media Communication | 10-29 |
| 10.9.4 | RMM High-Level Command Handling..... | 10-32 |
| 10.9.5 | Mandated Connectors | 10-33 |
| 10.9.6 | Real-Time Clock..... | 10-33 |
| 10.9.7 | Mandatory Commands for RMM Devices | 10-34 |
| 10.9.8 | Date and Time Setting Requirements | 10-34 |
| 10.9.9 | Checking Battery Status..... | 10-34 |
| 10.9.10 | Declassification Supporting Commands..... | 10-34 |
| 10.9.11 | SCSI and iSCSI Devices..... | 10-34 |
| 10.9.12 | Using IEEE 1394b | 10-34 |
| 10.9.13 | Using Ethernet | 10-34 |
| 10.10 | Ground-Based Recorders..... | 10-34 |
| 10.10.1 | Interface | 10-35 |
| 10.10.2 | Data Format | 10-35 |
| 10.10.3 | Recording Media..... | 10-35 |
| 10.10.4 | Remote Command and Control | 10-36 |
| 10.10.5 | Data Replay and Reproduction..... | 10-36 |
| 10.11 | Data Interoperability | 10-36 |
| 10.11.1 | Original Recording Files..... | 10-36 |
| 10.11.2 | Modified Recording Files | 10-37 |
| 10.11.3 | Original Recording and Modified Recording File Extension..... | 10-38 |
| 10.11.4 | File Naming | 10-38 |
| 10.11.5 | Data Transfer File | 10-40 |
| 10.11.6 | Recording Directory File | 10-41 |
| Appendix 10-A. | Definitions | A-1 |
| Appendix 10-B. | Sanitization..... | B-1 |
| B.1. | Approach | B-1 |
| B.2. | Algorithm..... | B-1 |
| Appendix 10-C. | Citations | C-1 |



Changes to This Edition of Chapter 10

Numerous changes to Chapter 10 have been made. Highlighting the changes using different font colors, highlights, or other means was not practical and would make reading the document difficult. Therefore, a summary of changes is provided below.

| Paragraph | Description |
|---|--|
| 10.3.9.1 , 10.3.9.1.5 | tsccRR 18 CR-014 – Clarification for sequence numbering |
| | CR88 – |
| | CR89 – |
| | CR91 – |
| | CR94 – |
| | CR95 – |

List of Figures

| | | |
|---------------|--|-------|
| Figure 10-1. | Functional Layout of Digital Recorder Standard..... | 10-2 |
| Figure 10-2. | UDP Transfer Format 1 Header for Non-Segmented Data..... | 10-8 |
| Figure 10-3. | UDP Transfer Format 1 Header for Segmented Data..... | 10-9 |
| Figure 10-4. | UDP Transfer Format 1 (Full Packets)..... | 10-10 |
| Figure 10-5. | UDP Transfer Format 1 (Segmented Packet)..... | 10-10 |
| Figure 10-6. | UDP Transfer Format 2 Header..... | 10-10 |
| Figure 10-7. | UDP Transfer Format 2 (Segmented Packet)..... | 10-11 |
| Figure 10-8. | UDP Transfer Format 3 Header..... | 10-11 |
| Figure 10-9. | Directory Structure..... | 10-18 |
| Figure 10-10. | Directory Block..... | 10-19 |
| Figure 10-11. | File Name Examples..... | 10-24 |
| Figure 10-12. | Data Recording Structure..... | 10-25 |
| Figure 10-13. | Removable Media..... | 10-29 |

List of Tables

| | | |
|--------------|---|-------|
| Table 10-1. | On-Board Recorder Mandatory Compliance Requirements..... | 10-4 |
| Table 10-2. | Ground-Based Recorder Mandatory Compliance Requirements..... | 10-4 |
| Table 10-3. | Source Field Lengths..... | 10-11 |
| Table 10-4. | Offset Field Meanings..... | 10-12 |
| Table 10-5. | Required and Recommended SCSI Commands, Features, and Parameters..... | 10-14 |
| Table 10-6. | Directory Block Format..... | 10-19 |
| Table 10-7. | Data File Entry Format..... | 10-20 |
| Table 10-8. | Prohibited Characters (Hexadecimal Representation)..... | 10-23 |
| Table 10-9. | Required Packets and Locations..... | 10-26 |
| Table 10-10. | Ethernet Service Location Protocol Characteristics..... | 10-30 |

This page intentionally left blank.

Acronyms

| | |
|---------|---|
| BCS | basic character set |
| CCM | command and control mnemonics |
| CDB | command descriptor block |
| CLI | command line interface |
| COTS | Commercial Off-the-Shelf |
| DHCP | Dynamic Host Control Protocol |
| EUI | enterprise-unique identifier |
| FC-PLDA | Fibre Channel Private Loop SCSI Direct Attach |
| FTP | file transfer protocol |
| IAW | in accordance with |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| IQN | iSCSI qualified name |
| IRIG | Inter-Range Instrumentation Group |
| iSCSI | Internet Small Computer Systems Interface |
| ISO | International Organization for Standards |
| ITU-T | International Telecommunications Union/Telecommunication Standardization Sector |
| kb | kilobyte |
| lsb | least significant bit |
| LUN | logical unit number |
| Mbps | megabit per second |
| MHz | megahertz |
| MIL-STD | Military Standard |
| mm | millimeter |
| ms | millisecond |
| msb | most significant bit |
| MTU | maximum transmission unit |
| NADSI | NATO Advanced Data Storage Interface |
| NATO | North Atlantic Treaty Organization |
| ORB | operation request block |
| PoE | Power Over Ethernet |
| ppm | parts per million |
| RCC | Range Commanders Council |
| RFC | Request For Comment |
| RMM | removable memory module |
| RS | Recommended Standard |
| RSCF | recorder setup configuration file |
| RTC | relative time counter |
| SBP | Serial Bus Protocol |
| SCSI | Small Computer Systems Interface |

| | |
|--------|-------------------------------|
| SLP | service location protocol |
| STANAG | Standardization Agreement |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| UO | unexpected one |
| UZ | unexpected zero |

CHAPTER 10

Digital Recording Standard

10.1 General

A large number of unique and proprietary data structures has been developed for specific data recording applications that required unique decoding software programs. The activities of writing unique decoding software, checking the software for accuracy, and decoding the data tapes are extremely time-consuming and costly. In the late 1990s, the test ranges started to see the implementation of non-tape-based, high-data-rate recorders, the most predominant of which were solid-state memory devices. Then, as high-data-rate digital recorders were fielded and as solid-state technology began to emerge, the Telemetry Group saw the need and formed an ad hoc committee for a computer-compatible digital data acquisition and recording standard.

10.1.1 Digital Recorder Requirements

There is a need for a digital data acquisition and recording standard (see the functional layout at [Figure 10-1](#)) that supports a broad range of requirements, including:

- a. Data download and interface
- b. One or more multiplexed data streams
- c. One or more single-data streams
- d. Data format definitions
- e. Recorder control
- f. Media declassification
- g. Data interoperability

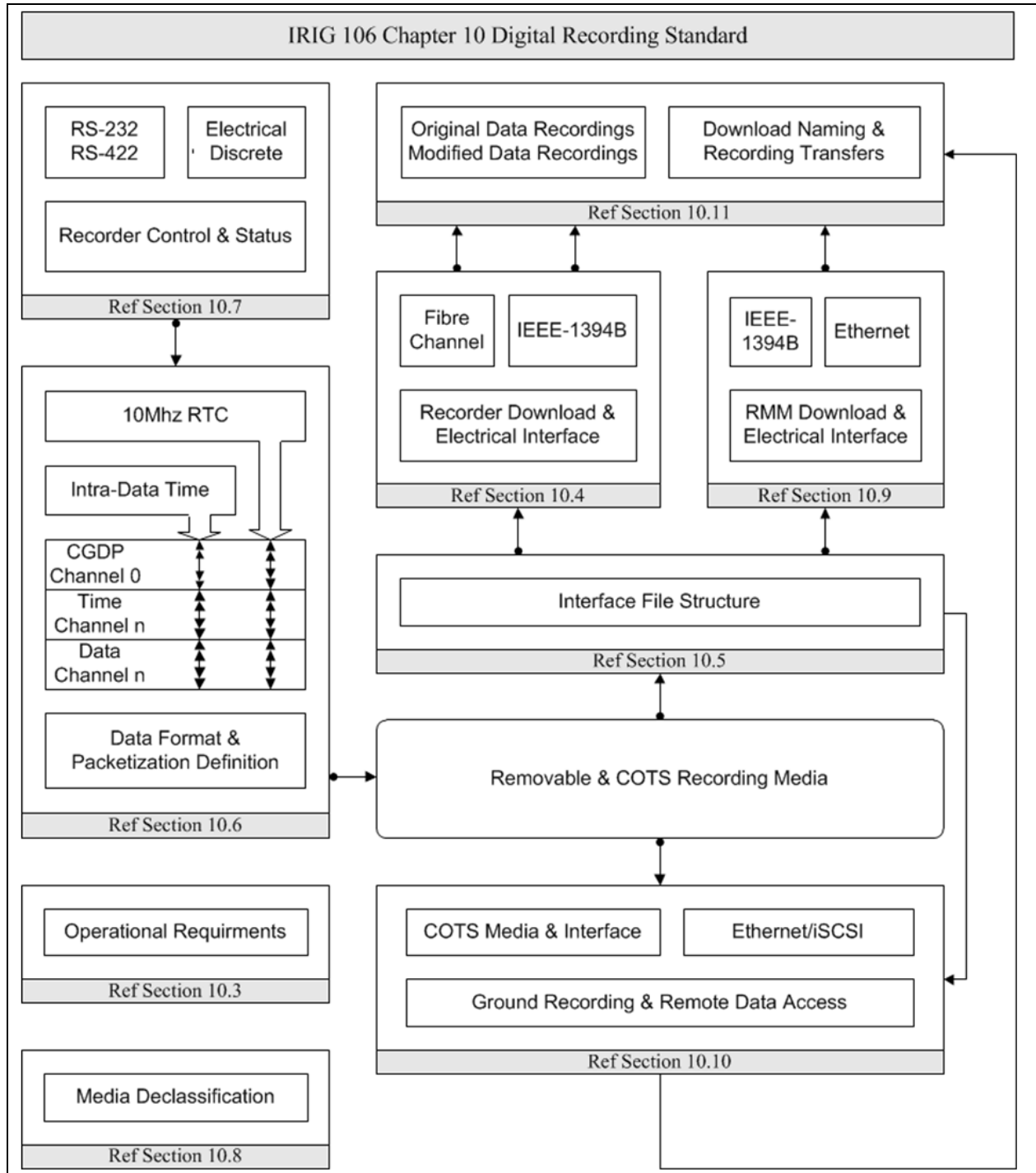



Figure 10-1. Functional Layout of Digital Recorder Standard

Specifically, this digital recording standard shall be compatible with the multiplexing of both synchronous and asynchronous digital inputs such as pulse code modulation and Military Standard (MIL-STD) 1553 data bus, time, analog, video, Aeronautical Radio, Inc. 429, discrete, and Universal Asynchronous Receiver and Transmitter containing Recommended Standard (RS)-232/422/485 communication data. This digital recording standard will allow use of a

common set of playback/data reduction hardware/software to take advantage of emerging random access recording media.

| | |
|---|--|
|  NOTE | Within this standard, where text, figures, or tables are used to provide descriptions, meaning, and/or explanations, the text shall take precedence over figures and tables. |
|---|--|

10.1.2 Interface Levels

The purpose of this chapter is to establish a common interface standard for the implementation of digital data acquisition and recording systems by the organizations participating in the Range Commanders Council (RCC). This standard does not imply hardware architecture such as the coupling of data acquisition, multiplexing, and media storage. The required interface levels are contained in this standard.

- a. Data Download and Electrical Interface, which is the physical interface for data access, is defined in Section [10.4](#).
- b. Interface File Structure, which defines data access structure, is described in Section [10.5](#).
- c. Data Format Definition, which defines data types and packetization requirements, is defined in Section [10.6](#).
- d. Recorder Control and Status, which defines command and control mnemonics (CCM), status, and their interfaces, is described in Section [10.7](#).
- e. Host Platform Interface to Recorder Removable Media is defined in Section [10.9](#).
- f. Ground-Based Recorder Interface, which defines unique interoperability requirements of a ground-based recorder, is described in Section [10.10](#).
- g. Data Interoperability, which defines requirements for the annotation, modification, and exchange of recorded data, is described in Section [10.11](#).

10.2 **Definitions**

As of RCC 106-13 published June 2013, the definitions that in previous versions comprised this section are now located in [Appendix 10-A](#).

10.3 **Operational Requirements**

On-board recorders are the basis and original justification for this standard. This section defines the requirements for on-board recorders to be in 100 percent compliance.

10.3.1 Recorder Compliance Requirements

[Table 10-1](#) and [Table 10-2](#) represent the mandatory recorder requirements to meet 100 percent compliance with this standard. Meeting these compliance requirements guarantees interoperability of recorders, recorder media, and recorded data. Optional functions and/or capabilities are not shown but when implemented in a recorder shall be in accordance with (IAW) the definitions in this standard in order to meet 100 percent compliance of this standard.

| Table 10-1. On-Board Recorder Mandatory Compliance Requirements | |
|--|---|
| Applicable Compliance Section | Function/Capability |
| Recorder Electrical Interfaces | |
| 10.3 , 10.4 | Fibre Channel and/or IEEE 1394b Data Download Port |
| 10.3 , 10.7 | Discrete Lines and/or RS-232 and 422 Full Duplex Communication |
| 10.3 | External Power Port |
| Recorder Download Interface Protocols | |
| 10.4 , 10.9 | Fibre Channel SCSI and/or IEEE 1394b SCSI/SBP-2 |
| Recorder Control/Status Interface Protocols | |
| 10.7 | Discrete Control/Status and/or RS-232 and 422 Control/Status |
| Removable Memory Module (RMM) Electrical Interface and Power | |
| 10.3 , 10.9 | IEEE 1394b Bilingual Socket or Ethernet 8P8c/RJ45 |
| Commercial Off-the-Shelf (COTS) Media Electrical Interfaces | |
| 10.3 | COTS Media Interface |
| RMM Interface Protocols | |
| 10.9 | IEEE 1394b SCSI/SBP-2 or IEEE 802.3 IPv4 |
| COTS Media Interface Protocols | |
| 10.3 | COTS Media Interface |
| Recorder Media/RMM/COTS Media Interface File Structure | |
| 10.5 | Directory, File Structures, and Data Organization |
| 10.3.7 | Directory and File Table Entries |
| Packetization and Data Format | |
| 10.6 | Packet Structures, Generation, Media Commitment, Time Stamping, and Data Type Formats |
| Data Interoperability | |
| 10.11 | Original Recording Files |

| Table 10-2. Ground-Based Recorder Mandatory Compliance Requirements | |
|--|---|
| Applicable Compliance Section | Function/Capability |
| Recorder Electrical Interfaces | |
| 10.10 | Ethernet |
| Recorder Remote Interface Protocols | |
| 10.10 , 10.4 | Internet Small Computer Systems Interface (iSCSI) and/or Telnet |
| COTS Media Electrical Interfaces | |
| 10.10 | COTS Media Interface |
| COTS Media Interface Protocols | |
| 10.10 | COTS Media Interface |
| Remote Data Access Interface File Structure | |
| 10.5 | Directory, File Structures, and Data Organization |

| Table 10-2. Ground-Based Recorder Mandatory Compliance Requirements | |
|--|---|
| Applicable Compliance Section | Function/Capability |
| 10.3.7 | Directory and File Table Entries |
| Packetization and Data Format | |
| 10.6 | Packet Structures, Generation, Media Commitment, Time Stamping, and Data Type Formats |
| Data Interoperability | |
| 10.11 | Original Recording Files |

10.3.2 Required Configuration

An on-board recorder, as a minimum, shall provide the following functionality.

- a. Data download port
- b. Recorder control/maintenance port
- c. External power port

The required data download port interface shall be IAW Section [10.4](#). This combination will allow data extraction and transfer from any recorder to any Section [10.4](#)-compliant intermediate storage unit. The required control port interface shall be IAW Section [10.7](#).

10.3.3 Exclusions to Standard

The physical size, configuration, and form factor for the on-board recorder and the RMM are not controlled by this standard. Due to the variation in capacity/rate/cost requirements of the users, this standard does not specify the technology to be used in the RMM or the on-board recorder.

10.3.4 Internal System Management

Any processing performed on the stored data by the on-board recorder (e.g., for the purposes of internal system management, error detection and correction, physical frame formatting, etc.) shall be removed from the stored data when the stored data is downloaded or transferred from storage media.

10.3.5 Data Download

On-board recorders may have an RMM capability or the on-board recorder can be removed from the acquisition platform and taken to a ground station for data download. Refer to Subsection [10.4.1](#) for recorder download and electrical interface, Section [10.9](#) for RMM interface, and Section [10.11](#) for data transfer and file management.

10.3.6 Host Platform Interface to Recorder Media

Interface to on-board recorder media shall be accomplished utilizing IEEE 1394b or Ethernet interfaces. Interface connectors IAW Subsection [10.9.5](#) shall be provided on the media to allow direct download of data to the host computer or storage device.

10.3.7 Required File Table Entries

Within Section [10.5](#), [Table 10-7](#) File Size, File Create Date, File Create Time, and File Close Time are either optional or can be empty (filled with 0x2D) if data is unavailable. [Table 10-7](#) has been adopted from Standardization Agreement (STANAG) 4575¹ but in the case of Chapter 10 unless Time Type is 0xFF (time data packet) and the time data packet source is 0xF (None) date and time will always be available.

10.3.7.1 File Table Entry Conditions

If [Table 10-6](#) Shutdown value is 0xFF or 0x00 and Time Type is 0xFF and the time data packet source is not 0xF File Size, File Create Date, File Create Time, and File Close Time entries shall be filled in their entirety.

10.3.8 Recorder Setup Configuration File

A recorder setup configuration file (RSCF) can reside on the recorder or optionally reside in the RMM. Recorder setup configuration must be IAW [Chapter 9](#). Recorder setup configurations shall be programmed IAW Section [10.7](#). Optionally the recorder can be configured from a Chapter 10 configuration file residing in the RMM. The RMM RSCF will have priority over setup records residing in the recorder.

10.3.8.1 Recorder Configuration File Location

When a setup record transfer to a recorder is made via the RMM Computer-Generated Data, Format 1 setup record packet(s) will be used. The RMM shall contain a directory and one directory block file entry IAW Subsection [10.5.2](#).

- a. All directory block format fields shall be IAW [Table 10-6](#). The field *n* File Entries value shall be 1.
- b. All directory entry format fields shall be IAW [Table 10-7](#). The field “Time Type” value shall be 0x01, System time. The field “Name” value shall be:

recorder_configuration_file_SAVE_n

This will notify the recorder to use the recorder configuration transfer file for the next recording and store the setup information contained within the file to non-volatile memory in the recorder pre-defined setup location *n*, where *n* is a value of 0-15. This shall be the equivalent of sending .TMATS SAVE [*n*] and .SETUP [*n*] commands.

10.3.8.2 Recorder Configuration File Structure

The RSCF structure will only contain Computer-Generated Data, Format 1 setup record packets. More than one packet is allowed only if the required recorder configuration information exceeds the packet size limits in Subsection [10.6.1](#), thus forcing more than one Computer-Generated Data, Format 1 setup record packet. The standard method of using the sequence counter will be utilized until all the configuration information has been packetized.

¹ North Atlantic Treaty Organization. “NATO Advanced Data Storage Interface (NADSI).” STANAG 4575 (Edition 3). 8 May 2009. Superseded by NATO Standard AEDP-6 Edition B Version 2, published August 2016. Superseding document retrieved 18 April 2019, available at <https://nso.nato.int/nso/nsdd/apdetails.html?APNo=2310>.

10.3.8.3 Configuration of Recorder from RMM

A setup record may reside in the RMM and be utilized for configuration of the recorder. A Computer-Generated Data, Format 1 setup record packet(s) will be used. The RMM shall contain a directory and at least one directory block file entry IAW Subsection [10.5.2](#).

- a. All directory block format fields shall be IAW [Table 10-6](#). The field “*n* File Entries” value shall be 1.
- b. All directory entry format fields shall be IAW [Table 10-7](#). The field “Time Type” value shall be 0x01, System time. The field “Name” value shall be:

recorder_configuration_file_SETUP_RMM

This will notify the recorder to configure from the RMM. The RSCF shall NOT be able to be erased by the recorder .ERASE or DISCRETE command.

10.3.9 Recorder Data Streaming Transport

Data streaming transport may be accomplished across the Section [10.4](#) recorder download and electrical interfaces using the definitions in Section [10.2](#) and commands in [Chapter 6](#). For ground-based recorders, this will be accomplished across the required remote data access Ethernet interface.

The active configuration of the recorder can be detected by means of Chapter 11 Computer-Generated Data Packet, Format 4 Streaming Configuration packets inserted into the reserved channel ID 0x0000.


10.3.9.1 IP Streaming


The network interface, such as Ethernet, can be used for data streaming over Internet Protocol (IP) using either User Datagram Protocol (UDP/IP) or Transmission Control Protocol (TCP/IP). This shall be controlled with the Chapter 6 PUBLISH command.

A network stream is defined, as described in [Chapter 6](#) section 6.2.4.22, as a sequence of packets with a common network source/destination and set of channels. Multiple concurrent network streams may be supported.

When streaming data over IP networks, the Stream Commit Time requirement shall apply to the time at which the data is made available for transmission by the network subsystem.

IP Streaming may use either IPv4 or IPv6.

| | |
|--|---|
|  <p>NOTE</p> | <p>As IP networks are non-deterministic with respect to timing, packets may be delayed, lost, and/or resent, which may result in an unpredictable delay between the packet being made available for transmission and it being received.</p> |
|--|---|

| | |
|--|--|
|  <p>NOTE</p> | <p>The IP protocol supports low-level packet sizes up to 64 kb; however, common IP transports such as Ethernet impose restrictions on the size of the maximum transmission unit (MTU), beyond which fragmentation is required. It is generally desirable to manage streaming data so that fragmentation is avoided. For Ethernet, an MTU of 1500 bytes is common, unless “jumbo frames” are enabled, in which case an MTU of around 9000 bytes is typical.</p> |
|--|--|


An IPv4 datagram is limited to 65,507 bytes, which is significantly less than the maximum size of a Chapter 11 packet. An IPv6 datagram may support “jumbograms” that support payloads larger than the maximum permitted Chapter 11 packet size, but support of this feature is not guaranteed by every IPv6 device. A UDP transfer header shall be used to support all valid Chapter 11 packets and to help protect against undetected data loss.

Three UDP transfer header formats are defined. Format 1 has been supported since IRIG 106-11 and was specifically designed to support streaming data from a recorder to a monitoring station. Format 2 is documented to reflect existing but legacy hardware but is not recommended for use in new applications. Format 3 has been designed to add support for distributed acquisition systems; it supports streaming both to and from the recorder.

Format 3 is recommended for all new designs.

10.3.9.1.1 Ethernet Packet Payload Byte Order

The byte ordering of the streamed packet payload (i.e., the Chapter 11 packets) shall be IAW Subsection [10.5.3.2](#).

| | |
|--|---|
|  <p>NOTE</p> | <p>The IP, TCP and UDP network headers use “big endian” byte ordering, also known as “network byte ordering”.</p> |
|--|---|

The byte order of the UDP/IP transfer header is explicitly defined as part of the definition of the header.

10.3.9.1.2 Format 1, UDP Transfer Header

The structure shown in [Figure 10-2](#) shall be used for Format 1 UDP transfer headers in datagrams containing one or more full Chapter 11 data packets. The UDP transfer header, Format 1 uses “little endian” byte ordering.

| Most Significant Bit (msb) | | | | | | Least Significant Bit (lsb) |
|-----------------------------|---|---|-----------------|---|--------|-----------------------------|
| 31 | 8 | 7 | 4 | 3 | 0 | |
| UDP Message Sequence Number | | | Type of message | | Format | |

Figure 10-2. UDP Transfer Format 1 Header for Non-Segmented Data

The structure in [Figure 10-3](#) shall be used for Format 1 UDP transfer headers in UDP datagrams containing a segmented Chapter 11 data packet.

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------------------|--|--|--|-----|--|---|--|-------------------------|--|---|--|--------|--|--|--|------------|--|--|--|---|--|--|--|--|--|--|--|--|--|--|--|
| msb | | | | lsb | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 31 | | | | 8 | | 7 | | 4 | | 3 | | 0 | | | | | | | | | | | | | | | | | | | |
| UDP Message Sequence Number | | | | | | | | Type of message | | | | Format | | | | | | | | | | | | | | | | | | | |
| 31 | | | | 24 | | | | 23 | | | | 16 | | | | 15 | | | | 0 | | | | | | | | | | | |
| Reserved | | | | | | | | Channel Sequence Number | | | | | | | | Channel ID | | | | | | | | | | | | | | | |
| Word 5 | | | | | | | | | | | | Word 4 | | | | | | | | | | | | | | | | | | | |
| msb | | | | | | | | | | | | | | | | lsb | | | | | | | | | | | | | | | |
| 31 | | | | | | | | | | | | | | | | 0 | | | | | | | | | | | | | | | |
| Segment Offset | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 10-3. UDP Transfer Format 1 Header for Segmented Data

Format (4 bits)

- 0000: Reserved
- 0001: Format 1 (This format)
- 0010: Format 2
- 0011: Format 3
- 0100-1111: Reserved

Type of Message (4 bits)

- 0000: Full packets
- 0001: Segmented
- 0010-1111: Reserved

UDP Message Sequence Number (24 bits). Binary value incrementing by one for each UDP message even if segment of Chapter 10 packet.

Channel ID (16 bits). Segmented packets only, channel ID of the data in the Chapter 10 packet.

Channel Sequence Number (8 bits). Segmented packets only, channel sequence number of the data in the Chapter 10 packet.

Reserved (8 bits). Reserved.

Segment Offset (32 bits). Segmented packets only, position of the data in the Chapter 10 packet.

10.3.9.1.3 Format 1, UDP Chapter 11 Packet Transfer

When more than one complete Chapter 11 packet is contained within a UDP datagram, there shall be an integral number of Chapter 11 packets. The packets shall be sent in the same sequence as the recording segment of a packet and shall be ordered (segment offset incrementing). [Figure 10-4](#) and [Figure 10-5](#) present the sequence of the general UDP network transmission of full or segmented packets.

| |
|-------------------------------|
| UDP/IP Headers |
| UDP Transfer Header, Format 1 |
| Chapter 11 Packet 1 |
| : |
| Chapter 11 Packet N |

Figure 10-4. UDP Transfer Format 1 (Full Packets)

| |
|-------------------------------|
| UDP/IP Headers |
| UDP Transfer Header, Format 1 |
| Chapter 11 Packet Segment |

Figure 10-5. UDP Transfer Format 1 (Segmented Packet)

10.3.9.1.4 Format 2, UDP Transfer Header

The structure shown in [Figure 10-6](#) shall be used for Format 2 UDP transfer headers in datagrams. Format 2 uses “big endian” or network byte ordering for the header:

| | | | | | | | | | | | | | | | |
|-----------------|--|----|--|-------------|-----|----------------|--|--------|--|---|--|---|--|--|--|
| MSW | | | | | LSW | | | | | | | | | | |
| 31 | | 8 | | 7 | | 4 | | 3 | | 0 | | | | | |
| Sequence Number | | | | | | Type | | Format | | | | | | | |
| 31 | | 24 | | 23 | | | | | | 0 | | | | | |
| Segment Offset | | | | Packet Size | | | | | | | | | | | |
| 31 | | | | 16 | | | | 15 | | | | 0 | | | |
| Segment Offset | | | | | | Channel Number | | | | | | | | | |

Figure 10-6. UDP Transfer Format 2 Header

Format (4 bits)

- 0000: Reserved
- 0001: Format 1
- 0010: Format 2 (This format)
- 0011: Format 3
- 0100-1111: Reserved

Type of Message (4 bits)

- 0000: Chapter 11 packet contains a complete Chapter 10 packet
- 0001: Chapter 11 packet contains a partial Chapter 10 packet
- 0010-1111: Reserved

UDP Message Sequence Number (24 bits). Binary value incrementing by one for each Chapter 11 packet.

Channel ID (16 bits). Channel ID of the embedded Chapter 11 packet.

Packet Size (24 bits). Size of the complete Chapter 11 packet in units of 32 bits.

Segment Offset (24 bits). Offset for this data in the Chapter 11 packet in units of 32 bits.

As shown in [Figure 10-7](#), all Chapter 11 packets shall be sent contained within 1 or more UDP datagrams. Each datagram shall contain a payload of 1472 bytes or less. Each datagram shall contain 1 or more whole or partial Chapter 11 packets. A datagram may begin and/or end with a partial Chapter 11 packet, or contain a single partial Chapter 11 packet. A datagram may

contain multiple whole Chapter 11 packets. Every whole or partial Chapter 11 packet contained within a UDP datagram is prefixed with a Version 2 UDP transfer header.

| |
|-------------------------------|
| UDP/IP Headers |
| UDP Transfer Header, Format 2 |
| Chapter 11 Packet Segment N-1 |
| UDP Transfer Header, Format 2 |
| Chapter 11 Packet N |
| UDP Transfer Header, Format 2 |
| Chapter 11 Packet Segment N+1 |

Figure 10-7. UDP Transfer Format 2 (Segmented Packet)

10.3.9.1.5 Format 3, UDP Transfer Header

The structure shown in [Figure 10-8](#) shall be used for Format 3 UDP transfer headers in UDP datagrams. Format 3 uses “little endian” byte ordering for the header:

| | | | | | | | | | |
|------------------------|--|--|--|--|--------------------------|--|--|--|--|
| msb | | | | | lsb | | | | |
| 31 | | | | | 0 | | | | |
| 16 | | | | | 8 | | | | |
| 15 | | | | | 7 | | | | |
| 4 | | | | | 3 | | | | |
| Offset to Packet Start | | | | | Reserved | | | | |
| SrcID Len | | | | | Format | | | | |
| Source ID | | | | | Datagram Sequence Number | | | | |

Figure 10-8. UDP Transfer Format 3 Header

Format (4 bits)

- 0000: Reserved
- 0001: Format 1
- 0010: Format 2
- 0011: Format 3 (This format)
- 0100-1111: Reserved

SrcID Len (4 bits). Number of bits in the Source ID field. Permissible values are 0 to 4, which defines the number of 4-bit “nibbles” to be used with the interpretation shown in [Table 10-3](#).

| Table 10-3. Source Field Lengths | | | |
|---|-------------------------------------|-------------------------------|--|
| “SrcID Len” Value | Length of “Source ID” (bits) | Max. Number of Sources | Length of Datagram Sequence Number (bits) |
| 0 | 0 | 1 | 32 |
| 1 | 4 | 16 | 28 |
| 2 | 8 | 256 | 24 |
| 3 | 12 | 4096 | 20 |
| 4 | 16 | 65536 | 16 |

The purpose of this field is to provide enough information to detect when the datagram sequence number “wraps”; the median value of 2 is recommended as a good compromise between the maximum number of sources on the same network (which is controlled by the length of the “Source ID” field) and resilience against undetected “wrapping”, which requires a large datagram sequence number.

Offset to Packet Start (16 bits). Offset, in bytes, to the start of the first Chapter 11 packet within the datagram. As the Format 3 UDP transfer header is 8 bytes in length, values less than 8 cannot refer to the start of a packet, and instead are used to designate the conditions indicated in [Table 10-4](#).


| Value | Meaning |
|--------------|--|
| 0 | No Chapter 11 packet starts in this datagram (i.e., this is datagram is entirely a partial packet). |
| 1 | The sending device has no information about whether a Chapter 11 packet starts in this datagram. |
| 2 | The datagram size is an IPv6 “jumbogram” larger than 64 kb and no Chapter 11 packet starts in the first 64 kb of the jumbo datagram. |
| 8 – 65,507 | The first byte of the first Chapter 11 packet in this datagram is located at this offset from the start of the datagram. |

The use of the special value “1” is discouraged except in the case of “bridge” or routing devices that have no inherent knowledge of Chapter 11 packet structure.

Source ID (0 to 16 bits, depending on “SrcID Len” field). Value indicating which of a number of devices is generating this packet stream; must be unique on the network. Assignment of this value is not controlled by this standard, and has no inherent meaning other than as an identifier.

Datagram Sequence Number (16 to 32 bits, depending on “SrcID Len” field). This is a monotonically increasing sequence number for each datagram sent for a given network stream. This sequence number will wrap from “all 1s” to 0.



| | |
|--|--|
|  <p>NOTE</p> | <p>The core features of the original Format 1 UDP transfer header can be provided by setting “SrcID Len” to 0 and ignoring the ability to have multiple sources.</p> |
|--|--|

10.3.9.1.6 Format 3, UDP Chapter 11 Packet Transfer

In Format 3, the Chapter 11 packet stream may be packed into as many or as few discrete UDP datagrams as suits the implementation. This facilitates the use of datagrams sized to fit the MTU of the transmission medium (e.g., Ethernet).

10.3.9.2 TCP Data Transfer

When supporting TCP/IP streaming, the recorder can act either as client (i.e., it establishes the connection to the remote device) or a server (i.e., it waits for a connection from the remote device). When acting as a server, the default port for TCP/IP connections is defined to be (decimal) 10620.

Using TCP/IP, Chapter 11 packets are transmitted in the exact same format (byte for byte) as they would be written to local storage media.

The data availability (e.g., the channel selection) can be controlled with the remote control command: `.PUBLISH_TCP` (see [Chapter 6](#)).

When a TCP connection is first established, the first byte transmitted shall be the first byte of a Chapter 11 packet.

10.3.9.3 Non-IP Streaming

Streaming over connections that do not support IP are treated identically to TCP/IP data transfer as described in Subsection [10.3.9.2](#).

[Chapter 7](#) provides a Non-IP Streaming mode for Chapter 11 packets.

10.3.10 Commercial Off-the-Shelf Media

In conjunction with an on-board recorder and/or a multiplexer when an RMM or internal on-board recorder media is not used, COTS media can be used for recording media. The COTS media shall be accessible at a minimum from the on-board recorder data download port IAW Section [10.4](#) and optionally by at least one COTS media interface. When accessing COTS media the interface file structure definition defined in Section [10.5](#) shall be presented at the on-board recorder or COTS media interface.

10.4 Data Download and Electrical Interface

The required recorder download port interface (see Subsection [10.3.2](#)) shall be Fibre Channel, IEEE 1394b, Ethernet (Subsection [10.4.3](#)), or any combination of the three. The physical, signaling, and command protocols contained in subsections [10.4.1](#) and [10.4.2](#) are a subset of, and adapted from STANAG 4575.

10.4.1 Fibre Channel Recorder Download Interface

10.4.1.1 Physical and Signaling

The interface shall comply with Fibre Channel-Physical Interfaces and Fibre Channel-Framing and Signaling in Section [10.9](#), with configuration options as specified.

- a. Physical Media. Fibre Channel copper interface will be utilized.
- b. Signaling Rate. The transmission signaling rate shall be 1.0625 gigabaud.

10.4.1.2 Command Protocol

The interface shall conform to the requirements of the Fibre Channel Private Loop SCSI Direct Attach (FC-PLDA) (American National Standards Institute/International Committee for Information Technology Standards TR19-1998)² interoperability, except as defined herein. Table 17 of FC-PLDA specifies a control protocol using a subset of commands, features, and parameters defined for the Small Computer System Interface (SCSI)-3. Table 17 of FC-PLDA also defines the command feature and parameter usage categories of “Required,” “Allowed,” “Invokable,” and “Prohibited” between the SCSI initiator and target. These definitions assume that the target is a magnetic disk drive or equivalent device.

² International Committee for Information Technology Standards. “Fibre Channel - Private Loop SCSI Direct Attach (FC-PLDA).” INCITS TR-19-1998. January 1998. Retrieved 3 July 2019. Available for purchase at <http://www.techstreet.com/incits/searches/385689>. Replaced by “INCITS Technical Report - for Information Technology - Fibre Channel - Device Attach (FC-DA).” INCITS TR-36-2004. February 2005. Retrieved 3 July 2019. Available for purchase at <http://www.techstreet.com/incits/searches/385707>.

The control protocol must support a number of data storage media types. Only the minimum set of SCSI commands needed to download mission data from a memory cartridge are defined as “Required.” The FC-PLDA SCSI commands, features, and parameters not defined as “Required” for this standard are redefined as “Allowed” so that they may be implemented as appropriate. In addition, it is recognized that numerous applications will be required to write to the RMM as well. Commands required to format and/or write to an RMM are defined as “Recommended.” These commands are not required for any STANAG 4575 RMM implementation; however, if the functions are incorporated into an application, the recommended commands shall be used to preclude a proliferation of unique commands. All other required FC-PLDA SCSI commands, features, and parameters not defined as “Required” or “Recommended” for STANAG 4575 are redefined as “Allowed” such that they may be implemented as appropriate. [Table 10-5](#) provides the five required STANAG 4575 SCSI commands and two recommended commands and their features and parameter usage definitions. The NATO Advanced Data Storage Interface (NADSI)-compliant recorders may respond to the inquiry command with a 00h SCSI version code and the ground/shipboard NADSI host must be prepared to accept this response and restrict SCSI commands issued to the STANAG 4575 mandatory set.

| Table 10-5. Required and Recommended SCSI Commands, Features, and Parameters | | | |
|---|------------------|----------------|--------------|
| Feature (Command) | Initiator | Target* | Notes |
| Inquiry | I | R | |
| Standard INQUIRY data (bytes 0-35) | I | R | |
| Enable Vital Product Data= 1 | I | R | |
| Enable Vital Product Data page codes: | | | |
| 0x00 (supported vital product pages) | I | R | |
| 0x80 (unit serial number page) | I | R | |
| 0x81 (implemented operations definition page) | I | A | |
| 0x82 (Basic Character Set [BCS] implemented operations definition page) | I | A | |
| 0x83 (device identification page) | I | R | |
| Read (10) | I | R | |
| DPO = 0 | I | A | 1 |
| DPO = 1 | I | A | 1 |
| FUA = 0 | I | A | 2 |
| FUA = 1 | I | A | 2 |
| RelAdr= 0 | R | R | |
| RelAdr= 1 | P | P | 3 |
| Read Capacity | I | R | |
| RelAdr= 0 | R | R | |
| RelAdr= 1 | P | P | 3 |
| PMI = 0 | I | R | |
| PMI = 1 | I | A | |
| Test Unit Ready | I | R | |
| Request Sense | I | R | |

| | | | |
|---|---|---|------|
| Write (10) | C | C | 4 |
| DPO = 0 | I | A | 1 |
| DPO = 1 | I | A | 1 |
| FUA = 0 | I | A | 2 |
| FUA = 1 | I | A | 2 |
| RelAdr= 0 | C | C | |
| RelAdr= 1 | P | P | 3 |
| Format Unit | C | C | 4, 5 |
| FMT DATA = 0 | I | A | |
| CMPLST = 0 | I | A | |
| DEFECT LIST FMT= 0 | I | A | |
| INTERLEAVE = 0 | I | A | |
| Notes | | | |
| <ol style="list-style-type: none"> 1. The Disable Page Out (DPO) bit is associated with a device data caching policy. 2. The Force Unit Access (FUA) bit is associated with whether the device may or may not return the requested read data from its local cache. 3. Relative offset is prohibited since this requires the use of linking, which is prohibited. 4. All RMMs not supporting recommended or allowed commands shall respond to these commands with an appropriate error response and shall not cease operations. 5. The FORMAT command shall implement an initialization of the target device such that the entire user memory space shall be writable. After performing this command, the content of the memory may be indeterminate. | | | |
| *LEGEND | | | |
| P Prohibited: The feature shall not be used between NADSI-compliant devices. | | | |
| R Required: The feature or parameter value shall be implemented by NADSI-compliant devices. | | | |
| C Recommended: The feature is recommended and shall be used for applications requiring the functionality of these commands. The initiator determines if a recommended feature/parameter is supported via a required discovery process or a minimal response by the recipient. | | | |
| A Allowed: The feature or parameter may be used between NADSI-compliant devices. The initiator determines if an allowed feature/parameter is supported via a required discovery process or a minimal response by the recipient. | | | |
| I Invokable: The feature or parameter may be used between NADSI-compliant devices. The recipient shall support invokable features or provide a response that it is not implemented as defined by the appropriate standard. | | | |

The RMM shall provide Fibre Channel responder functionality and the NATO ground station shall provide Fibre Channel originator functionality. The RMM shall also provide SCSI target functionality and the NATO ground station shall provide SCSI initiator functionality. When an RMM is powered up directly through the NADSI interface, the RMM shall automatically initialize into a mode where the NADSI port is active and is the priority data and control interface.

10.4.2 IEEE 1394b Recorder Interface


The IEEE 1394b recorder download interface shall use the same mechanisms as Section [10.9](#) where applicable.

10.4.2.1 Physical and Signaling

The interface shall allow control of vendor-specific recorder devices. The command protocol shall be IAW Subsection [10.4.1.2](#) and [Table 10-5](#).

10.4.2.2 Recorder Communication

The fundamental method of communicating shall be IAW the IEEE 1394b protocol.³ Packets sent and received shall be asynchronous transmissions. The IEEE 1394b packets shall encapsulate Serial Bus Protocol (SBP)-2 formatted packets for the transport of commands and data. Recorder devices are to use SCSI command set(s) and therefore SCSI commands and status shall be encapsulated in SBP-2 operation request blocks (ORBs).

| | |
|--|---|
|  <p>NOTE</p> | <p>The SBP-2 provides for the transport of 6-, 10-, and 12-byte SCSI command descriptor blocks (CDBs) within a command ORB.</p> |
|--|---|

10.4.3 Ethernet Recorder Interface

For a recorder containing an Ethernet interface for the data download port, FTP and/or iSCSI protocols shall be used. If FTP will be implemented the requirements set forth in Subsection [10.9.3.4](#) shall be followed. If the iSCSI protocol is to be implemented then the host ground system will act as the *initiator* and the recorder will act as the *target*.

The recorder Ethernet interface shall use the Telnet protocol. As a minimum requirement, the Telnet interface will implement Internet Engineering Task Force (IETF) Request for Comment (RFC) 854⁴, RFC 855⁵, and RFC 1184.⁶ The protocol will support Chapter 6 CCM (Subsection [10.7.8](#)) over a TCP/IP connection on port # 10610. The Telnet interface must respond with a "*" when a connection is made.

10.4.3.1 Target Logical Unit Number Assignments

The following iSCSI target logical unit number (LUN) assignments shall be used.

- a. The LUN 0 or 32 shall be used for recorder data download via Section [10.5](#) interface.
- b. The LUN 1 or 33 shall be used for recorder CCM IAW the requirements for the optional iSCSI recorder control defined within Section [10.7](#).

³ Institute of Electrical and Electronics Engineers. *IEEE Standard for a High Performance Serial Bus: Amendment 2*. IEEE 1394b-2002. New York: Institute of Electrical and Electronics Engineers, 2002.

⁴ Internet Engineering Task Force. "Telnet Protocol Specification." RFC 854. May 1983. Updated by RFC 5198. Retrieved 3 July 2019. Available at <http://tools.ietf.org/html/rfc854>.

⁵ Internet Engineering Task Force. "Telnet Option Specifications." RFC 855. May 1983. May be superseded or amended by update. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc855/>.

⁶ Internet Engineering Task Force. "Telnet Linemode Option." D. Borman, ed. RFC 1184. October 1990. May be superseded or amended by update. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc1184/>.

10.4.3.2 Naming and Addressing

The host ground system (initiator) and recorder (target) devices on the network must be named with a unique identifier and assigned an address for access. The iSCSI initiators and target nodes can either use an iSCSI qualified name (IQN) or an enterprise-unique identifier (EUI). Both types of identifiers confer names that are permanent and globally unique.

Each node has an address consisting of the IP address, the TCP port number, and either the IQN or EUI. The IP address can be assigned by using the same methods commonly employed on networks, such as Dynamic Host Control Protocol (DHCP) or manual configuration.

10.4.3.3 Physical and Signaling


The interface shall allow control of vendor-unique recorder devices. The command protocol shall be IAW Subsection [10.4.1.2](#) and [Table 10-5](#).


10.4.3.4 Recorder Communication

The fundamental method of communicating shall be IAW the iSCSI protocol. Packets sent and received shall be asynchronous transmissions.

10.5 Interface File Structure Definitions

The definitions in this paragraph are a subset of, and were adapted from Section 3 of STANAG 4575. This file structure was selected to facilitate host computing platform independence and commonality. By incorporating an independent file structure, backward and forward compatibility is ensured for the life of the standard.

| | |
|--|---|
|  <p>NOTE</p> | <p>This section duplicates text from STANAG 4575. Any definition in this standard that varies from the STANAG 4575 text is noted in a NOTE box. The text in a NOTE box takes precedence over the text from STANAG 4575.</p> |
|--|---|

| | |
|--|---|
|  <p>NOTE</p> | <p>This file structure definition does not define how data is physically stored on the recorder media but provides a standardized method for access of the stored data at the interface. Data can be organized in any way appropriate to the media, including multiple directories, as long as the file structure IAW Section 10.5 is maintained or seen at the interface (Section 10.4).</p> |
|--|---|

10.5.1 Data Organization

A data recording can contain a single file, which is composed of one or more types of packetized data, or multiple files, in which one or more types of data are recorded simultaneously in separate files. For a recording file to be IAW this standard, it must contain as a minimum the following.

- a. Computer-Generated Packet(s), Format 1 setup record IAW [Chapter 11](#) Subsection 11.2.7.2 as the first packets in the recording
- b. Time data packet(s) IAW [Chapter 11](#) Subsection 11.2.3 as the first dynamic packet after the computer-generated packet, setup record
- c. One or more data format packets IAW Section [10.6](#)

Multiple recordings may reside on the media, and each recording may contain one or more compliant files.

The data hierarchy used to define the data stored according to this standard shall have the following structural relationships (highest to lowest). See [Figure 10-9](#).

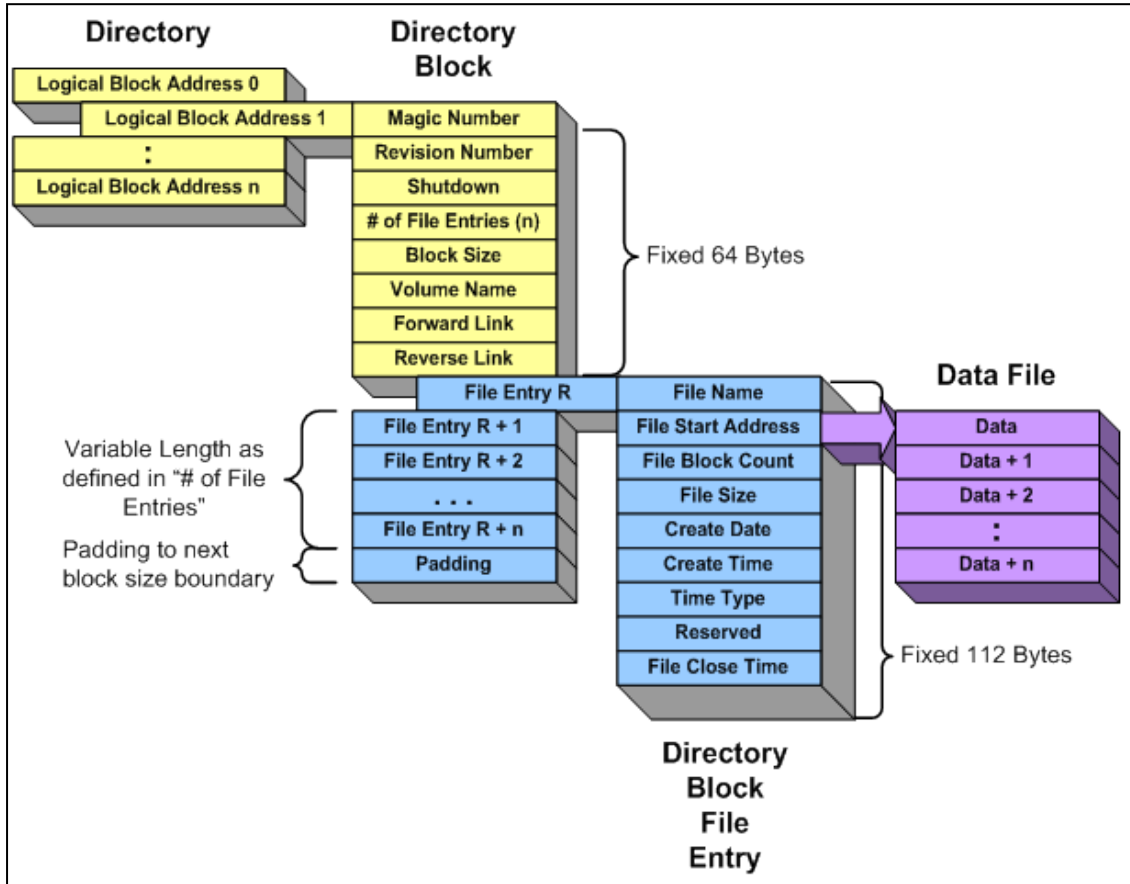


Figure 10-9. Directory Structure

- Directory.** One or more directory blocks of data comprising a list of all data files located under the guidance of this standard. Also contains supporting data that may be of interest to those manipulating the data files. The list of files is made up from “File Entries.” The directory shall always start at logical address zero of each directory block.
- Directory Block.** A memory block containing file entries and other metadata.
- Directory Block File Entry.** A fixed-length data structure used to describe files. It contains the name, the starting address, the number of blocks of data assigned to the data file, the total number of bytes contained in the file, and the file’s creation date and time. It also contains a reserved field for future growth and file close time.
- Data Files.** Data files are comprised of user data, presented at the interface in monotonically increasing contiguous logical addresses per file. Thus if a file starts at logical address X, the next location containing file data must be at the next logical address, X+1, and the next location after that must be at the next logical address, X+2, etc.

10.5.2 Directory Definition

The name and location information for all files recorded in a directory is illustrated in [Figure 10-9](#). The directory is composed of one or more directory blocks as shown in [Figure 10-10](#). At least one directory block is required and it must be located at SCSI logical block address 1. Logical block address 0 is reserved.

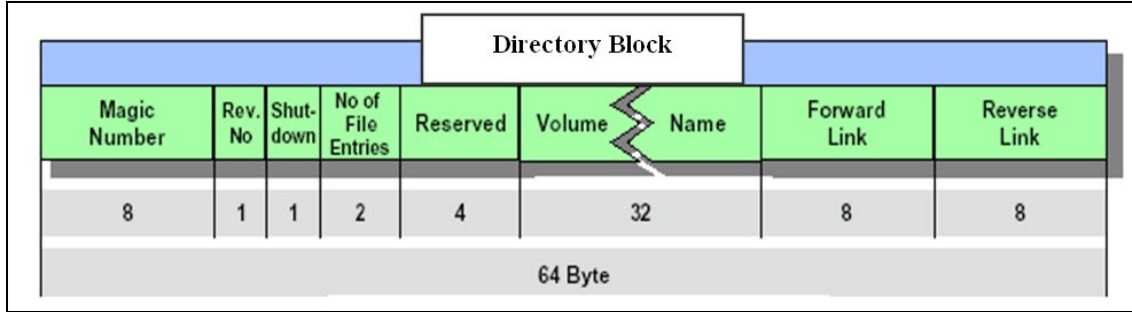


Figure 10-10. Directory Block

- a. Directory Fixed Fields. The fixed fields within a directory block are used to name the volume of data, identify the number of entries, and provide pointers to other addresses that contain additional directory blocks. Forward and backward links to the next address for the next directory block (if any) or the preceding directory block (if any) allow for directory expansion beyond a single block. This does not limit the placement of directory information.
- b. Block Size. The media types used to implement this standard have varying block lengths. Some will have blocks as small as 512 bytes; others may have blocks as large as 64 kb or larger. The block size used by a given media can be determined via the SCSI Read Capacity command (not defined here).
- c. Directory to Data File Link. Each data file on the media has a directory entry within a directory block that describes the file, as shown in [Table 10-6](#). The directory entry for a data file, as shown in [Table 10-7](#), contains a link to the starting location of the data contained in each file and the total number of blocks assigned for the storage of data. This standard does not define the meaning of the data recorded within these data file blocks.

| Table 10-6. Directory Block Format | | | |
|------------------------------------|-------|--|-----------------|
| Field Name | Bytes | Description | Data Type |
| Magic Number | 8 | An identifier for a directory block. This identifier supports discovery of lost directory entries and directory reconstruction after a fault. The value is BCS “FORTYtwo” (0x464F52545974776F) | BCS |
| Revision Number | 1 | Revision number of the standard compiled by the recording system. 0x01 = RCC 106-03 through RCC 106-05 0x0F = RCC 106-07 or later | Unsigned Binary |

Table 10-6. Directory Block Format

| Field Name | Bytes | Description | Data Type |
|--------------------------|-----------------------------------|--|--------------------------------|
| Shutdown | 1 | Flag, if cleared to a 0x00, indicates that the volume was not properly dismounted, and if seen on power-up is an indication that the directory chain may be faulty. If set = 0xFF, then the file system properly shutdown. This field is only valid in the first directory located in logical block 1; other directory blocks set to 0xFF. | Unsigned Binary |
| Number of File Entries | 2 | Defines the number of file entries that follow in this block. | Unsigned Binary |
| Block Size | 4 | Bytes per block size referenced in FileBlkCnt in Table 10-7 . | Unsigned Binary |
| VolName | 32 | Volume name, see character set for restrictions. (Fill any unused VolName byte positions with 0x00.) | BCS |
| Forward Link | 8 | Block address of the next block containing directory information. Set equal to address of this block if this is the end of the chain. | Unsigned Binary |
| Reverse Link | 8 | Block address of the directory block pointing to this block. Set equal to this block address if this is the start of the chain. | Unsigned Binary |
| (<i>n</i> File Entries) | 112 * <i>n</i> | One entry for each file specified in “Number of File Entries.” The maximum value of <i>n</i> is dependent upon media block size. | See Table 10-7 |
| Unused | Varies with <i>n</i> & block size | It is possible for bytes to remain between the last byte of the last-used file entry and the end of the directory block. These bytes are defined as unused and should be filled with 0xFF. | Unsigned Binary |

Note: 64 bytes in fixed fields.

Table 10-7. Data File Entry Format

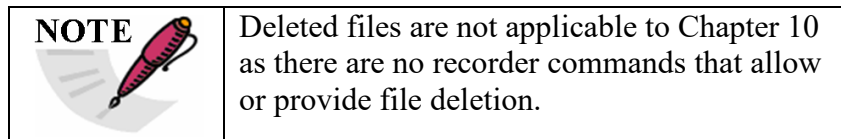
| Field Name | Bytes | Description | Data Type |
|--------------|-------|--|-----------------|
| Name | 56 | File name (see character set for restrictions). Fill any unused File Name byte positions with 0x00. | BCS |
| FileStartAdd | 8 | Zero-based address of the first block reserved for data associated with this file. Fill with 0xFF for unused directory entries. | Unsigned Binary |
| FileBlkCnt | 8 | One-based number that is the count of consecutive address blocks reserved for data for this file including the block pointed to by the FileStartAdd field. | Unsigned Binary |
| FileSize | 8 | The actual number of bytes contained in this file. This file size will be equal to or less than the FileBlkCnt multiplied by the block size. This is an optional entry and will be filled with 0xFF if not used. | Unsigned Binary |

| Table 10-7. Data File Entry Format | | | |
|---|--------------|---|------------------|
| Field Name | Bytes | Description | Data Type |
| File Create Date | 8 | DDMMYYYY BCS character values, with no embedded spaces or other formatting characters, representing the numeric date on which the file was created (e.g., BCS codes for the decimal digits 02092000 → 0x3032303932303030 represents 2 September 2000). Fill with 0x2D if a value for the field is not available, or for portions of the field where data is not available. | BCS |
| File Create Time | 8 | HHMMSSss character values, with no embedded spaces or other formatting characters, representing the numeric time at which the file was created. HH is the number of hours in a 24-hour-based day, MM is the number of minutes after the hour, SS is the number of seconds after the minute, and ss is the hundredths of seconds after the second. Fill with 0x2D if a value for the field is not available, or for portions of the field where data is not available (e.g., “ss” is not available). | BCS |
| Time Type | 1 | A numeric code that qualifies the time and date values recorded in the “Create Date” and “Create Time” and “Close Time” fields. 0x0 = Universal Coordinated Time (Zulu) 0x1 = System Time 0x2 - 0xFE = Reserved 0xFF = Time data packet | Unsigned Binary |
| Reserved | 7 | Bytes in this region are reserved for future growth. Fill with 0xFF. | Unsigned Binary |
| File Close Time | 8 | HHMMSSss character values, with no embedded spaces or other formatting characters, representing the numeric time at which the file was closed. HH is the number of hours in a 24-hour-based day, MM is the number of minutes after the hour, SS is the number of seconds after the minute, and ss is the hundredths of seconds after the second. Fill with 0x2D if a value for the field is not available, or for portions of the field where data is not available (e.g., “ss” is not available). | BCS |

Note: 112 bytes in fixed fields.

- d. File Entry Name. Each file entry in a directory shall have a unique name (see Subsection [10.5.3.4](#)). Default file name is a BCS numeric value incrementally increasing, starting at value “1.”
- e. File Entry Singularity. Multiple file entries are not permitted to refer to the same regions of memory, partially or completely.

- f. Directory Entries and Fields. Directory block fields and entries shall be logically contiguous.
- g. Directory and Memory Region Relationships. File entries shall be entered sequentially into a directory block as files are recorded, starting with file entry #1 in the primary directory block (logical address 1). All file entry positions in the primary directory block shall be filled before the first secondary directory block is used, and so on; however, there is no a priori relationship between the memory region associated with a file entry and the place-order of the file entry within the overall directory. For example, the very first file entry could refer to the very last logical address region of memory, the second file entry could refer to the beginning logical address of memory, and so on. Similarly, there is no presumed temporal ordering of file entries; the very last entry to be inserted could be inserted in such a fashion so as to be the first entry encountered when traversing the directory chain of blocks.
- h. Empty Memory Reads. Reads of regions of memory not containing directory blocks or data file blocks may return unpredictable data values or result in other error conditions.
- i. Contiguous Directory Entries. File entries and all fields in a directory block are contiguous.



- j. Deleted Files. In some applications, previously recorded files may be deleted in order to recover media space for new recordings. Deleted files shall be denoted by marking the corresponding file entry's file block count field with 0x00 indicating "unused." If the file block count has been set to 0x00, then other fields in that file entry are no longer meaningful.
- k. Reserved Field. Reserved fields shall not be used in Chapter 10 implementations and shall be filled with 0xFF. Reserved fields are intended for future Chapter 10 use.
- l. Number of File Entries. The numerical value placed in the "Number of File Entries" field of a directory block shall equal the number of active file entries plus any file entries marked as deleted files within that directory block.

10.5.3 Data Definitions

10.5.3.1 Directory Byte Order

The directory structures described in Section [10.5](#) of this standard are defined to have the following bit and byte orientation. The most significant byte of any multi-byte structure is byte 0. The msb of each byte is bit 0. This ordering is commonly referred to as "Big Endian."

10.5.3.2 Data Format Byte Order

The data format structures (Packet Header, etc.) are defined by [Chapter 11](#) to have the following bit and byte orientation. The least significant byte shall be transmitted first, the lsb of each byte shall be transmitted first, and data is read from the lowest logical address first. This

ordering is commonly referred to as “Little Endian.” The packet data remains in its native byte order format.

10.5.3.3 Character Set

The character set for all character fields is based on ISO/IEC 10646:2012.⁷ The NATO Imagery Interoperability Architecture limits characters to a subset rather than allowing all characters. The subset will be single octets, known as the BCS.

10.5.3.4 Naming Restrictions

The following rules shall be applied when forming names in order to assure the highest degree of interchange among other operating systems.

- a. Characters. Characters from the first 127 common BCS characters (0x00 through 0x7E) may be used in names except for specific prohibited characters.
 - (1) Any BCS character code value smaller than 0x20 is prohibited, except where the 0x00 is used to terminate the name.
 - (2) The other prohibited characters with their hexadecimal representation are defined in [Table 10-8](#).

| Forbidden Characters in Names | Hexadecimal Value | Forbidden Characters in Names | Hexadecimal Value |
|--------------------------------------|--------------------------|--------------------------------------|--------------------------|
| “ | 0x22 | = | 0x3D |
| ‘ | 0x27 | > | 0x3E |
| * | 0x2A | ? | 0x3F |
| / | 0x2F | \ | 0x5C |
| : | 0x3A |] | 0x5D |
| ; | 0x3B | [| 0x5B |
| < | 0x3C | | 0x7C |

- b. Names. Names used for this interface will observe the following rules.
 - (1) Upper and lowercase characters are considered to be different within file names.
 - (2) Leading and trailing spaces are not permitted.
 - (3) Leading periods are not permitted.
 - (4) Names shall fill their field starting with byte 0 per Subsection [10.5.3.1](#) and be terminated with a 0x00. Unused name characters shall be filled with 0x00. Names may utilize the full length of the field, in which case the terminating 0x00 must be omitted. Examples of host-provided and default file names are shown in [Figure 10-11](#).

⁷ ISO/IEC. *Information Technology - Universal Coded Character Set (UCS)*. ISO/IEC 10646:2012. May 2012. Superseded by ISO/IEC 10646:2017. Retrieved 3 July 2019. Available at <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.

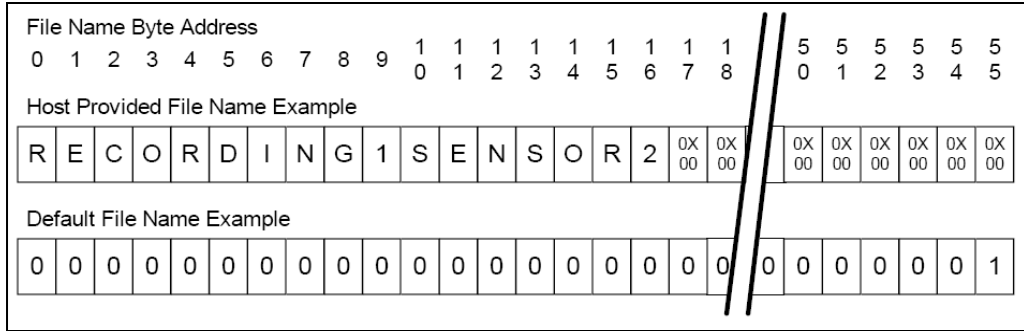


Figure 10-11. File Name Examples

10.6 Data Format Definition

10.6.1 IRIG 106 Chapter 11

Data shall be formatted IAW [Chapter 11](#).

Single or multiple channel recordings will always conform to the structure outlined in [Figure 10-12](#); note that the details of the packet structure are defined by [Chapter 11](#) and are included here for information only.

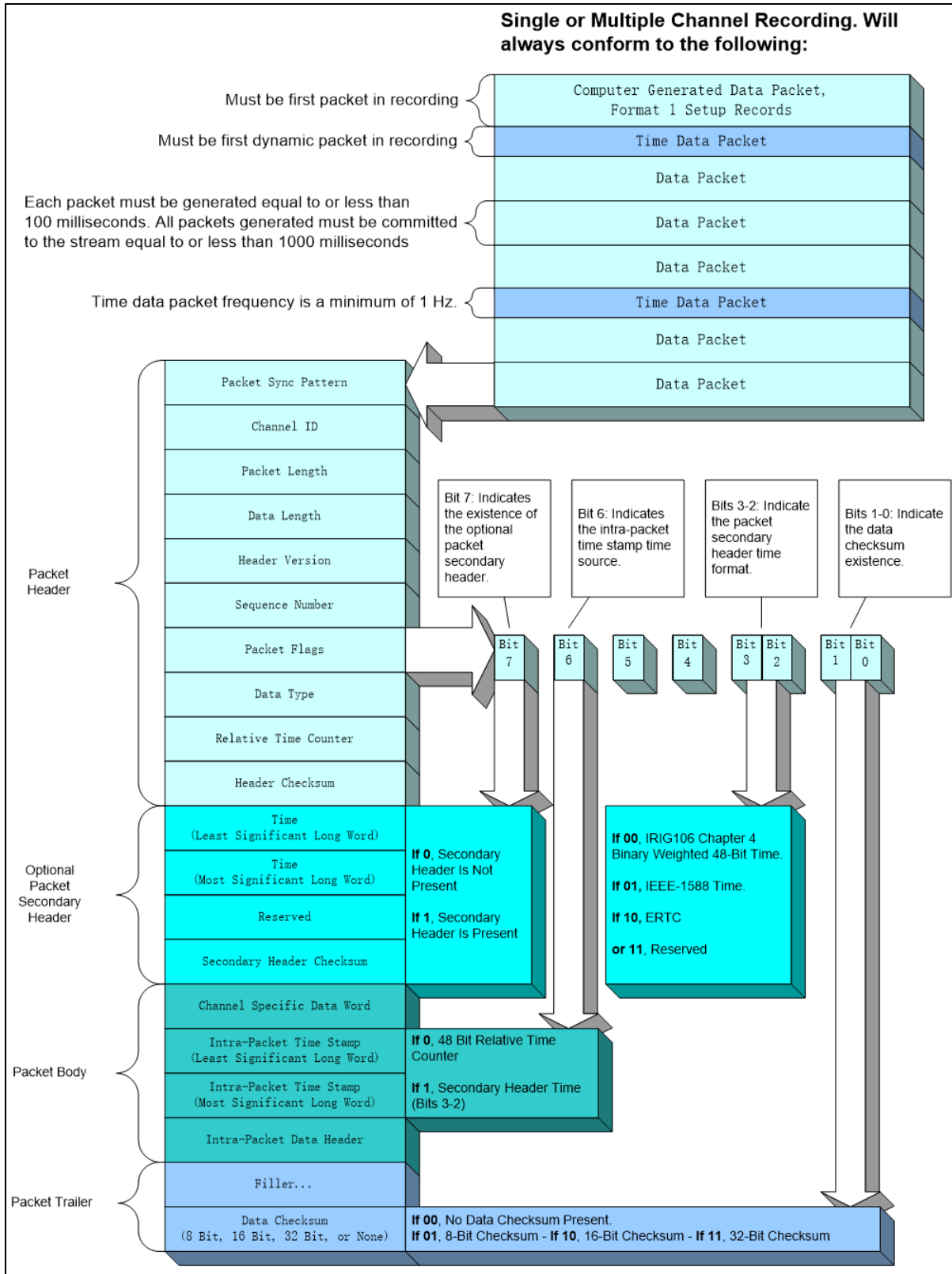


Figure 10-12. Data Recording Structure

a. Certain packets are required by this standard, and areas shown in [Table 10-9](#).

Table 10-9. Required Packets and Locations

| Packet Type | Required | Required Packet Location |
|---|--|--|
| Computer-Generated Data Packet, Format 1 Setup Record | Yes | First packets in recording. A single setup record may span across multiple Computer-Generated Data Packet, Format 1 setup records. |
| Time Data Packet | Yes | First dynamic data packet following setup record packet(s). Refer to the time data packet description for packet rate. |
| All other data type packets with the exception of Computer-Generated Data Packet, Format 1 setup record, time data packets, and Computer-Generated Data Packet, Format 3 recording index (root index) | No | After first time data packet and before the last Computer-Generated Data Packet Format 3, recording index (root index) if enabled. |
| Computer-Generated Data Packet, Format 3 recording index (root index) | Yes, if recording events are enabled. No, if recording events are disabled. | If recording index packets are enabled, root index packet type will be the last packet in a recording. |

- b. With the exception of computer-generated packets, all other packet generation times shall be equal to or less than 100 milliseconds (ms) as measured by the 10-megahertz (MHz) relative time counter (RTC) whenever data is available. This requirement ensures that a packet shall contain equal to or less than 100 ms worth of data, and that a packet containing any data must be generated equal to or less than 100 ms from the time the first data was placed in the packet. This strategy will assure packet granularity and save bandwidth by not forcing or marking empty/idle packets.
- c. With the exception of computer-generated data packets, all other packets shall have a stream commit time equal to or less than 1000 ms as measured by the 10-MHz RTC contained in the packet header.

10.6.2 Time Data Packets

Time is treated like another data channel. If a time source other than None is used (see [Chapter 11](#), Section 11.2.3), the time packet shall be generated at a minimum frequency of 1 hertz.

A time data packet shall be the first dynamic data packet at the start of each recording. Only static Computer-Generated Data, Format 1 packets may precede the first time data packet in the recording. If the time data packet source is “None”, at least one time data packet is required IAW the previous sentence.

10.7 Recorder Control

The recorder shall be controlled by either discrete control/status lines and/or serial communication ports. The serial interface shall consist of both RS-232 and RS-422 full duplex serial communications.

10.7.1 Recorder Control and Status

The RS-232 and RS-422 serial communication ports shall be functional simultaneously without requiring selection of either port. Status requested by either port shall be returned on both ports. Note that unexpected results may occur if commands are issued on both ports simultaneously.

10.7.1.1 Mandatory Recorder Control

The recorder shall provide control by either serial communications ports supporting a command line interface (CLI) IAW [Chapter 6](#) Subsection 6.2 and/or discrete control/status lines IAW Subsection 6.4.

10.7.1.2 Optional Recorder Control

The recorder may be controlled over the Fibre Channel, IEEE 1394b, or Ethernet recorder download interface ports from Section [10.4](#). These interfaces shall support communications using SCSI (Fibre Channel) IAW Subsection [10.4.1](#), SCSI over SBP-2 (IEEE 1394b) IAW Subsection [10.4.2](#), or iSCSI (Ethernet) IAW Subsection [10.4.3](#). Recorder login and Chapter 6 CCM shall be transmitted and received using the SCSI ORB structures IAW subsections [10.9.3](#) (as required for IEEE 1394b), [10.9.4](#), and [10.9.12](#).

10.7.1.3 Optional Telnet Control

The recorder may be controlled over Ethernet/Telnet utilizing CLI as defined in [Chapter 6](#).

10.7.2 Communication Ports

The RS-232 and RS-422 serial communication ports shall be functional simultaneously without requiring selection of either port. Status requested by either port shall be returned on both ports. Note that unexpected results may occur if commands are issued on both ports simultaneously.

10.7.3 RS-232/422 Port

An RS-232/422 port shall be available at the download port.

10.7.4 Commands

Commands received through the serial communication ports shall not override hardware discrete controls.

10.7.5 Status Requests

Status requests received through the serial communication ports shall not interfere with hardware controls.

10.7.6 Serial Status

Serial status shall be provided on either serial status request or discrete activation.

10.7.7 Default Interface

Default interface with user equipment shall utilize the following ASCII serial communication protocol.

- a. 38400 baud
- b. One start bit
- c. 8-bit data
- d. No parity
- e. One stop bit

10.7.8 Serial Commands

The serial ports shall implement a CLI as described in [Chapter 6](#).

10.7.9 Required Discrete Control Functions


Discrete control functions and associated status are described in [Chapter 6](#), Subsection 6.4.

10.8 **Declassification**

As of IRIG 106-17 this section was moved to [Appendix 10-B](#).

10.9 **Host Platform Interface to Recorder Media**

Two interfaces, IEEE 1394b and IEEE 802.3 “Ethernet”, are defined to provide a communication path to read and/or download data from an RMM and to write an RSCF to an RMM. The selection of these protocols was adopted to facilitate a common interface between the media and the computing platform. It is anticipated that any particular RMM will support only one of the two host platform interfaces.

| | |
|---|--|
|  NOTE | This definition does not mandate the interface between the recorder and media. |
|---|--|

10.9.1 Media Time Synchronization

In order to allow recorders to be synchronized to the same time without requiring platform modification or an external time source being provided to the recorder, the removable media cartridges can optionally maintain time, allowing for time initialization of the recorder. Removable media cartridges can optionally provide a battery back-up real-time clock device. Initialization of time can optionally be accomplished via the host platform interface.

10.9.2 Physical and Signaling

Each host platform interface has distinct requirements for the physical interface and signaling levels.

10.9.2.1 IEEE 1394b Interface

The IEEE 1394b host platform interface shall provide data communications and power using the same connector IAW IEEE 1394b.

10.9.2.2 Ethernet Interface

The Ethernet host platform interface shall be IAW the IEEE 802.3 standards. Only a subset of the physical interfaces defined by IEEE 802.3 shall be employed. A power input accepting 8-30 volts direct current and drawing a current of not to exceed 5 amps shall be provided. Additionally, Power Over Ethernet (PoE) IAW IEEE 802.3at-2009⁸ may be used to deliver power to the RMM.

- a. 100Base-TX. For data rates of up to 100 megabits per second (Mbps), 100Base-TX signaling IAW IEEE 802.3 shall be employed.
- b. 1000Base-T. For data rates in excess of 100 Mbps but less than 1000 Mbps, 1000Base-T with auto negotiation to lower speeds as defined in Paragraph a above shall be employed IAW IEEE 802.3.
- c. 10G-Base-T. For data rates in excess of 1000 Mbps, 10GBase-T with auto negotiation to lower speeds as defined in item b above shall be employed IAW IEEE 802.3.

10.9.3 Removable Media Communication

Logically, each compliant RMM shall contain two distinct functional entities as per [Figure 10-13](#). The mechanisms used to communicate with the two functional entities vary according to the host platform interface type.

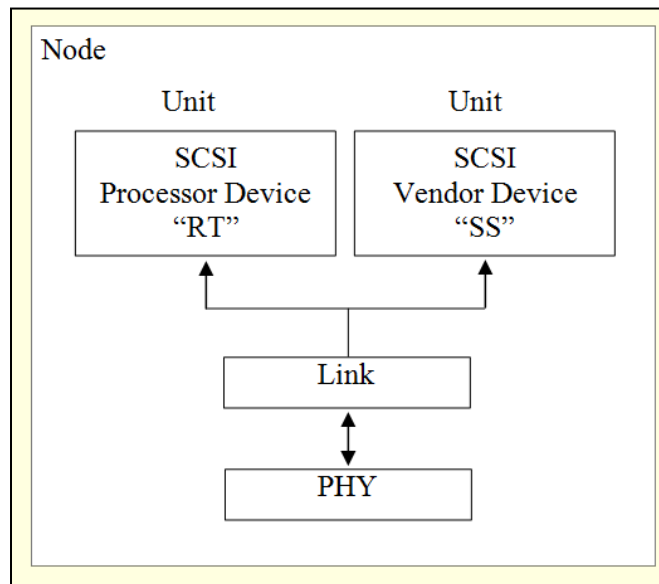



Figure 10-13. Removable Media

10.9.3.1 IEEE 1394b Host Platform Interface

The fundamental method of communicating shall be IAW the IEEE 1394b protocol. Packets sent and received shall be asynchronous transmissions. The IEEE 1394b packets shall encapsulate SBP-2-formatted packets for the transport of commands and data. Removable media

⁸ Institute of Electrical and Electronics Engineers. *IEEE Standard for Information technology - Telecommunications and information exchange between systems...Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements*. IEEE 802.3at-2009. October 2009. Superseded by update. Retrieved 3 July 2019. Available with registration at <http://standards.ieee.org/findstds/standard/802.3at-2009.html>.

devices are to use SCSI command set(s) and therefore SCSI commands and status shall be encapsulated in SBP-2 ORBs.

| | |
|---|---|
|  | <p>NOTE SBP-2 provides for the transport of 6-, 10-, and 12-byte SCSI CDBs within a command ORB.</p> |
|---|---|

10.9.3.2 IEEE 802.3 Ethernet Host Platform Interface

The fundamental method of communicating shall be IAW the IPv4 protocol defined by IETF RFC 791⁹ and subsequent related documents.

- a. MTU (Frame size). Following power on or reset, the RMM shall select an MTU of 1500 bytes.
- b. RMM IP Addressing. Each RMM should attempt to obtain an IP addressing using DHCP IAW IETF RFC 2131¹⁰ with the options as described below. In the event no IP address can be obtained via DHCP, the RMM shall use a static IP. By default, the static IP address shall be set to 10.9.3.2, with a net mask of 255.0.0.0, and a default gateway of 10.9.3.1. The default static IP can be changed by sending a .RMMIP IP address command as defined in [Chapter 6](#) Subsection 6.5.6.3.

When using DHCP to obtain an IP address, the RMM shall send a DHCP vendor class identifier option (code 60) IAW IETF RFC 2131 to the server, and the first 10 characters of the data string sent with the vendor class identifier option shall be the text “RMM:CH10:”, optionally followed by information further identifying the type of RMM.

- c. RMM Discovery. The RMM shall implement a service location protocol (SLP) service agent IAW IETF RFC 2608¹¹ and [Table 10-10](#). The ground station may implement an SLP user agent or any other suitable method (e.g., tight integration with the DHCP server) to determine the IP address assigned to an RMM. The RMM may provide a set of service attributes IAW [Table 10-10](#). The SLP authentication blocks shall not be required.

| Table 10-10. Ethernet Service Location Protocol Characteristics | | | |
|--|-----------|--------|--|
| Characteristic | Provision | Type | Value |
| Service Name | Required | String | service:RMM:IRIG 106: |
| Service Location | Required | String | //nnn.nnn.nnn.nnn[:pppp]representing the IP address of the RMM and optionally the port number (pppp) on which the Telnet service will respond if not port 923 (see Subsection 10.9.4.2) |
| Naming Authority | Optional | String | RCC. If used, the service name shall be service:RMM.RCC:IRIG 106: |

⁹ Internet Engineering Task Force. “Internet Protocol.” RFC 791. September 1981. Updated by RFC 1349, RFC 6864, and RFC 2474. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc791/>.

¹⁰ Internet Engineering Task Force. “Dynamic Host Configuration Protocol.” RFC 2131. March 1997. Updated by RFC 5494, RFC 4361, RFC 6842, and RFC 3396. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc2131/>.

¹¹ Internet Engineering Task Force. “Service Location Protocol, Version 2.” RFC 2608. June 1999. Updated by RFC 3224. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc2608/>.

| Table 10-10. Ethernet Service Location Protocol Characteristics | | | |
|--|-----------|---------|---|
| Characteristic | Provision | Type | Value |
| Attributes | | | |
| Product | Optional | String | Identification of manufacturer, vendor, and/or part number of the RMM |
| SerialNo | Optional | String | Identification of the unique RMM |
| Capacity | Optional | Integer | Size of the RMM in gigabytes, rounded up. |
| Note: If present, the product string, serial number, and capacity attributes shall be used solely to identify a particular RMM, and shall not be used to modify the behavior of the ground system. | | | |

- d. Ping Response. The RMM shall respond to an internet control message protocol echo request IAW RFC 792.¹²
- e. Accessing RMM Storage. In addition to the mandatory control interface via Telnet, the RMM bulk storage device shall support at least one of the following two methods of accessing data, and may support both:
- (1) iSCSI. To facilitate random access, the iSCSI protocol IAW IETF RFC 3270¹³ and the companion RFC 5048¹⁴ may be implemented according to Subsection [10.9.3.3](#).
 - (2) File Transfer Protocol. To facilitate efficient downloading with low overhead, the file transfer protocol (FTP) IAW IETF RFC 959¹⁵ with optional extensions IAW RFC 3659¹⁶ may be implemented according to Subsection [10.9.3.4](#).

10.9.3.3 iSCSI Data Access Method

The RMM shall act as an iSCSI target and a host computing platform shall act as the iSCSI initiator. The RMM shall implement the commands defined by Subsection [10.9.11](#) when sent using iSCSI CDBs.

10.9.3.3.1 iSCSI Session Establishment

The RMM shall support iSCSI features described in this section, sufficient to establish an iSCSI full-feature phase between the ground system and the RMM.

- a. IPsec. IPsec shall not be used.

¹² Internet Engineering Task Force. "Internet Control Message Protocol." RFC 792. September 1981. Updated by RFC 950, RFC 4884, RFC 6633, RFC 6918. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc792/>.

¹³ Internet Engineering Task Force. "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services." RFC 3270. May 2002. Updated by RFC 5462. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc3270/>.

¹⁴ Internet Engineering Task Force. "Internet Small Computer System Interface (iSCSI) Corrections and Clarifications." RFC 5048. October 2007. Updated by RFC 7146, obsoleted by RFC 7143. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc5048/>.


¹⁵ Internet Engineering Task Force. "File Transfer Protocol (FTP)." RFC 959. October 1985. Updated by RFC 7151, RFC 5797, RFC 2773, RFC 2228, RFC 2640, RFC 3659. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc959/>.

¹⁶ Internet Engineering Task Force. "Extensions to FTP." RFC 3659. March 2007. May be superseded or amended by update. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc3659/>.

- b. Login Security. The ground system shall invoke the iSCSI login phase with the *LoginOperationalNegotiation* stage. The *SecurityNegotiation* stage shall not be used.
- c. Target Naming. When an iSCSI target name is required, e.g., as a result of a SendTargets exchange, the RMM shall provide exactly one IQN per supported target. The name shall take the form:

iqn.yyyy-10.org.tssc: RMM:CH10.vvvvvvvv-ssssss

Where *yyyy* is the year corresponding to the applicable version of this standard and *vvvvvvvv-ssssss* is a pair of arbitrary length strings separated with a “-” that identify the manufacturer/vendor and part identifier of the type of RMM and the serial number or other unique identifier of that particular RMM. These strings shall not contain a colon (“:”) symbol.

| | |
|--|--|
|  <p>NOTE</p> | <p>An RMM may support multiple targets. The name format described above shall not be used for any target that does not adhere to this standard, e.g., for non-compliant storage areas.</p> |
|--|--|

- d. Header and Data Digests. Error detection digests shall not be required, but may be supported.
- e. Redirection. The RMM shall not employ redirection via the TargetAddress and TargetPortalGroupTag keys.
- f. Burst and Segment Lengths. The RMM and the ground station shall support the default values per RFC 3720.¹⁷
- g. Other Keys. For features to be negotiated during the login phase not otherwise specified, the RMM and the ground station shall support the default values per RFC 3720.

10.9.3.4 FTP Data Access Method

The RMM shall implement an FTP server, and shall support image (aka binary) data representation and passive mode. Unless changed by means of the .TCPPOPTS command, the RMM shall employ TCP port 921. By default, the RMM shall accept a login username of “IRIG:CH10” with the associated password “RMM:FTP”. The RMM may also support anonymous FTP. If so the RMM shall provide a mechanism to disable this feature.

The RMM FTP server shall respond with an error code 550 and take no action in response to the DELE, MKD, RMD, RNFR, and RNT0 commands.

10.9.4 RMM High-Level Command Handling

Removable devices shall implement high-level Chapter 6 commands in addition to the data transport commands. These high-level commands and the associated responses shall be transported to the RMM depending on the host platform interface in use.

¹⁷ Internet Engineering Task Force. “Internet Small Computer Systems Interface (iSCSI).” RFC 3720. April 2004. Obsolete by RFC 7143. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc3720/>.

10.9.4.1 High-Level Commands for IEEE 1394b Host Platform Interface

When using the IEEE 1394b interface, the SEND and RECEIVE processor device SCSI-2 commands shall be implemented. The Chapter 6 commands and data will be transported using these SCSI commands and the data buffers.

10.9.4.2 High-Level Commands for Ethernet Host Platform Interface

When using the Ethernet interface, the RMM shall support a Telnet server IAW IETF RFC 854 using TCP port 923

10.9.5 Mandated Connectors

Distinct from the recorder/RMM data interface, the removable media shall use the connector mandated for the host platform interface type.

10.9.5.1 IEEE 1394b Interface Connector

The connector type for the removable media shall be an IEEE 1394b bilingual socket connector. Power for the removable media shall be derived from the bilingual interface connector.

10.9.5.2 Ethernet Connector - Data

The connector type for the removable media data connection shall be an 8P8c, commonly known as RJ45, connector. Power may also be supplied using this connector by means of the POE mechanism.

10.9.5.3 Ethernet Connector - Power

The connector type for power when using Ethernet shall be a socket that accepts a barrel plug with a 5.5-millimeter (mm) outside diameter, a 2.5-mm inside diameter, and a shaft length of 9.5 mm. The plug shall be wired center-positive, and the connector shall carry a current of at least 5 amps.

10.9.6 Real-Time Clock

Removable media configured with a real-time clock can optionally allow for time to be preset in the media, allowing for the transfer to the recorder.

10.9.6.1 Minimum Operational Requirements

If an optional real-time clock is implemented, its time setting accuracy shall be better than 1 ms. The short time accuracy of the real-time clock device must be at least 10 parts per million (ppm) in the temperature range 0-40°C, and at least 50 ppm in the temperature range -40°C - +85°C.

10.9.6.2 Accessing time using the IEEE 1394b Host Platform Interface

The SCSI command set shall be utilized to access time on the cartridge.

- a. Real-Time Clock Time Format. If an optional real-time clock is implemented the time format shall be IAW [Chapter 6](#) Subsection 6.2.3.10. The date format shall be IAW ISO 8601:2004.¹⁸

¹⁸ International Organization for Standardization. *Data elements and interchange formats--Information interchange--Representation of dates and times*. ISO 8601:2004. Geneva: International Organization for Standardization, 2004.

- b. Real-Time Clock Logical Unit Number. The standard SCSI media devices are using LUN = 0. The real-time clock shall be assigned LUN = 1.

10.9.6.3 Accessing time using the Ethernet Host Platform Interface

If an optional real-time clock is implemented the cartridge time shall be accessed via the .TIME command including the precision time protocol extensions if supported.

10.9.7 Mandatory Commands for RMM Devices

The required command set for RMM devices is defined by [Chapter 6](#), Section 6.5.

10.9.8 Date and Time Setting Requirements

To support setting the time and date of the real-time clock, the RMM should follow the procedures defined by [Chapter 6](#), Subsection 6.5.2.

10.9.9 Checking Battery Status

Verification of health of battery shall be accomplished with .CRITICAL and .HEALTH commands IAW [Chapter 6](#), Subsection 6.2.3.1 and Subsection 6.2.3.3.

10.9.10 Declassification Supporting Commands

Commands to support sanitization for declassification or other purposes are described in [Chapter 6](#), Subsection 6.5.3.

10.9.11 SCSI and iSCSI Devices


The mandatory SCSI command set is defined in [Chapter 6](#), Subsection 6.5.4.

10.9.12 Using IEEE 1394b

The mandatory ORB formats and related command information is documented in [Chapter 6](#), Subsection 6.5.5.

10.9.13 Using Ethernet

Additional mandatory commands required when using Ethernet are documented in [Chapter 6](#), Subsection 6.5.6.

| | |
|---|--|
|  NOTE | The RMMs using IEEE 1394b, SCSI or iSCSI shall support as a minimum the SCSI command set to support data download IAW Section 10.4 . |
|---|--|

10.10 **Ground-Based Recorders**

This section specifies the basic requirements of ground-based recorders. The main functional requirements of ground-based recorders areas follows.

- a. Recorder Interface
- b. Recorder Data Format
- c. Recorder Media
- d. Recorder Command and Control (if the ground-based recorder is to be controlled remotely)

Optionally, ground-based recorders may support replay, reproduction, and display of Chapter 10 data recordings. Basic replay and reproduction interoperability requirements will be defined in this section. Data display requirements are outside the scope of this standard and will not be defined.

10.10.1 Interface

- a. At a minimum, the required ground-based recorder interface shall be Ethernet for remote command and control IAW Section [10.4](#) and Section [10.7](#).
- b. Optionally, ground-based recorders can implement additional interfaces for remote command and control, remote data access, and/or data streaming. If a ground-based recorder uses iSCSI or contains an RS-232/422, IEEE 1394, and/or Fibre Channel for these interfaces, it shall be IAW Section [10.4](#) and Section [10.7](#).
- c. Data streaming
 - The recorder can optionally have the capability to stream Chapter 10 format data (Subsection [10.10.2](#)) out of its required Ethernet interface IAW Subsection [10.3.9.1](#).
 - Stream commit time as defined in Subsection [10.6.1](#) item [c](#) shall apply to Ethernet interface data streaming.


10.10.2 Data Format


Ground-based recorders shall format, multiplex, and record all data IAW Section [10.6](#).

10.10.3 Recording Media

Ground-based recorders shall record data IAW Subsection [10.10.2](#) to COTS media. The term COTS is defined as any recording media (such as hard disks, solid-state drives, tape, Redundant Array of Independent Disks, and Just a Bunch of Disks) that is ready-made and available for sale to the general public.

The COTS media shall have an electrical interface (such as Parallel Advanced Technology Attachment, Serial Advanced Technology Attachment, IEEE 1394, Universal Serial Bus, SCSI, Ethernet) to the ground-based recorders that is ready-made and available for sale to the general public.

| | |
|--|--|
|  <p>NOTE</p> | <p>If ground-based recorders use COTS media for recording of the Subsection 10.10.2 data format, the recorded data remote data access at a minimum shall be across the required ground-based recorder Ethernet interface using iSCSI IAW Subsection 10.4.3 and Section 10.5.</p> |
|--|--|

| | |
|--|--|
|  <p>NOTE</p> | <p>If ground-based recorders provide remote data access across the ground-based recorder Ethernet interface, the interface file structure described in Section 10.5 at a minimum shall be presented at the interface. This does not dictate which COTS media format or data organization is implemented, but does require that the interface file structure is presented at the recorder Ethernet interface.</p> |
|--|--|

All COTS media used by ground-based recorders shall provide the capability of recording valid Chapter 10 original recording file(s) IAW Section [10.11](#). All Section [10.11](#) data transfer and file management requirements shall apply to ground-based recorders.

10.10.4 Remote Command and Control

- a. Optionally, if a ground-based recorder is controlled remotely, it shall provide command and control IAW Subsection [10.7.8](#) across the Ethernet interface port as defined in Subsection [10.10.1](#).
- b. Ground-based recorders at a minimum are required to use iSCSI or Telnet as the command and control Ethernet transport mechanism as defined in Section [10.4](#) and Section [10.7](#).
- c. Ground-based recorders providing remote command and control capability shall provide the functionality for all commands defined in Subsection [10.7.8](#).
- d. Optionally, if a ground-based recorder contains an RS-232/422/485, IEEE 1394b, and/or Fibre Channel interface as defined in Subsection [10.10.1](#) the recorder will provide command and control IAW Section [10.7](#) and [Chapter 6](#).

10.10.5 Data Replay and Reproduction

10.10.5.1 Channel Mapping

- a. Optionally, if a ground-based recorder provides data playback capability, it shall provide for the logical assignment of recorded channels to physical channels on the ground-based recorders.
- b. Playback will not require movement of cards between slots to make assignments for playback.

10.10.5.2 Recording/Reproduction Data Rates

Optionally, if a ground-based recorder provides a data playback capability, it shall provide information using the [Chapter 6](#) .CRITICAL and .HEALTH commands (Subsection 6.2.3.1 and Subsection 6.2.3.3) if the bandwidth of data to be played back exceeds the aggregate bandwidth of the ground-based recorder.

10.10.5.3 Network Recording Playback

- a. Optionally, if a ground-based recorder provides a data playback capability, it shall provide replay from COTS media (Subsection [10.10.3](#)) to the Ethernet interface. The Ethernet format of the network recording playback will be IAW Subsection [10.3.9](#).
- b. If the network recording playback capability is commanded remotely, ground-based recorders shall support the functionality specified in [Chapter 6](#).

10.11 **Data Interoperability**

10.11.1 Original Recording Files

All files contained within a recorder, RMM, COTS media, or that are a byte-for-byte single file downloaded to a host computing platform in unaltered form shall be considered original recording files and be in full compliance with the data organization in Subsection [10.5.1](#) and data format in Section [10.6](#).

In order to provide a standardized method of annotation for original recording files, the following procedures shall be used to ensure Chapter 10 compliance:

- The Computer-Generated Data, Format 1 setup record shall always contain the required attributes IAW Section [10.11](#).
- The original recording file setup record R-x\RI3 “Original Tape/Storage” attribute value shall be R-x\RI3:Y;

10.11.2 Modified Recording Files

Modified recording files are created from original recording files directly from a recorder, RMM, COTS media, or from original recording files that have been downloaded to a host computing platform. There are several instances of modified recording files-filtered or sanitized data, a subset of channels, a superset of channels, a subset of time, a subset of both channels and time, or a superset of channels and subset of time.

10.11.2.1 Modified Recording File Annotation

In order to provide a standardized method of annotation for modified recording files, the following procedures shall be used to ensure Chapter 10 compliance.

- a. The Computer-Generated Data, Format 1 setup record shall always contain the required attributes IAW Section [10.11](#).
- b. Any time a modification is made to an original recording the R-x\RI3 Original Tape/Storage attribute value shall be changed:

From: R-x\RI3:Y;

To: R-x\RI3:N;

In addition, the R-x\RI6 Date of Modification attribute will be added if not already present, in which case if R-x\RI3 contains a “Y” R-x\RI6 shall be empty. The R-x\RI8 attribute value shall contain the last date and time the modified recording file was created.

- c. If the modified recording file is not a time subset but either a channel subset or both a time and channel subset, then the step b attributes shall be changed as defined. The original channels that are not included in the recording subset file shall have the R-x\CHE-n Channel Enable attribute changed:

From: R-x\CHE-n:T;

To: R-x\CHE-n:F;

A comment attribute R-x\COM will be inserted directly after the changed R-x\CHE-n attribute and shall contain the following:

“original recording change-removed channel-*n*” (where *n* represents the channel ID of the channel that was removed).

- d. If the modified recording file is not a time subset but either a channel superset or both a time subset and channel superset, then the step b attributes shall be changed as defined. In addition, the channels added in the modified recording file shall contain the required attribute IAW Section [10.11](#).

A comment attribute R-x\COM will be inserted directly after the added channel R-x\CHE-n attribute and shall contain the following:

“original recording change-additional channel-*n*” (where *n* represents the channel ID of the channel that was added).

If the modified recording file contains filtered (removed packets or data) or sanitized data (overwrite of data), then the step b attributes shall be changed as defined. Also the channels that contain filtered or sanitized data in the modified recording file shall also contain a comment attribute R-x\COM inserted directly after the channel R-x\CHE-*n* attribute and shall contain the following:

“original recording change-filtered channel-*n*” (where *n* represents the channel ID of the channel that was filtered).

10.11.2.2 Modified Recording File Restructuring

When a modified recording file is created there will be alterations to original packets or possibly structure. Therefore:

- a. All files shall reflect any sequence number, packet length, or checksum changes in the appropriate packet header fields.
- b. If enabled in the original recording, Computer-Generated Data, Format 3 recording index packets shall be recalculated to ensure correct information is contained within the entries as they relate to the newly created modified recording file.

10.11.3 Original Recording and Modified Recording File Extension

Upon data download to a host computing platform, all original and/or modified recording files shall use the file extension *.ch10 (or *.c10 extension for use on systems with a 3-character extension limit). The use of this standard extension will indicate that any original and/or modified recording file on a ground computing or storage platform shall be IAW this section.

10.11.4 File Naming

Upon data download from the recorder or RMM to a host computing platform, all or modified recording files shall use the following structure and naming conventions unless the host computing platform operating system imposes naming length limits. In this case the directory and file names are to be truncated after the last component that completely fits within the name length limit.

10.11.4.1 On-Board Recorder

- a. Data Recording Directory Name. Each directory block from an RMM to be downloaded to a ground computing or storage platform shall use VolName as defined in [Table 10-6](#) as the directory name where the data files will be placed. The directory name shall use lower-case letters.

If the VolName is empty (0x00), a default name or user-defined name shall be used. If used the default name shall be ch10dirnnn, where nnn is the sequential directory block count.

- b. Data File Name. Each data file contained within a directory block on the RMM to be downloaded will be placed in the directory identified in item a above and shall use the following naming convention. The data file name shall use lower-case letters.

“filennnn”; where nnnn is the sequential RMM file count from each directory block file entry (must be 8 alpha-numeric characters).

Example: “file0001,” “file0002,” ...: “file9999.”

If available, File Create Date, File Create Time, and File Close Time from [Table 10-7](#), DDMMYYYY_HHMMSSss_HHMMSSss (8 numeric characters for File Create Date, 8 numeric characters for File Create Time separated by an underscore ASCII character code 0x5F, and 8 numeric characters for File Close Time). No spaces or other non-numeric characters allowed.

Example: 02092004_21302731_21451505.

If the File Create Date, File Create Time, and File Close Time values are not available and are filled with 0x2D, then the system time from the host download platform will be used for File Create Date and File Create Time (DDMMYYYY_HHMMSS). File Close Time will not be used. File Close Time shall be replaced with sys_time.

A structure example follows:

...\VolName\FileName_FileCreateDate_FileCreateTime_FileCloseTime

When VolName not empty example:

...\<VolName>\file0001_02092004_21302731_21451505.ch10

When VolName empty default example:

...\ch10dir001\file0001_02092004_21302731_21451505.ch10

When VolName empty user defined example:

...\<User Defined>\file0001_02092004_21302731_21451505.ch10

When date/time not available (0x2D fill) example:

...\file0001_02092004_213027_sys_time.ch10

The use of this standard recording and file naming convention will indicate that any file on a ground computing or storage platform is IAW this standard.

10.11.4.2 Ground-Based Recorder

- a. Recording Directory Name. Each directory where the data files will be placed shall use the naming convention \ch10dir_DDMMYYYY_nnn; where *n* is the sequential number of Chapter 10 recording directories created on the DDMMYYYY date. The directory name shall use lower-case letters.
- b. Recording File Name. Each data file contained within a directory shall use the following naming convention. The data file name shall use lower-case alpha characters.

“filennnn”; where nnnn is the sequential file count from each recording (must be 8 alpha-numeric characters)

Example: file0001, file0002, ...:file9999

File Create Date, File Create Time, and File Close Time shall use the following naming convention.

DDMMYYYY_HHMMSSss_HHMMSSss (8 numeric characters for File Create Date, 8 numeric characters for File Create Time separated by an underscore ASCII character code 0x5F, and 8 numeric characters for File Close Time). No spaces or other non-numeric characters allowed.

Example: 02092004_21302731_21451505.


A structure example follows.

```
...\ch10dir_02092005_001\file0001_02092005_21302731_21451505.ch10
```

The use of this standard recording and file naming convention will indicate that any file on a ground computing or storage platform is IAW this standard.

10.11.5 Data Transfer File

In order to ensure the highest degree of interoperability for transfer of Chapter 10 recorder or RMM contents or original or modified recording files between organizations, the data transfer file structure shall be used. Essentially, a data transfer file contains all the same information and data that a recorder or RMM would present at the interface albeit within a single binary structure on either tape or random access devices. The data transfer file could also contain original or modified recording files from multiple recordings or dates.

| | |
|--|--|
|  NOTE | Original or modified recording files downloaded to a host computing platform and transferred as a single file shall follow Subsection 10.11.1 and Subsection 10.11.2 . |
|--|--|

10.11.5.1 Data Transfer File Structure Definition

The following describes data transfer file structure and media environments.

- a. Tape Devices. A data transfer file on tape devices is treated essentially the same as a recorder or RMM in that the directory structure and data contents are as defined and organized in this standard. The data transfer file is a single binary file containing a directory structure IAW Section [10.5](#) and a single or multiple Chapter 10 original recording files or modified recording files. Only one data transfer file will be contained on a tape device media. The tape block size shall be 32 kb.
 - Logical address 1 will contain a directory and file structure IAW Subsection [10.5.2](#).
 - The corresponding Chapter 10 original recording files or modified recording files will follow the directory structure in contiguous bytes until the end of the data transfer file. The beginning of each Chapter 10 original or modified recording file in the data transfer file will begin at the byte offset contained in each file entry table file Start Address value.
- b. Random Access Devices. A data transfer file on a random access device is treated essentially the same as a recorder RMM in that the directory structure and data contents are as defined and organized in this standard. The data transfer file is a single binary file containing a directory structure IAW Subsection [10.5.2](#) and a single or multiple Chapter 10 original or modified recording files. Multiple data transfer files can be contained on a random access device.

- The Subsection [10.5.2](#) directory structure within the data transfer file begins at byte 0 and runs contiguously until the last file entry paragraph. The next byte after the last file entry block shall be the first byte in the first data file.
- The corresponding Chapter 10 original or modified recording files will follow the directory structure in contiguous bytes until the end of the data transfer file. The beginning of each Chapter 10 original or modified recording file in the data transfer file will begin at the byte offset contained in each file entry table file Start Address value.

10.11.5.2 Data Transfer File Extension

Upon creation, all Chapter 10-compliant data transfer files not on tape devices shall use the file extension *.tf10 (or *.t10 extension for use on systems with a 3 character extension limit). The use of this standard extension will indicate that any data transfer file on a host computing or storage platform shall be IAW Subsection [10.11.5](#)

10.11.6 Recording Directory File

A recording directory file is a binary file that is a byte-for-byte copy of the RMM or recorder directory structure presented at the interface. This file should represent the contents of an RMM or recorder directory at the time of Chapter 10 data download. The bytes in this file contain the byte-for-byte contents of the RMM's directory blocks in the order the directory blocks are linked, using each block's forward link field.

10.11.6.1 Recording Directory File Extension

Upon creation, all Chapter 10-compliant recording directory files shall use the file extension *.df10 (or *.d10 extension for use on systems with a three-character extension limit). The use of this standard extension will indicate that any recording directory file on a host computing or storage platform shall be IAW Subsection [10.11.6](#).

This page intentionally left blank.

APPENDIX 10-A

Definitions

The following are definitions that are used in this standard and are provided as a means of removing ambiguities within the standard.

Absolute Time: A hypothetical time that either runs at the same rate for all the observers in the universe or the rate of time each observer can be scaled to by multiplying the observer's rate by a constant.

Block: The smallest unit of addressable memory that can be written to, read from, and/or erased.

Bad Block: A block determined to be unreliable for storing user data.

Bad Block Table: A table of bad block entries for a memory board. The data stored in the entry identifies the chip and block number of the bad block. The table entry also contains a flag field. The flag field is used to determine the circumstance in which the bad block was detected. It also provides a flag indicating whether the corresponding bad block has previously been secure erased.

Byte: A contiguous set of 8 bits that are acted on as a unit.

Channel-Specific Data Word: A required word for each data type channel that has data-specific information.

Data Streaming: Streaming of current value data whether it is being recorded or not, and playback streaming of recorded data from a file. Data streaming sends the data to one or more destinations simultaneously (e.g., recording media, recorder data interfaces).

Extended Relative Time Counter: A 1-GHz extension to the existing 10-MHz RTC.

Long Word: A contiguous set of 32 bits that are acted on as a unit.

Mandatory: Defines a mandatory requirement of this standard for full compliance. Mandatory requirements as defined in this standard are based on the use of "shall".

Memory Clear: Rendering stored information unrecoverable unless special utility software or techniques are used.

Memory Sanitization: The removal of information from information system media such that data recovery using known techniques or analysis is prevented. Sanitizing includes the removal of data from the media and verification of the action. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures.

Multiplexer: The entity that includes all the inputs, control interfaces, and functionality required to properly record data.

Non-volatile: Memory media that retains data when power is removed.

Packet: Encapsulates a block of observational and ancillary application data to be recorded.

Packet Generation: The placing of observational and ancillary data into a packet.

Page: Storage unit within the flash memory. A page is the smallest storage unit that can be written.

Playback: See Replay

Reconstruction: The output of a recorder where the timing and data content of the output signal are identical to the timing and data content of the originally recorded signal. This is generally the case where the input signal is captured using digital sampling techniques. Also see Reproduction.

Recorder: Is used where a function or requirement shall apply to both an on-board recorder and a ground-based recorder.

Recording: Is defined as the time interval from first packet generated (which by mandatory requirements is a Computer-Generated Data Packet, Format 1) and committed to the recorder media to the last packet generated and committed to the recorder media. Packet generation time and stream commit time, as defined within the standard, apply.

Removable Memory Module: The element of the on-board recorder that contains the stored data.

Replay: The virtual reconstruction of a recorded signal. This virtually reconstructed signal exists for the purposes of display, presentation, extraction, or retransmission.

Reproduction: The output of a recorder where the electrical characteristics of the output signal are identical to the characteristics of the originally recorded signal. This is generally only achievable when the input signal is captured using analog recording techniques. Also see Reconstruction.

Setup Record: TMATS IAW [Chapter 9](#) annotated in the Computer-Generated Data, Format 0 packet.

Stream: All packets from all enabled channels (including computer-generated data) that are generated until the end of a recording.

Stream Commit Time: The time span in which all generated packets must be committed to a stream.

Word: A contiguous set of 16 bits acted on as a unit.

APPENDIX 10-B

Sanitization

Associated documents such as National Security Agency Manual 9-12,¹⁹ DoD Directive 5200.28,²⁰ and DCID 6/3²¹ historically covered sanitization guidelines/requirements. These documents focused on sanitization of standard disk and other conventional memory technologies. Sanitization is the determination by an authorized official that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure. This standard provides for the minimum set of commands that *may be* utilized to allow for user sanitization of solid-state media residing in an RMM. The solid-state media may consist of COTS solid-state disks or a memory configuration unique to the manufacturer. There are several approaches for sanitization. The responsibility for ensuring that a proper sanitization process has been effectively implemented will reside ultimately with the user/customer/program manager.

B.1. Approach

The following approaches for sanitization are currently recommended. It is believed that the user is the most qualified to determine the sanitization procedures for any program situation. It is the user's responsibility to correctly apply the guidelines to the program in each location to optimize the cost/effect while providing appropriate protection for the data. The guidelines are planned to be available on the Internet at [Defense Link](#).

B.2. Algorithm

The algorithm to erase secure data is described below. During the secure erase procedure, all blocks of memory shall be processed. No block in memory shall be excluded from secure erase processing for any reason.

- a. First Erase. Every memory block on the board is erased. Any erase failures reported by memory chips will result in the corresponding chip/block being declared a bad block. In the event this bad block is not already in the corresponding board's bad block table, a new bad block entry will be appended onto the board's bad block table. Note that this new entry will not have the secure erase flag set.
- b. First Write (0x55). Every memory chip location is recorded with the pattern 0x55. As each location is written, the data is read back to guarantee that all bits were written to the expected pattern. Any write failures reported by the chips or any data errors will result in

¹⁹ National Security Agency. "NSA/CSS Storage Device Declassification Manual." Manual 9-12. 15 December 2014. May be superseded by update. Retrieved 18 April 2019. Available at <https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/storage-device-declassification-manual.pdf>.

²⁰ Department of Defense. "Security Requirements for Automated Information Systems (AIs)." DoDD 5200.28. 21 March 1988. Canceled by DoDI 8500.01. Superseding document retrieved 18 April 2019, available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.

²¹ Director of Central Intelligence. "Protecting Sensitive Compartmented Information Within Information Systems." DCID 6/3. Superseded by ICD 503. Superseding document retrieved 18 April 2019, available at https://www.dni.gov/files/documents/ICD/ICD_503.pdf.

the corresponding chip/block being declared a bad block. In the event this bad block is not already in the corresponding board's bad block table, a new bad block entry will be appended onto the board's bad block table. Note that this new entry will not have the secure erase flag set.

- c. Second Erase. Every memory chip shall be erased. Any erase failures reported by the memory chips will result in the corresponding chip/block being declared a bad block. In the event this bad block is not already in the corresponding board's bad block table, a new bad block entry will be appended onto the board's bad block table. Note that this new entry will not have the secure erase flag set.
- d. Second Write (0xAA). Every memory chip location is recorded with the pattern 0xAA. As each location is written, the data is read back to guarantee that all bits were written to the expected pattern. Any write failures reported by the memory chips or any data errors will result in the corresponding chip/block being declared a bad block. In the event this bad block is not already in the corresponding board's bad block table, a new bad block entry will be appended onto the board's bad block table. Note that this new entry will not have the secure erase flag set.
- e. Third Erase. Every memory location is erased. Any erase failures reported by the memory chips will result in the corresponding chip/block being declared a bad block. In the event this bad block is not already in the corresponding board's bad block table, a new bad block entry will be appended onto the board's bad block table. Note that this new entry will not have the secure erase flag set.
- f. Usable Secure Erased Blocks. All blocks that do not have an entry in the bad block table are now considered to be secure erased.
- g. Unusable Secure Erased Blocks. If a bad block entry contains the flag indicating it has already been secure erased, this block has already been secure erased and requires no further processing, since it is known that this block was skipped during the previous recording.
- h. Unsecure Bad Block Processing. A board's bad block table may contain bad block entries that have not previously been secure erased. If any such entries exist, the following steps are performed on each block.
 - Write Zeros Loop. For each page in the block, a pattern of all zeros is written to the page, and the page is checked to determine if any unexpected ones (UOs) are found. If any UOs are found, the page is re-written to all zeros. This process is repeated up to 16 times. After all allowed re-writes, the board, chip, and block numbers of the block containing any remaining UOs are written to a failed erase table.
 - Write Ones Loop. For each page in the block, the page is erased (to all ones) and checked to determine if any unexpected zeros (UZs) are found. If any UZs are found, another erase command is issued to the block. This process is repeated up to 16 times. After all allowed erase operations, the board, chip, and block numbers of the block containing any remaining UZs are written to the failed erase table.

- i. Failed Erase Table Processing. Any remaining entries in the failed erase table correspond to blocks that cannot be erased. These blocks may still contain user data and therefore are declared to have failed the secure erase.

A count of the number of bad blocks in the failed erase table that have not been secure erased is returned as part of the secure erase results. A non-zero count indicates a secure erase failure of at least one block. A command will allow the user to retrieve the failed erase table. A command will also allow a user to retrieve the data from such blocks and manually determine if these blocks can be designated as “Secure Erased.” In most cases, a single stuck bit will not compromise any user data and the offending block can be manually declared to be secure erased. If the results of manual inspection are indeterminate, the chip containing the failed block must be removed and destroyed, and the secure erase procedure must be repeated.

- j. Secure Erase Completion. When all blocks are secure erased (no entries in the failed erase table), the content of the file is the ASCII string “Secure Erase” repeated over and over.

This page intentionally left blank.

APPENDIX 10-C

Citations

- Department of Defense. "Security Requirements for Automated Information Systems (AIs)." DoDD 5200.28. Canceled by DoDI 8500.01. Superseding document retrieved 18 April 2019, available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.
- Director of Central Intelligence. "Protecting Sensitive Compartmented Information Within Information Systems." DCID 6/3. Superseded by ICD 503. Superseding document retrieved 18 April 2019, available at https://www.dni.gov/files/documents/ICD/ICD_503.pdf.
- Institute of Electrical and Electronics Engineers. *IEEE Standard for a High Performance Serial Bus: Amendment 2*. IEEE 1394b-2002. New York: Institute of Electrical and Electronics Engineers, 2002.
- . *IEEE Standard for Information technology - Telecommunications and information exchange between systems...Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements*. IEEE 802.3at-2009. October 2009. Superseded by update. Retrieved 3 July 2019. Available with registration at <http://standards.ieee.org/findstds/standard/802.3at-2009.html>.
- International Committee for Information Technology Standards. "Fibre Channel - Private Loop SCSI Direct Attach (FC-PLDA)." INCITS TR-19-1998. January 1998. Retrieved 3 July 2019. Available for purchase at <http://www.techstreet.com/incits/searches/385689>. Replaced by "INCITS Technical Report - for Information Technology - Fibre Channel - Device Attach (FC-DA)." INCITS TR-36-2004. February 2005. Retrieved 3 July 2019. Available for purchase at <http://www.techstreet.com/incits/searches/385707>.
- International Organization for Standardization. *Data elements and interchange formats--Information interchange--Representation of dates and times*. ISO 8601:2004. Geneva: International Organization for Standardization, 2004.
- International Organization for Standardization/International Electrotechnical Commission. *Information Technology -Universal Coded Character Set (UCS)*. ISO/IEC 10646:2012. May 2012. Superseded by ISO/IEC 10646:2017. Retrieved 3 July 2019. Available at <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.
- Internet Engineering Task Force. "Dynamic Host Configuration Protocol." RFC 2131. March 1997. Updated by RFC 5494, RFC 4361, RFC 6842, and RFC 3396. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc2131/>.
- . "Extensions to FTP." RFC 3659. March 2007. May be superseded or amended by update. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc3659/>.

- . “File Transfer Protocol (FTP).” RFC 959. October 1985. Updated by RFC 7151, RFC 5797, RFC 2773, RFC 2228, RFC 2640, RFC 3659. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc959/>.
 - . “Internet Control Message Protocol.” RFC 792. September 1981. Updated by RFC 950, RFC 4884, RFC 6633, RFC 6918. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc792/>.
 - . “Internet Protocol.” RFC 791. September 1981. Updated by RFC 1349, RFC 6864, and RFC 2474. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc791/>.
 - . “Internet Small Computer Systems Interface (iSCSI).” RFC 3720. April 2004. Obsoleted by RFC 7143. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc3720/>.
 - . “Internet Small Computer System Interface (iSCSI) Corrections and Clarifications.” RFC 5048. October 2007. Updated by RFC 7146, obsoleted by RFC 7143. Retrieved 3 July 2019. May be superseded or amended by update. Available at <http://datatracker.ietf.org/doc/rfc5048/>.
 - . “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services.” RFC 3270. May 2002. Updated by RFC 5462. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc3270/>.
 - . “Service Location Protocol, Version 2.” RFC 2608. June 1999. Updated by RFC 3224. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc2608/>.
 - . “Telnet Linemode Option.” D. Borman, ed. RFC 1184. October 1990. May be superseded or amended by update. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc1184/>.
 - . “Telnet Option Specifications.” RFC 855. May 1983. May be superseded or amended by update. Retrieved 3 July 2019. Available at <http://datatracker.ietf.org/doc/rfc855/>.
 - . “Telnet Protocol Specification.” RFC 854. May 1983. Updated by RFC 5198. Retrieved 3 July 2019. Available at <http://tools.ietf.org/html/rfc854>.
- National Security Agency. “NSA/CSS Storage Device Declassification Manual.” Manual 9-12. 15 December 2014. May be superseded by update. Retrieved 18 April 2019. Available at <https://www.nsa.gov/Portals/70/documents/resources/everyone/media-destruction/storage-device-declassification-manual.pdf>.
- North Atlantic Treaty Organization. “NATO Advanced Data Storage Interface (NADSI).” STANAG 4575 (Edition 3). 8 May 2009. Superseded by NATO Standard AEDP-6 Edition B Version 2, published August 2016. Superseding document retrieved 18 April 2019, available at <https://nso.nato.int/nso/nsdd/apdetails.html?APNo=2310>.

****** END OF CHAPTER 10 ******