ALLIED ENGINEERING DOCUMENTATION PUBLICATION

AEDP-6
(Edition 1)

NATO INTERNATIONAL STAFF - DEFENCE INVESTMENT DIV.

NATO Advanced Data Storage Interface (NADSI) Implementation Guide

APRIL 2006

NORTH ATLANTIC TREATY ORGANIZATION

NATO STANDARDIZATION AGENCY (NSA)

NATO LETTER OF PROMULGATION

20 April 2006

1. AEDP-6 (Edition 1) - NATO ADVANCED DATA STORAGE INTERFACE (NADSI) IMPLEMENTATION GUIDE - is a NATO UNCLASSIFIED publication.

2. AEDP-6 (Edition1) is effective upon receipt.

for
J. MAJ
Brigradier General, POL(A)
Director, NSA

RECORD OF CHANGES

Change Date	Date entered	Effective Date	By Whom Entered

FOREWARD

1. This Allied Engineering Documentation Publication (AEDP) was prepared by the NATO NADSI Custodial Support Team (CST) in response to user community requests for implementation guidance, related test plan and configuration management plan of STANAG 4575.

2. Questions or comments should be directed to the Custodian for this document.

Custodian, AEDP-6
Maj. Alvin Burse , USAF
DCGS & IBS RDT&E PEM
SAF/AQIZ
1060 Air Force Pentagon
Washington DC 20330-1060
United States
Phone: 703-588-6414
Fax:: 703-696-4337
E-Mail: Alvin.Burse@pentagon.af.mil

TABLE OF CONTENTS

ALLIED ENGINEERING DOCUMENTATION PUBLICATION (AEDP-6)
NATO ADVANCED DATA STORAGE INTERFACE (STANAG 4575)
IMPLEMENTATION GUIDE

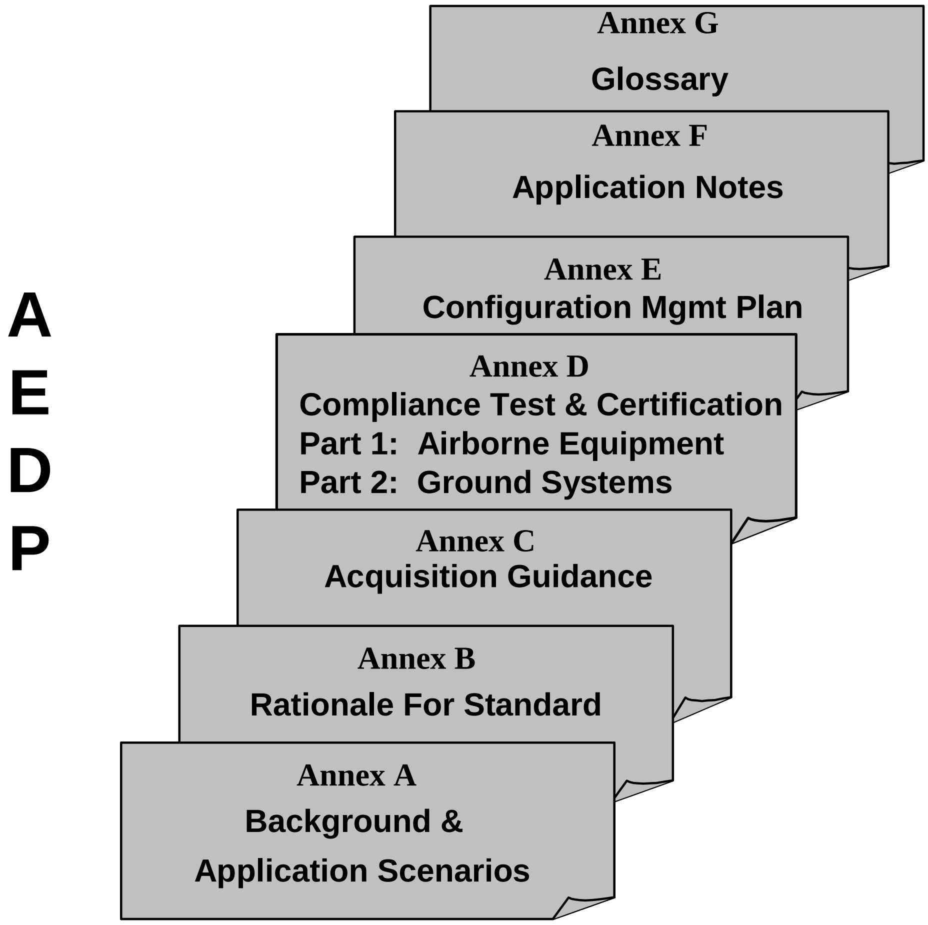
1. NADSI Objectives. The primary objective of the NATO Advanced Data Storage Interface (NADSI) standard (STANAG 4575) is to define a data transfer interface for a Removable Memory Module (RMM), which will download any data to any NATO ground station, within a set of defined constraints.

2. NADSI Philosophy. Conformance with the NADS Interface requirements will allow any compliant ground station to download data from any NADSI compliant data storage removable memory module. Individual files, file segments or the full contents of the memory module can be downloaded using sequences of SCSI Read commands. The NADSI standard relies on existing commercial standards and definitions whenever possible. A straightforward directory and file structure is used, that is specific to the NADSI interface but was created using common techniques.

The NATO NADSI working group defined an interface to allow download and transfer of information at high transfer rates and with a low error rate. Multiple industry and government organizations participated in this development. Since multiple data storage technologies and techniques can be used for the storage media, the interface has been defined to allow all media to be read via this protocol. This allows for wide variation in the implementation of the standard.

3. AEDP SCOPE. This document provides the technical information that was developed during the production of the STANAG. This information was identified as important to the acquisition communities of the member Nations, but inappropriate for the STANAG. This information is divided into seven discrete sections, each provided in the Annexes to this AEDP as shown in Figure-1.

Annex A explains the NADSI background and application scenarios. Annex B provides the rationale for the selection of the elements of the interface. Since most aspects of the interface were chosen after considerable discussion, it was appropriate to document that discussion and include it for future reference. Annex C provides specific guidance to the acquisition communities in the form of recommendations for specifications for the airborne recorder and ground NADS Interface of a reconnaissance or surveillance system. Many of the parameters are important to the operation of the recorder, but do not affect the interface. Annex D includes the Compliance Test and Certification procedures for verifying that a product meets the standard. This Annex has two parts: part one providing the certification information for the airborne equipment, and part two for the ground systems. Annex E includes the configuration management plan for managing the STANAG and this documentation. Annex F provides application notes for advanced memory systems. Finally, Annex G is a global glossary for the entire AEDP.


A
E
D
P
Annex G
Glossary
Annex F
Application Notes
Annex E
Configuration Mgmt Plan
Annex D
Compliance Test & Certification
Part 1: Airborne Equipment
Part 2: Ground Systems
Annex C
Acquisition Guidance
Annex B
Rationale For Standard
Annex A
Background &
Application Scenarios

4. Applicable or Referenced Documents:

AEDP-2	NATO ISR Interoperability Architecture (NIIA)
AEDP-3	Declassification/Sanitization Procedures
ANSI/NCITS TR19-1998	Fibre Channel - Private Loop SCSI Direct Attach (FC-PLDA)
ANSI/NCITS 352-2002	Information Technology - Fibre Channel Physical Interfaces (FC-PI)
ANSI/NCITS 373-2003	Information Technology - Fibre Channel Framing and Signaling Interfaces (FC-FS)
ANSI/NCITS X3.301-1997	Information Technology - SCSI-3 Primary Commands (SPC)
ANSI/NCITS 306-1998	Information Technology - SCSI-3 Block Commands (SBC)
ANSI X3.270-1996	SCSI-III Architecture Model
ANSI X3.272-1996	Information Technology - Fibre Channel Arbitrated Loop (FC-AL)
ANSI X3.269-1996	Information Technology - Fibre Channel Protocol for SCSI (FCP)
FED-STD-595	Colors Used in Government Procurement
DOD 5220.22-M	National Industrial Security Program Operating Manual
EIA/RS-422	Electronic Industries Association RS for serial transmissions
IEC 61000-4-2	Testing and measurement techniques for Electrostatic Discharge immunity test
ISO/IEC 4873	Information technology - ISO 8-bit code for information interchange – Structure and rules for implementation
ISO/IEC 7498-1	Information Technology – Open System Interconnection – Basic Reference Model.
ISO/IEC 10641	Information technology - Computer graphics and image processing - Conformance testing of implementations of graphic standards
ISO/IEC 10646-1-1993	Information Technology - Universal Multiple-Octet Amd 2: 1996 Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane - Amendment 2: UCS Transformation Format 8 (UTF-8)
ISO 9001	Quality Assurance in Design, Development, Production Installation and Servicing
MIL-DTL-24308E	Connectors, electrical, rectangular, non-environmental, miniature, polarized shell, rack and panel, general specification for
MIL-DTL-38999	Connectors, electrical, circular, miniature, high density, quick disconnect (bayonet, thread, and breech coupling), environmental resistant, removable crimp and hermetic solder contacts, general specification for.
MIL-STD-130	Identification Marking of U.S. Military Property
MIL-HDBK-217F	Reliability Prediction of Electronic Equipment
MIL-HDBK-454	Standard General Requirements for Electronic Equipment
MIL-HDBK-740	Airborne and Structureborne Noise Measurement and Acceptance of Shipboard Equipment
MIL-HDBK-5400	Electronic Equipment, Airborne, General Guidelines
MIL-STD-461	Requirements for the Control of Electromagnetic Interference
MIL-STD-704	Aircraft Electrical Power Characteristics
MIL-STD-810	Environmental Engineering Considerations and Laboratory Tests
MIL-STD-882	System Safety
MIL-STD-1472	Human Engineering
MIL-STD-1553	Digital Time Division Command/Response Multiplex Data Bus
STANAG 4250	NATO Reference Model for Open Systems Interconnection
STANAG 4545	NATO Secondary Imagery Format
STANAG 4559	NATO Standard Imagery Library Interface
STANAG 4575	NATO Advanced Data Storage Interface
STANAG 4607	Ground Moving Target Indication
STANAG 4609	NATO Digital Motion Imagery Standard
STANAG 7023	Air Reconnaissance Imagery Data Architecture
STANAG 7024	Imagery Air Reconnaissance Cassette Tape Recorder Standard
STANAG 7085	Interoperable Data Links For Imaging Systems

BACKGROUND AND APPLICATION SCENARIOS

1. Background.

As ISR systems transitioned to digital sensors, the existing Standardization Agreements, based on film cameras, no longer defined the necessary interfaces to achieve interoperability. NATO Air Force Armaments Group (NAFAG), Air Group IV undertook a study to develop the NATO ISR Interoperability Architecture (NIIA), which defined the key electronic and physical interfaces needed to achieve interoperability between the forces of the respective nations. This architecture defined the interface between the airborne and ground elements as one element requiring standardization. The standards were developed based on the technologies available at the time. The interface consists of the imagery format, like STANAG 7023 or STANAG 4545, and either a wideband data link (STANAG 7085) and/or wideband digital tape recorder (STANAG 7024). The other key interface defined was the output of the ground station, providing standards for the textual report formats, annotated imagery, and imagery library interface.

As technologies have continued to advance, solid-state memories and hard disk drives became viable as airborne, non-volatile, mass memory systems. The format defined by STANAG 7024 for the tape recorders provided interchange in the form of the removable tape cartridge, but this is not applicable to some newer forms of ISR data storage. Further, as technology continues to advance, other forms of mass storage, including optical disk, optical tape, and holographic techniques, will be developed. Although some may lend themselves to interchange of only the media, there will still be a basic requirement to have interoperability at a higher level. A Removable Memory Module (RMM) of the airborne recorder can be removed from the platform and attached to a ground station to allow download of the ISR data. The interface defined in this STANAG provides a common connection that can be used with this RMM for most technologies.

2. Application Scenarios.

2.1 Levels of Interoperability. In the NATO ISR Interoperability Architecture (NIIA) document AEDP 2, NATO defines four levels or Degrees of interoperability. They are:

1. Degree 1: Unstructured Data Exchange. Involves the exchange of human interpretable unstructured data such as the free text found in operational estimates, analysis and papers.
2. Degree 2: Structured Data Exchange. Involves the exchange of human interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt and/or message dispatch.
3. Degree 3: Seamless Sharing of Data. Involves the automated sharing of data amongst systems based on a common exchange model.
4. Degree 4: Seamless Sharing of Information. An extension of degree 3 to the universal interpretation of information through data processing based on cooperating applications.

It should be noted that the objective of the NIIA is to achieve interoperability at Degree 2, with some specific interfaces achieving Degree 3. Degree 4 can be considered a long-term objective, but it was determined that lower degrees of interoperability should not be delayed in favor of ultimately achieving a higher degree. Degree 2 interoperability is a significant accomplishment, and will provide a high level of capability to NATO and coalition forces. Higher degrees of interoperability will be addressed once Degree 2 is achieved and demonstrated.

2.1.1 Levels of Interoperability for Memory Systems. In evaluating the interface definitions possible with advanced memory systems, three levels of interoperability were identified. All relate to degree two above, and include operational implications. The highest level of interoperability provides complete cross servicing of the ISR aircraft. That implies that all RMMs have the same form factor (size and shape), and be connected to the recorder in exactly the same fashion using identical interfaces. A unit servicing an aircraft of a different nation would be able to remove the RMM and replace it with a new, completely initialized module so that the aircraft could return to its mission. The used RMM could then be transferred to a ground station for complete exploitation. The middle level of interoperability would provide for only access to the data in an intelligent fashion. When the RMM is removed from the aircraft, it could be connected directly to the ground station and the ISR data could be accessed for download or exploitation within normal reporting timelines. For example, if a file was saved within the RMM that included all of the event marks recorded during a mission, it could be identifiable. This could enable priority targets in these files to be examined first. The lowest level of interoperability would provide only a mass dump of the data. Depending on the amount of data collected during the mission and the transfer capabilities of the ground station, a mass dump of the data could be a lengthy and time consuming process. Only after downloading all of the mission data could the ground station interpret the data and identify where files are located, which files contain which information, and how the data should be exploited.

2.1.2 STANAG Exclusions. It should be noted that this STANAG does not include all elements of a complete interface to exchange and exploit data. The higher levels of the complete interface, including the format of the stored user data, must be defined in other Agreements (for example, STANAGs 4545 or 7023 for imagery).

2.2 Preferred Approach. In discussions with both operational and developmental personnel, the middle level interoperability option was selected as the preferred approach for the memory system.

The highest level of interoperability requires that the interface between the RMM and the recorder be precisely defined. This implies that the architecture of all recorders be identical as well. Given that many manufacturers have already developed products and some are already in the field, it would be impossible to require all to adhere to an arbitrarily selected architecture and physical constraints. Further, in some cases, the developers of the ISR systems require that the recorders have some unique attributes and trade-offs in the design, due to needed memory capacity, data rate, environmental hardening, or a designated size or space for the recorder. If we define a specific form factor for the RMM, then the ISR system developers would be very limited in their ability to fit the recorder to the requirements.

The lowest level of interoperability does provide for complete interchange of the data. However, in order to achieve that interchange, precious time is lost performing the mass dump of the data and possibly much more definition would be required of the ground station capabilities. Requiring the complete transfer of the data into the ground station prior to exploitation would not provide the required data exploitation capability within the time constraints imposed by typical operational requirements.

2.3 File Interpretation. As files are written to the Advanced Data Storage System (ADSS), the directory of the files will be retained in the RMM and can be read through the interface defined by this document. This makes it possible for the ground station to find and recover discrete files. It should be noted, however, that it is not intended that the memory system will have "knowledge" of the information stored in it. This is analogous to a tape recorder being able to play back data from specific portions of the tape based on track set ID, but the recorder doesn't know if the data is directories, infrared, radar, or voice. The ground station will be required to identify the content of the memory and to read from the RMM to download the appropriate portion of the data. The ground station must also be able to interpret the contents of the files.

2.4 Operational Scenarios. It is recognized that the optimal use of advanced ISR data storage technologies will only be achieved when the media is replayed in a unit specifically designed for that purpose, such as in its companion ground station. In most cases, the ground station defined for operational use with a particular sensor system will include a playback unit designed for the RMMs used in the aircraft. For example, a ISR system using a solid-state recorder in the aircraft will likely provide a playback unit compatible with the solid state RMMs in the appropriate ground station. This will allow complete use of the memory system's capabilities. However, there are numerous occasions when the RMMs may be provided to a different ground station for exploitation of the data. This will require that the secondary ground station be able to access the data. It was accepted by the technical team defining this document that the retrieval would be done using data blocks that have been structured into files in accordance with this STANAG. This provides the ability to use the mission tasking and other information (such as an event mark file) to identify the priority data and download that imagery for immediate exploitation. The requirement for this type of operation is based on three operating scenarios.

The first scenario involves a limited action where coalition forces are operating with limited resources. If more than one nation were to provide ISR capabilities, the deployment could be accomplished using one ground station from one of the nations. The primary sensors associated with that ground station would have full operational capabilities, while the other sensors would be exploited using the interface defined in STANAG 4575. All of the ISR data could be exploited in the single ground station without the need for duplicate capabilities in the theater of operations.

The second scenario involves a larger scale operation. It is assumed that multiple ground stations have been deployed and that an aircraft has diverted to a base other than its main operating location. The aircraft may have diverted due to mechanical problems, battle damage, hostile action at its main operating location, or ground station failure. Use of the interface defined in this document, would allow the ISR data collected to be rapidly accessed and exploited, limiting the possible mission degradation due to the diversion.

The third scenario in which this interface can be used is for the direct download of ISR data while on the flight line. In some cases, portable equipment, conceptually ranging from backpacks to full aerospace ground equipment (AGE) carts or portable connections to local area networks (such as on an aircraft carrier), can be used to download the data without physically removing the RMMs from the aircraft. When this equipment is available, the data port defined by this standard can be used and no other connection needs to be defined. As such, ground equipment designed to be used with a specific advanced data recorder through the interface defined in this STANAG can be used with any other STANAG-compliant recorder. In this scenario, the RMM should only be powered by the aircraft through the recorder's normal power interface. Also for this scenario, only the NADS data/control interface should be used to download data from the RMM, but it is possible that the ADSS was being controlled via its native control interface at the time the NADS interface was to be used. Contention between the recorder's native control interface and the NADS interface must be avoided. The ADSS must also be placed in an operational state where its NADS interface is functional. In general it may not be possible to sequence power to the ADSS to enable its normal power-up NADSI discovery process. It is therefore recommended that at the conclusion of all airborne recording operations, the ADSS be commanded into a recorder state enabling the NADS interface and that all further airborne control communications be suspended. This procedure should be defined in the mission application scenarios.

3. Assumptions and Ground Rules.

The basic operation, architecture, physical make-up, and required interfaces for the NATO Advanced Data Storage Interface Standard were discussed during the initial working group meetings. The users and manufacturers agreed on the following assumptions and ground rules for development of this standard.

3.1 RMM Capability. The data acquisition recorder will have a removable memory capability, which incorporates the NADS Interface. This means that either the whole recorder can be treated as an RMM and be easily removed from the acquisition platform and taken to a ground station for data download, or the recorder will contain one or more RMMs, which can be easily removed from the recorder and taken to a ground station for data download.

3.2 RMM Port(s). The removable memory portion of the recorder (as defined in 3.1 above) will have port(s) for data download / control and power, as described in this STANAG for the transfer of data to a ground station. The NADS interface is defined as the essential interface between the removable RMM and a NATO ground system. The NADS interface will be capable of interfacing with "flying leads".

3.3 Interface. The STANAG 4575 interface defines the physical connector(s), power requirements, the command set, the data interface (electrical and signal protocol), and the file structure.

3.4 NADSI Connector Accessibility. The STANAG 4575 interface provides two RMM connector options that compliant ground systems must support: 1) A single 50-pin D subminiature connector providing both power and data/control interfaces or 2) Separate military 38999 type connectors for the power and data/control interfaces. Consideration should be given to the installed accessibility of the NADSI connectors for all NADSI operating scenarios (see paragraph 2.4). For RMMs implementing 38999 connectors, the 37-pin power connector may be located to inhibit access when mated to its IU within the aircraft (power safety) as long as it is accessible for operating scenario 2.

3.5 File Recovery. File recovery will be possible from the RMM when single or multiple channels of independent sensor data are recorded. Files can be randomly accessed from the download port based on directory listings.

3.6 Parameters Outside Control of the STANAG. The NADSI STANAG does not control the physical size, performance levels, configuration and form factor for the recorder and the removable RMM. Due to the variation in capacity/rate/ cost requirements of the users, the NADSI STANAG also does not specify the technology to be used within the removable RMM.

3.7 Data Download Alternatives. A minimum of three alternatives are anticipated for download of data from the recorder or RMM. These are: (1) normal operation between an acquisition platform and its normal ground station, (2) removal of the RMM from the acquisition platform and connection via the NADS interface to a “different” ground station and (3) download from the acquisition platform to a “different” ground station through the NADS interface via either an intermediate data storage unit or directly to a ground station via cable.

3.7.1 Normal Operation. Normal operation means that an acquisition platform and its associated ground station are fully integrated and provide maximum system capability. This capability is to be achieved in one of two ways and either method allows the ground station to fully meet its operational requirements. The first way is removal of the RMM from the acquisition platform and insertion into the ground station interface unit, which is fully integrated into the ground station. The second way would be transfer of the data to the ground station via either a dedicated cable or a dedicated intermediate storage unit.

3.7.2 Direct Download to Compliant Ground Station. Operation with a STANAG 4575 compliant ground station will allow transfer of all stored data or download of specific files via the NADS interface on the RMM. This allows data download rather than providing full recorder capability. This download can be accomplished by removal of the RMM and connection to the ground station via the NADS interface.

3.7.3 Download Via Intermediate Media or Cable. The third option is to transfer the stored data via the NADS interface to an intermediate storage unit or to the ground station via NADSI-compliant cable while the recorder is still installed in the acquisition platform.

3.7.3.1 Power During Download. When the data is downloaded from the RMM via the NADS interface to a compliant ground station and the RMM remains installed in the aircraft, recorder power will be supplied by the aircraft, not from an intermediate storage unit or cable. When the RMM is removed from the aircraft, power will be supplied from the ground station via the NADS interface.

RATIONALE FOR INTERFACE SELECTION

1. Scope. This Annex provides the rationale for the selections of the various elements of the interface.

2. RMM Intelligence and Internal Processing. Initial discussions focused on the allocation of functions to the elements of a recorder system. It was important to ensure that if a RMM was removed from the platform, the data could be recovered without special processing requirements. This required that processing performed by the recorder that affects the data (e.g. error detection and correction (EDAC), error masking, compression, or memory management schemes) be transparent to the user. If these functions are part of the application, then the recorder should not change it, but functions and processing provided by the recorder must be removed before the data is transmitted through the interface. This can require intelligence in the removable memory module unit.

Further, although some technology applications would require virtually no processing in a memory unit, the application of multiple technologies to storing easily recoverable data in a common format, also leads to the incorporation of basic processing capability in the RMM. The processing allows data in the RMM to be recovered based on a directory and the associated file structure in the RMM.

3. Rationale for Selecting Fibre Channel Interface. Fibre Channel was selected as the Physical and Signaling Interface after a thorough study of all the viable alternatives and consideration of the application scenarios intended for the use of this STANAG.

3.1 Alternatives Considered. A number of alternatives were examined as candidates for this interface. The first step in this process was to define the criteria for the selection. The criteria selected were the following:

1. Commercial standard (ISO, ANSI)
2. Not proprietary to any single company
3. Standard definition readily available to community
4. Data transfer rate: Current capability of 1 Gbps or better with planned growth by a factor of 2 or better

Because of the wide selection of possible candidates, a matrix of options was created and reviewed. The complete matrix included 17 different candidate protocols with 16 different parameters on each. A selection of the primary candidates is shown in Table B-1.

TABLE B-1
Candidate Protocols For NADSI (August 1999)

Protocol	***Data Rates***	***Connections***
SCSI Wide Ultra3	1.28 Gbps	68 wide parallel, 80 pin connector
SCSI Wide Ultra3	640 Mbps	68 wide parallel, 80 pin connector
SCSI Wide Ultra3	320 Mbps	68 wide parallel, 80 pin connector
SCSI Fast and Wide	160 Mbps	68 wide parallel, 80 pin connector
USB	12 Mbps	4 pin serial
Fibre Channel	100 Mbps – 4 Gbps	CAT5 T.P., fibre, or coax serial
Firewire	400 – 800 Mbps	6 pin serial
Ethernet	1.25 Gbps	CAT5 T.P. serial
ATM	622 Mbps – 2.48 Gbps	Copper, fibre
PCI	1 Gbps	120 pin parallel
SSA	640 Mbps	4 pin serial
HIPPI 6400	6.4 Gbps	20 wide copper, 10 wide fibre

3.2 Fibre Channel Selection. Fibre Channel was chosen because of a desire to use an industry standard interface, rather than developing a new custom interface or adopting an existing proprietary interface. Fibre Channel is already widely accepted for similar applications (rapid movements of large amounts of data) and several contributing vendors already have relevant experience.

The base Fibre Channel standards contain multiple options. There are some features that are mandatory, while others are optional. In addition, there are optional ways of implementing features; for example one can choose electrical or optical transmission media, different signaling rates, etc. So by themselves, the base standards do not ensure interoperability. The Fibre Channel community approaches the interoperability issue by developing profiles that tend to follow market areas. The most active market area is the storage industry. There are three main Fibre Channel interoperability documents for storage as listed below.

1. FC-PLDA FIBRE CHANNEL PRIVATE LOOP SCSI DIRECT ATTACH [NCITS TR 19:1998]
2. FC-FLA FIBRE CHANNEL FABRIC LOOP ATTACHMENT [NCITS TR 20:1998]
3. FC-TAPE FIBRE CHANNEL TAPE AND TAPE MEDIUM CHANGERS [in approval]

The NADSI Technical Support Team chose the FC-PLDA profile because of its flexibility and because it is optimized for the Small Computer System Interface (SCSI) as the command set that uses Fibre Channel as a transport mechanism. ANSI developed the FC-PLDA profile by selecting options from the FC-FCP Fibre Channel Protocol for SCSI [ANSI X3.269-1996], FC-AL Fibre Channel Arbitrated Loop [ANSI X3.272-1996], and the SCSI-3 architecture model [ANSI X3.270-1996]. SCSI –3 was selected as the command protocol for this NADSI standard because it is well suited to large file transfers and most of the contributing vendors have existing experience with SCSI. The Fibre Channel PLDA specification provides implementation details for mapping SCSI onto the Fibre Channel interface. Use of these existing, commercially accepted documents is preferable to developing new custom requirement specifications. Most, if not all, commercially available FC chips and adapter boards support the FC-PLDA profile.

These profiles typically do not specify the lowest physical level of behavior, so the selection of signaling rates, media type (optical or electrical and variants thereof), and connectors must also be made in order to ensure interoperability. A 1 Gbps signaling rate was selected because it is the fastest speed currently available. Copper cable was chosen instead of optical fiber because reliable copper connections that run at 1 Gbps are available. Optical fiber is more difficult to work with, and optical fiber connectors are not yet well suited to frequent mate-demate cycles, especially in harsh environments. The main advantage of optical cable is for extended length connections. At 1 Gbps, copper provides a 10-meter run length, which is considered more than adequate for this application. If longer run lengths are needed in the future, copper to fiber adapter modules are commercially available. The rationale behind connector selection is described in section 6.0 of this Annex.

It should be noted that the FC-3 level in the Fibre Channel protocol defines common services that may be available across multiple ports in a network. These include mandatory services such as "Login Server" but they also include optional services such as "Data Compression" and "Encryption" which are prohibited in the NADSI STANAG and should be avoided in selecting services for the FC-3 level. However, this in no way prevents the system from using encryption or compression at the application level. If needed, data encryption and/or compression should be performed independent of and transparent to the STANAG 4575 interface requirements.

4. Rationale for the STANAG 4575 SCSI Control Protocol. Fibre Channel has been selected as a well-defined, high-speed interface best suited for rapid download of ISR mission data from a removable memory cartridge via a simple connection. Fibre Channel supports a number of mapping layer (FC-4) protocols including SCSI, IPI, HIPPI, LE and SBCCS. Of these, the SCSI protocols are the most widely used in computer peripheral storage devices. The Fibre Channel Private Loop SCSI Direct Attach (FC-PLDA, ANSI NCITS TR19-1998) interoperability profile has been selected as a requirement document for STANAG 4575. Table 17 of the FC-PLDA document specifies a control protocol using a subset of SCSI-3 commands, features and parameters for SCSI Disk and Controller Devices. FC-PLDA defines SCSI command, feature and parameter usage categories of “Required”, “Allowed”, “Invokable” and “Prohibited” between the SCSI Initiator and its Target. FC-PLDA Table 17 definitions assume that the Target device is a magnetic disk drive or equivalent device.

The STANAG 4575 control protocol must support a number of data storage media technologies. Therefore the usage definitions of FC-PLDA Table 17 have been redefined for STANAG 4575. Only the minimum set of SCSI commands required to download ISR mission data from the memory cartridge are defined as “Required”. These five STANAG 4575 “Required” SCSI commands are:

1. Test Unit Ready
2. Inquiry
3. Read Capacity
4. Read (10) Logical Block
5. Request Sense

Figure B-1 illustrates the selected standards, how the FC-PLDA profile selects and restricts logical options in these standards to achieve interoperability and how STANAG 4575 further tailors the “Required” SCSI command set.

In addition, it is recognized that some 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 will 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 B-1 in the STANAG provides the five “Required” STANAG 4575 SCSI commands and two “Recommended” commands and their features and parameter usage definitions.

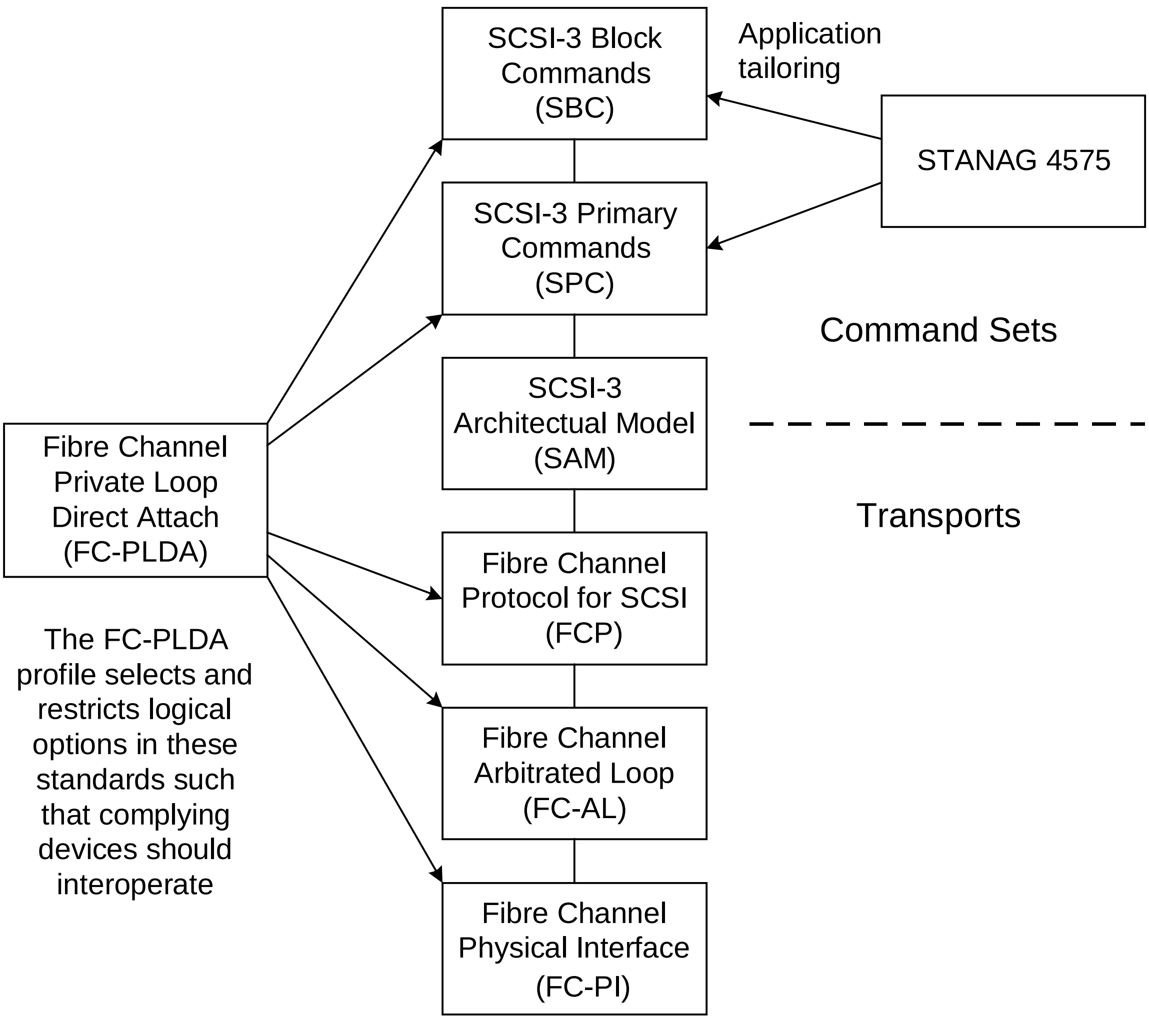


Figure B-1
STANAG 4575 Standards and Interoperability Tailoring

Figure B-2 shows an example STANAG 4575 mission data download command sequence following application of power to the compliant Memory Cartridge.

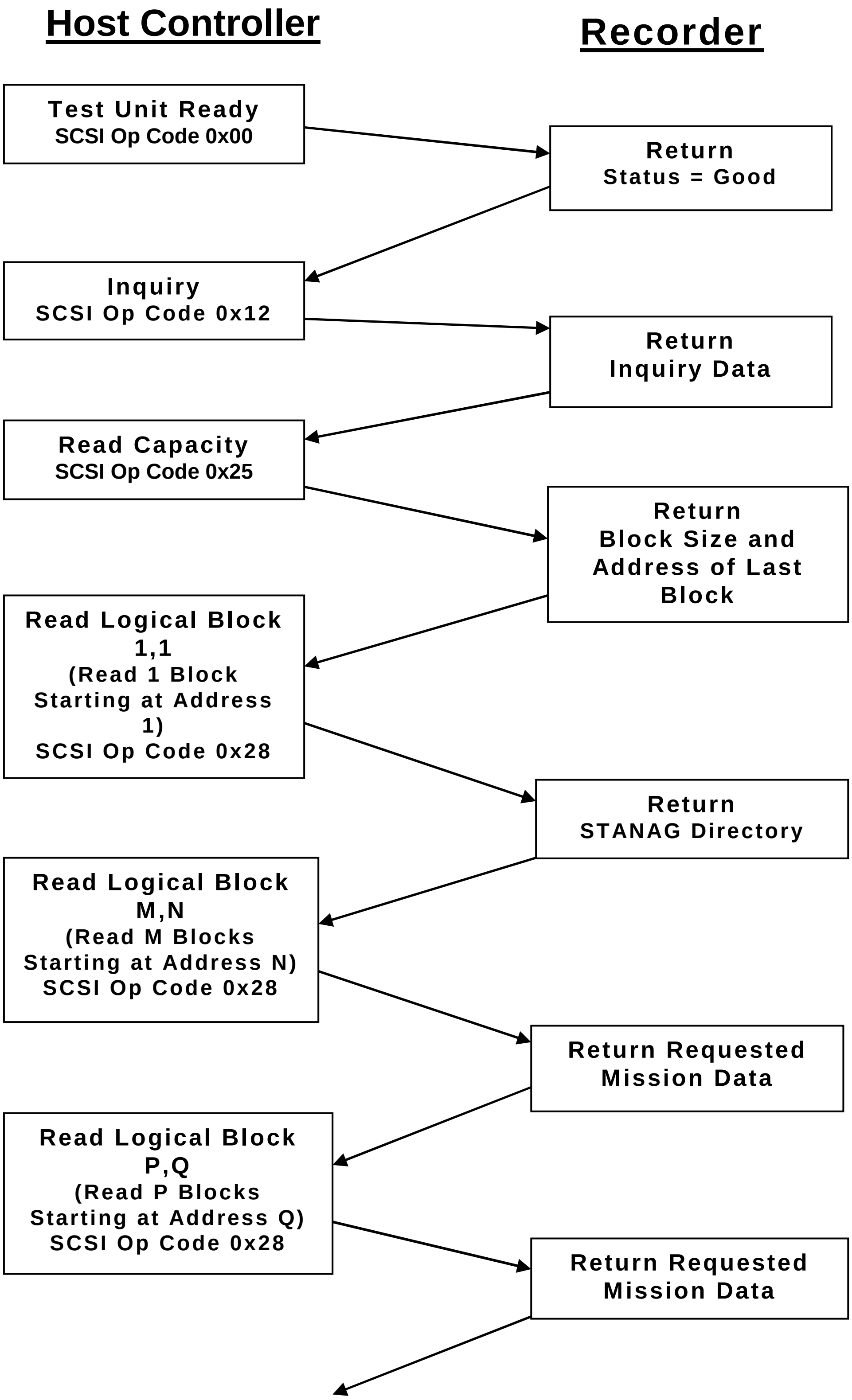


Figure B-2
Example STANAG 4575 Mission Data Download Command Sequence

Figure B-3 shows an example of a command sequence where the NADSI Host Controller issues a command not supported by the Memory Cartridge and how the Memory Cartridge responds using protocols defined by the SCSI-3 Architecture Model. (SAM). The SCSI-3 Architecture Model (SAM) defines SCSI status codes and Initiator-Peripheral protocols to be used when the peripheral receives unsupported or illegal SCSI commands. These protocols require the Peripheral to respond to an unsupported or illegal command with a CHECK CONDITION status and to subsequently respond to the Initiator's Request Sense command with appropriate SENSE KEY and SENSE CODE information. Since it is anticipated that ground download facilities will issue SCSI commands other than just those "required" by STANAG 4575, NADSI compliant devices must have a method of indicating unsupported or illegal commands.

NADSI compliant recorders, as a result of STANAG 4575 tailoring to the SCSI SPC and SBC mandatory command sets, 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. RMM support for STANAG 4575 defined ReCommended and Allowed commands can be determined by the host and the SAM defined Check Condition/Request Sense protocols. If an RMM responds to an Inquiry command with a specific SCSI version compliance, then the host can safely issue the corresponding mandatory SPC and SBC commands.

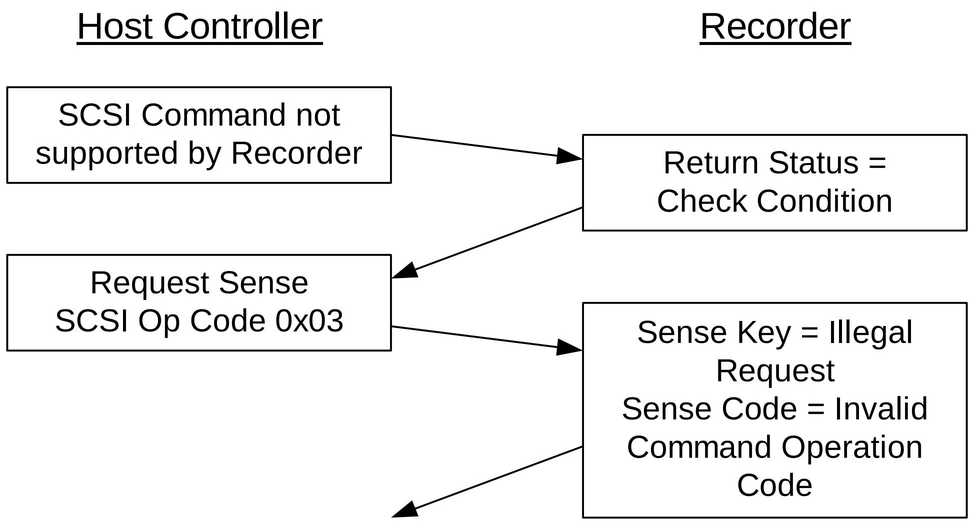


Figure B-3
Example Illustrating a Recorder's Response to an Unsupported SCSI Command

5. Rationale for Chosen File System Implementation. The recommended File System for the STANAG 4575 is unique but quite simple. It is flexible enough that it can be implemented in any media type. The file system provides a single directory that contains basic information about each recorded file and also contains pointers to the beginning of each file and block count for each file. The files described by the directory are the containers for all other recorded data. No assumptions are made regarding the contents of the files, any content and structure is permitted. Each file is required to be contained within strictly sequential logical memory locations.

5.1 Alternatives Considered. Commercial and modified commercial alternatives were considered in order to meet the needs of both embedded airborne files structures as well as the ground stations that may use commercial file structures.

5.1.1 Commercial Alternatives. Existing commercial file systems were examined for their suitability for this application. These included (but were not limited to):

5.1.1.1 UDF (CD-ROM and DVD file format). UDF is a new format, now used for recording data on CD-ROM and DVD media. Software was not available to write data in this format for any of the available embedded operating systems likely to be used by recorders. Software was likely to be available to read this file system in many commercial operating systems used at ground stations. Its complexity was judged too difficult at this time to implement for most acquisition systems. There was concern about the actual commercial support for media block sizes other than 2K. This was important; especially for some of the media types that require large media block sizes.

5.1.1.2 ISO-9660 (CD-ROM file format). ISO-9660, with its various extensions, is the standard format used for recording data on CD-ROM media. Software was likely to be available to read this file system in all commercial operating systems used at ground stations. The ISO-9660 file system's complexity was judged too difficult to implement by most of the recorder vendors. There was also a concern with this file system about actual support for various media block sizes.

5.1.1.3 NTFS (Microsoft Windows NT File System). The NTFS has attractive fault tolerance features, and permits very large files and a very large total address space. Its design is proprietary and it is judged to be very difficult to implement in the commonly used embedded operating systems used by many recorders. Multiple versions of NTFS have been released by Microsoft, and they are not necessarily compatible with each other. Thus broad compatibility with the installed base of NT workstations cannot be assured.

5.1.1.4 FAT (Microsoft Windows File System). FAT –16 was immediately rejected due to its file size limitations. FAT-32 is supported by both embedded and workstation operating systems. The total data permitted to be stored is large, however a single file is limited to a maximum of 4 gigabytes. This would require very large files to be broken down into multiple files. Common implementations are not optimized for very high-speed transfers and some modifications or tests would be required of existing systems.

5.1.1.5 XFS (Silicon Graphics File System). The XFS file system is widely regarded as extremely high performance, with regard to sustainable data rates and file sizes and total file system sizes. It is being placed into the public domain by SGI for use by Linux based systems. Unfortunately the file system is quite complex. The source code released to date is tens of thousands of lines of code. Understanding and porting the relevant portions of this code to embedded systems was considered a prohibitively expensive task. Only SGI workstations support this file system at this time.

5.1.2 Modified Commercial Alternatives. The option to modify an existing standard was also considered. These were considered because of the diverse architectures available with advanced memory systems. The options examined include:

5.1.2.1 Logically Sequential Access Mode. A very simple approach of placing all data in logically sequential files was proposed from within the group. Code would need to be developed by both the recorder and ground segment devices to access data in this format. Although new code would need to be developed by all parties, its implementation is expected to be quite simple.

5.1.2.2 Hybrid Sequential/Random Access Mode. A more complex approach was proposed that allowed for alternate means of addressing data. The data would be permitted to be placed either strictly sequentially (as preferred by solid state recorder vendors) or to be placed interleaved with other data (as preferred by rotating disk recorder vendors). This proposal also provided for multiple volumes or partitions (with their individual directories) to be defined within one physical media and for one volume to be constructed from multiple physical media. Although simple to implement for the recorders, this is complex to implement for the ground segments.

5.2 Conclusion. The two modified commercial alternatives developed widely polarized positions within the industry participants. There was no compromise position developed to bridge these views. The government participants concluded that no common solution was going to be developed. In a government-only session, an agreement was reached to ensure that the interface was as simple as possible and that the interface places the minimum burden on the ground station. The “Logically Sequential Access Mode” approach was selected as the file system to be used for this STANAG.

An example of the chosen NADSI approach is provided in Appendix 1 to this Annex for four sample files to be stored in a file system with an arbitrary block size of 300 bytes. This will allow a maximum of two file entries per directory block, given the size of the Directory block and File entries provided in the STANAG (Figures B-2 and B-3).

6. Physical and Power Interface Selection Rationale. The rationale used in selecting the connectors and power is discussed in this section. The choices made in this determination were primarily based on the STANAG 4575 Interface Requirements as provided below.

Primary consideration in connector selection was given to the D-sub connectors and MIL-STD-38999 round twist-lock military connectors. Of these, the D-sub connectors were commonly available, proven with Fibre Channel, lower cost, and had been used successfully in an aircraft environment. However, some applications in pods, aircraft and on the flight line will require MIL twist lock connectors in order to meet requirements for grounding, EMI, RFI, environmental covers and other considerations. Therefore, the standard will include provisions for both styles so that the acquisition office responsible for a particular application can choose between the most rugged or the lower cost. The ground station must support both connector types. The use of adapter cables or multiple cable sets is anticipated.

The original power (both voltages and the associated currents) was estimated by the manufacturers for all anticipated RMMs. The working group reviewed this data and a worse case set of voltages and currents was compiled. Subsequently, this list was reviewed and revised downward to the current STANAG requirement.

6.1 STANAG 4575 Interface Requirements. The interface was based on the following requirements:

1. Support the 3 operational scenarios for data download
2. Maintain Fibre Channel signal integrity and impedance control
3. Provide regulated, noise-free secondary power voltages to the RMM
4. Meet applicable EMI/EMC requirements in the NATO Processing Facility and on the Flight Line when the STANAG 4575 interface is connected
5. Meet applicable EMI/EMC requirements within the acquisition platform when the STANAG 4575 interface is not connected (captive EMI/dust connector cover)
6. Provide an environmental seal on the RMM
7. Provide an easy and secure connection (connector retention mechanism)

6.2 Connector Considerations.

6.2.1 Connector Characteristics Considered. The specific characteristics of the connectors that were of concern are as follows:

1. Physical Characteristics:
   a. Size and Mounting
   b. Environmental Qualifications/Hermetic Seal/Corrosion Resistance
   c. Covers, caps and seals
   d. Retention and Release
   e. Pin Count & pin current carrying capacity
   f. Mate/De-mate Cycles
   g. Carrier Deck Operations

2. Electrical Characteristics:
   a. Copper versus Fibre connections
   b. Converters and Adapters available
   c. Voltage/Current and Sense Requirements
   d. Grounding, Bonding and Shielding
   e. EMI/EMC

3. Practical Application Characteristics:
   a. Availability and Cost
   b. Repair ability
   c. Commercial Standards

6.2.2 Specific Connector Considerations. Areas of emphasis are highlighted below.

6.2.2.1 Fibre Channel Performance. The requirement for simultaneously maintaining Fibre Channel signal integrity and impedance control plus providing noise-free power in a common interface was thoroughly analyzed during the development of the STANAG. Gigabit Fibre Channel has bit cells less than one nanosecond in width. Fibre Channel relies on high signal integrity interconnect and provides no embedded Forward Error Correction (FEC) mechanisms. Users are specifying recorders with Bit Error Rates better than 10^{-12}. This level of performance will not be met if the download interface introduces data errors. At its 1GHz data rate, Fibre Channel can also be a very significant noise radiator.

6.2.2.2 EMI/EMC Considerations. EMI/EMC must be taken into consideration for all three configurations of the RMM, including the case where cables are attached to the RMM in the acquisition platform. MIL-STD-461 is typically invoked in these applications. The various versions of MIL-STD-461 require a range of conducted and radiated emission and susceptibility testing. The radiated susceptibility testing is typically performed with shields over all cables including power. The conducted emission and susceptibility testing is typically performed with shields removed from power cables. In the case of the single 50-pin connector, it was thought that the CE tests may be difficult to pass with expected out-of-specification energy at the Fibre Channel baud rate. The two-connector approach was considered in order to resolve this issue in addition to testing of the 50-pin connector.

Another issue considered was that MIL-STD-461 conducted susceptibility testing includes subjecting the unit's power lines to tests which inject voltage/current spikes, pulses and damped sine wave waveforms. Passing some of these tests requires the use of protection devices that are not considered appropriate for secondary input voltages such as 3.3VDC and therefore, those tests may not apply to all the NADS power interface applications.

6.2.2.3 Connectors/Cables Considered. Various MIL and Commercial connectors were considered for use. The RMM is expected to blind mate into its housing, therefore both blind mate and other mounts were considered. MIL connectors and the associated connectors are invariably a high cost alternative to standard computer type connectors and cables. Data transfer during download is expected to be 1 to 2 Gigabits per second, which will require high integrity of the signal path including the connector chosen. Naval Air Warfare Center Weapons Division (NAWCWD) at China Lake investigated Fibre Channel connector use in Navy aircraft systems and found that both D-Sub and MIL Circular connectors were being used. They provided available test data and flight experience to the working group. In the selection of connector type, both fibre optic and copper connectors are defined for the Fibre Channel interface and each was considered in the selection process.

6.2.3 D-sub connector Considerations**.** The use of D-sub connectors was strongly desired by some members of the working group, based on size, expense and availability. However, a significant number of questions were raised concerning their physical and performance characteristics. A number of commercial and military users had test data and good experience with both 9 pin D-sub and other low pin count D-sub connectors. However, a single 50 pin D-Sub connector was being considered in order to support both the signal and power requirements for NADSI. A summary of the trade-offs between the single and two connector approach is provided in 6.2.3.3. Test data for the 50 pin D-sub connector with acceptable gigabit rate Fibre Channel performance was not available at the time. A number of groups agreed to technically investigate its performance, perform testing and report to the TST.

6.2.3.1 D-sub Connector Testing. The following specific tests and investigations were performed to determine adequacy of the D-sub connector:

1. One of the test groups at Naval Air Warfare Center Aircraft Division (NAWCAD) at Pax River had been investigating Fiber channel copper connections. They provided a test demonstration of the D-sub 9-pin connector with camera data. The 9-pin D-sub connector was clearly adequate for 1 Gbit data transmission.

2. NAWCWD China Lake provided some preliminary test reports in conjunction with Raytheon testing.

3. General Dynamics Advanced Information Systems (GDAIS) tests of the 50-pin D-sub connector showed acceptable performance with no power supply voltages applied.

4. Miltope EMI/EMC Tests of Dec 1999- Miltope passed EMI (MIL-STD-461C)on the Raytheon Mass Storage Unit that contained four cartridges and each cartridge was configured with a 50-pin D-sub I/O connector for power and data. The test data was provided to the TST at the March 01 meeting.

6.2.3.2 Locking Mechanisms for D-sub connectors. In the case where a D-sub connector is used for download on the flight line, a locking mechanism is required. Multiple locking methods were evaluated and the Positronics Corporation approach was determined to be the best. Documentation, part numbers and permission to specify the connectors based on ANSI Policies and Guidelines were obtained from Positronics Corporation.

6.2.3.3 Use of one D-sub connector for power and signal vs. two connectors. Although the 9 pin D-sub connectors were proven for both signal and power applications, meeting the power requirements for all RMMs would require a minimum of a 37-pin power connector. The use of a 9 pin and a 37-pin connector would have used much more space on the RMM than a single connector. The expense for two connectors, covers and locking mechanisms was contrary to the philosophy of minimum cost and size when using the D-sub connectors. The single 50-pin D-sub connector was seen as the best alternative.

6.2.3.4 Power/signal distribution for the D-sub connector. The power connections in the 50-pin D-sub connector are in the center with the signal connections at the ends. This allows separation of the input and output high data rate signals and optimum distribution of the power connections. The number of pins allocated to each voltage is dependent on the maximum required current for each voltage. Sense wires for each voltage are incorporated and additional pins are reserved.

6.2.3.5 Mate/Demate Cycles. The specified number of mate/demate cycles was investigated for the 50 pin D-Sub connector, to insure that it would be able to support a reliable connection to the ground stations over a long life. The socket connection is the primary factor controlling the number of mate-demate cycles of the connector set. The 50 pin connectors that were defined in the STANAG had a minimum mate-demate cycle specification in excess of 10,000. This was greater than the estimated number of cycles over the life of the RMM.

6.2.4 MIL-Circular Connector Considerations. A number of applications will require a MIL qualified connector for the NADS interface. The working group determined that both the D-sub and MIL connectors will be allowable on the RMM and that the ground stations will provide the adapter such that either version can be connected to the system.

6.2.4.1 Use of two MIL-Circular connectors for power and signal. In order to preserve the maximum performance and allow for the highest potential currents in the power connector, separate connectors for power and signal were chosen for the case where MIL connectors are required.

6.2.4.2 Investigation into MIL-Circular twist lock connectors. A number of circular MIL-DTL-38999 connectors were considered and test data was investigated. A non-shielded multi-pin connector could be used for the copper Fibre Channel connection, however, it was questioned if this configuration would meet crosstalk, EMI, RFI and bandwidth requirements. Test data were provided on the W.L. Gore & Associates, Inc. inserts for the size 11 shell MIL circular connectors that showed the best bandwidth and least interference performance in a shielded Fiber Channel connector. The four-connection configuration allows for a balanced and shielded data input and output. A separate MIL-DTL-38999 connector was chosen for use as the power input. The power connector will separate the effects of the power supply/connection from the signal I/O while allowing maximum current for all voltages used.

6.3 Aircraft Power Availability and Power Safety Interlocks. Members of the working group investigated the potential effects of an inadvertent connection to both the aircraft power and ground support equipment (GSE) power while downloading data from the RMM. Multiple interlock methods, both active and passive, were suggested. Each method increased the complexity of the RMM interface for the connector and ground station. No simple method was foolproof. The working group questioned the need for GSE power and the CONOPS that governed aircraft power. The country POCs investigated the availability of acquisition platform power during download of the RMM while installed in the acquisition platform and determined that power would be available in every case. It was therefore agreed by all members that power will not be applied by the GSE for data download of the RMM while the RMM is in the acquisition platform.

6.4 STANAG Selections. The STANAG provides for two alternate configurations for the signal and power connections to the RMM. The D-Sub connector with 50 pins is the low cost, small size option that is primarily intended for use on small, commercial, or low cost RMMs. The circular military connectors, such as with the W.L. Gore & Associates, Inc. (or equivalent) insert and cable, is intended for harsh environment (fighter/pod) use where circular military specifications are required. It also provides options for use in specific applications or operating scenarios.

6.4.1 D-sub Military Connector. A 50 contact male D-sub (pin contacts), Amp P/N 746790-1 or equivalent, may be utilized on the RMM for the signal and power interface. The pin assignments are provided in the STANAG and the quantity of pins supports the required currents. In applications requiring a positive locking mechanism, a Positronic Corporation 50 contact male D-sub connector, part number HDC50M32S0V30 (non-hermetic), SAVAC50M (hermetic), or equivalent will be utilized. The mating cable will utilize a 50 contact female D-sub connector, Amp P/N M24308/2-346F (solder) or T&B P/N 622-50S (mass terminated) or equivalent, with the Positronic Corporation 50 contact female D-sub connector with quick release locking mechanism and EMI backshell, part number RD50F10GVL0 (non-hermetic), SAVAC50F (hermetic), or equivalent for the applications requiring a positive locking mechanism. In no case will a connector use fittings that would preclude mating with the positive locking mechanism defined above.

6.4.2 Circular Military Connectors. Two connectors were chosen for use in this configuration, one for the data, and one to provide power. A chassis mount connector, part number W.L. Gore & Associates, Inc. FCN 1058 or FCN 1060, or equivalent is used for the data in this configuration of the interface. The mating cable utilizes the W.L. Gore & Associates, Inc. FCN 1059 connector or equivalent. A chassis mount connector, part number MIL-DTL-38999/20WD35SN, or equivalent, is used for the power in this configuration of the interface. The mating cable uses the MIL-DTL-38999/26WD35PN connector, or equivalent.

6.4.3 Power Connector and Pin Assignments. The Power Interface for the STANAG 4575 port will be implemented in the RMM for the chosen connector configurations. The voltage, currents and power pin definitions are specified in the STANAG, for each connector configuration. Power supply regulation is required to be +/- 5% for 3.3, 5.0, and 12 VDC, and +/- 10% for 28 VDC. These values were set, based on expected operation of known RMMs in a controlled environment such as a ground station, by the manufacturers in the working group.

6.4.4 Power Availability Policy. There are two scenarios that were considered in determining the power availability policy. The first scenario involves removal of the RMM from the acquisition platform and transportation to a ground facility to process the collected mission data. In that scenario the RMM will be powered through the STANAG 4575 power interface.

In the second scenario, the RMM remains on the acquisition platform, mounted within its native Interface Unit (IU). In that scenario the RMM will be powered via acquisition platform power only, using the recorder's native power supply located within its IU. The STANAG does not define or require RMM power protection logic for the potentially damaging case of both acquisition platform and STANAG power being simultaneously applied to the RMM. Power should never be applied by the download equipment in this scenario. This determination was based on an investigation regarding all participating countries into availability of acquisition platform power for data download after a mission.

EXAMPLE OF NADSI FILE IMPLEMENTATION.

1. Example description. This appendix describes an example of the NADSI implementation for the storage of four files in NADSI block 1 and block 2 in terms of the hexadecimal and decimal representation for the file structure. The assumption is a block size of 300 bytes, which would mean that a maximum of two file entries per directory block is possible (64bytes + 112 + 112 = 288 bytes). The spread sheet has 600 lines, representing the 2 x 300 byte blocks. Each line is a byte, with both the hex and decimal representation of which byte should be there. It can be assumed (as per the STANAG) that multiple byte numbers are stored with their MSB in the first memory address and with their LSB in the last memory address. Strings are represented as Left Justified, and are terminated with the ASCI 0x00 NULL character (EOS – End Of String). The file size parameter assumes that the file occupies the whole of each block, hence the total is a multiple of 300. This is perhaps unlikely in a real world scenario, but was made simple for the example.

Filename : NADSITESTFILEalpha
File Size : 70,500,000 Bytes
File Start Address : 100 dec
File Block Count : 235,000 dec
File Create Date : 02 Oct 2002
File Create Time : 13:04:27.00

Filename : NADSITESTFILEbravo
File Size : 151,310,100 Bytes
File Start Address : 236,000 dec
File Block Count : 504,367 dec
File Create Date : 02 Oct 2002
File Create Time : 17:07:15.03

Filename : NADSITESTFILEcharlie
File Size : 47,220,000 bytes
File Start Address : 741,000 dec
File Block Count : 157,400 dec
File Create Date : 03 Oct 2002
File Create Time : 08:09:59.07

Filename : NADSITESTFILEdelta
File Size : 419,346,300 bytes
File Start Address : 899,000 dec
File Block Count : 1,397,821 dec
* File Create Date : 03 Oct ----
* File Create Time : 09:59:----

* Note: The year and the seconds are not defined in the fourth file to show an example of how the file system should work when portions of the field are unavailable.

2. NADSI Block Layout. The layout for NADSI blocks 1 and 2 is provided below for the four files described above.

NADS Block 1 & 2 Layout for 4 files (a,b,c,d) with a block size of 300 bytes

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
1	Magic Number (8)	1		46	70	"F"
2		2		4F	79	"O"
3		3		52	82	"R"
4		4		54	84	"T"
5		5		59	89	"Y"
6		6		74	116	"t"
7		7		77	119	"w"
8		8		6F	111	"o"
9	Revision Number (1)	1		01	1	Edition 1
10	Shutdown (1)	1		FF	255	Good
11	Number of File Entries (2)	1		00	0	2 files
12		2		02	2	
13	Reserved (4)	1		FF	255	
14		2		FF	255	
15		3		FF	255	
16		4		FF	255	
17	Volume Name (32)	1		4E	78	"N"
18		2		41	65	"A"
19		3		44	68	"D"
20		4		53	83	"S"
21		5		54	84	"T"
22		6		45	69	"E"
23		7		53	83	"S"
24		8		54	84	"T"
25		9		52	82	"R"
26		10		4D	77	"M"
27		11		4D	77	"M"
28		12		31	49	"1"
29		13		00	0	EOS Null
30		14		00	0	EOS Null
31		15		00	0	EOS Null
32		16		00	0	EOS Null
33		17		00	0	EOS Null
34		18		00	0	EOS Null
35		19		00	0	EOS Null
36		20		00	0	EOS Null
37		21		00	0	EOS Null
38		22		00	0	EOS Null
39		23		00	0	EOS Null
40		24		00	0	EOS Null
41		25		00	0	EOS Null
42		26		00	0	EOS Null
43		27		00	0	EOS Null

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
44		28		00	0	EOS Null
45		29		00	0	EOS Null
46		30		00	0	EOS Null
47		31		00	0	EOS Null
48		32		00	0	EOS Null
49	Forward Directory Link (8)	1		00	0	
50	Block 2	2		00	0	
51	"Next Directory Block"	3		00	0	
52		4		00	0	
53		5		00	0	
54		6		00	0	
55		7		00	0	
56		8		02	2	
57	Reverse Directory Link (8)	1		00	0	
58	Block 1	2		00	0	
59	"This Block"	3		00	0	
60		4		00	0	
61		5		00	0	
62		6		00	0	
63		7		00	0	
64		8		01	1	
65	File Name (56)	1	a	4E	78	"N"
66		2	a	41	65	"A"
67		3	a	44	68	"D"
68		4	a	53	83	"S"
69		5	a	54	84	"T"
70		6	a	45	69	"E"
71		7	a	53	83	"S"
72		8	a	54	84	"T"
73		9	a	46	70	"F"
74		10	a	49	73	"I"
75		11	a	4C	76	"L"
76		12	a	45	69	"E"
77		13	a	61	97	"a"
78		14	a	6C	108	"l"
79		15	a	70	112	"p"
80		16	a	68	104	"h"
81		17	a	61	97	"a"
82		18	a	00	0	EOS Null
83		19	a	00	0	EOS Null
84		20	a	00	0	EOS Null
85		21	a	00	0	EOS Null
86		22	a	00	0	EOS Null
87		23	a	00	0	EOS Null
88		24	a	00	0	EOS Null
89		25	a	00	0	EOS Null

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
90		26	a	00	0	EOS Null
91		27	a	00	0	EOS Null
92		28	a	00	0	EOS Null
93		29	a	00	0	EOS Null
94		30	a	00	0	EOS Null
95		31	a	00	0	EOS Null
96		32	a	00	0	EOS Null
97		33	a	00	0	EOS Null
98		34	a	00	0	EOS Null
99		35	a	00	0	EOS Null
100		36	a	00	0	EOS Null
101		37	a	00	0	EOS Null
102		38	a	00	0	EOS Null
103		39	a	00	0	EOS Null
104		40	a	00	0	EOS Null
105		41	a	00	0	EOS Null
106		42	a	00	0	EOS Null
107		43	a	00	0	EOS Null
108		44	a	00	0	EOS Null
109		45	a	00	0	EOS Null
110		46	a	00	0	EOS Null
111		47	a	00	0	EOS Null
112		48	a	00	0	EOS Null
113		49	a	00	0	EOS Null
114		50	a	00	0	EOS Null
115		51	a	00	0	EOS Null
116		52	a	00	0	EOS Null
117		53	a	00	0	EOS Null
118		54	a	00	0	EOS Null
119		55	a	00	0	EOS Null
120		56	a	00	0	EOS Null
121	File Start Address (8)	1	a	00	0	
122	Block 100	2	a	00	0	
123		3	a	00	0	
124		4	a	00	0	
125		5	a	00	0	
126		6	a	00	0	
127		7	a	00	0	
128		8	a	64	100	
129	File Block Count (8)	1	a	00	0	
130	235,000 blocks	2	a	00	0	
131	0x0395F8	3	a	00	0	
132		4	a	00	0	
133		5	a	00	0	
134		6	a	03	3	
135		7	a	95	149	

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
136		8	a	F8	248	
137	File Size (8)	1	a	00	0	
138	70,500,000 bytes	2	a	00	0	
139	0x0433BEA0	3	a	00	0	
140		4	a	00	0	
141		5	a	04	4	
142		6	a	33	51	
143		7	a	BE	190	
144		8	a	A0	160	
145	Create Date (8)	1	a	30	48	
146	10/2/2002	2	a	32	50	
147		3	a	31	49	
148		4	a	30	48	
149		5	a	32	50	
150		6	a	30	48	
151		7	a	30	48	
152		8	a	32	50	
153	Create Time (8)	1	a	31	49	
154	13:04:27:00	2	a	33	51	
155		3	a	30	48	
156		4	a	34	52	
157		5	a	32	50	
158		6	a	37	55	
159		7	a	30	48	
160		8	a	30	48	
161	Time Type (1) Zulu	1	a	00	0	
162	Reserved (7)	1	a	FF	255	
163		2	a	FF	255	
164		3	a	FF	255	
165		4	a	FF	255	
166		5	a	FF	255	
167		6	a	FF	255	
168		7	a	FF	255	
169	Vendor Unique (8)	1	a	FF	255	
170		2	a	FF	255	
171		3	a	FF	255	
172		4	a	FF	255	
173		5	a	FF	255	
174		6	a	FF	255	
175		7	a	FF	255	
176		8	a	FF	255	
177	File Name (56)	1	b	4E	78	"N"
178		2	b	41	65	"A"
179		3	b	44	68	"D"
180		4	b	53	83	"S"

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
181		5	b	54	84	"T"
182		6	b	45	69	"E"
183		7	b	53	83	"S"
184		8	b	54	84	"T"
185		9	b	46	70	"F"
186		10	b	49	73	"I"
187		11	b	4C	76	"L"
188		12	b	45	69	"E"
189		13	b	62	98	"b"
190		14	b	72	114	"r"
191		15	b	61	97	"a"
192		16	b	76	118	"v"
193		17	b	6F	111	"o"
194		18	b	00	0	EOS Null
195		19	b	00	0	EOS Null
196		20	b	00	0	EOS Null
197		21	b	00	0	EOS Null
198		22	b	00	0	EOS Null
199		23	b	00	0	EOS Null
200		24	b	00	0	EOS Null
201		25	b	00	0	EOS Null
202		26	b	00	0	EOS Null
203		27	b	00	0	EOS Null
204		28	b	00	0	EOS Null
205		29	b	00	0	EOS Null
206		30	b	00	0	EOS Null
207		31	b	00	0	EOS Null
208		32	b	00	0	EOS Null
209		33	b	00	0	EOS Null
210		34	b	00	0	EOS Null
211		35	b	00	0	EOS Null
212		36	b	00	0	EOS Null
213		37	b	00	0	EOS Null
214		38	b	00	0	EOS Null
215		39	b	00	0	EOS Null
216		40	b	00	0	EOS Null
217		41	b	00	0	EOS Null
218		42	b	00	0	EOS Null
219		43	b	00	0	EOS Null
220		44	b	00	0	EOS Null
221		45	b	00	0	EOS Null
222		46	b	00	0	EOS Null
223		47	b	00	0	EOS Null
224		48	b	00	0	EOS Null
225		49	b	00	0	EOS Null
226		50	b	00	0	EOS Null

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
227		51	b	00	0	EOS Null
228		52	b	00	0	EOS Null
229		53	b	00	0	EOS Null
230		54	b	00	0	EOS Null
231		55	b	00	0	EOS Null
232		56	b	00	0	EOS Null
233	File Start Address (8)	1	b	00	0	
234	Block 236,000	2	b	00	0	
235	0x0399E0	3	b	00	0	
236		4	b	00	0	
237		5	b	00	0	
238		6	b	03	3	
239		7	b	99	153	
240		8	b	E0	224	
241	File Block Count (8)	1	b	00	0	
242	504,367 Blocks	2	b	00	0	
243	0x07B22F	3	b	00	0	
244		4	b	00	0	
245		5	b	00	0	
246		6	b	07	7	
247		7	b	B2	178	
248		8	b	2F	47	
249	File Size (8)	1	b	00	0	
250	151,310,100 bytes	2	b	00	0	
251	0x0904CF14	3	b	00	0	
252		4	b	00	0	
253		5	b	09	9	
254		6	b	04	4	
255		7	b	CF	207	
256		8	b	14	20	
257	Create Date (8)	1	b	30	48	
258	10/2/2002	2	b	32	50	
259		3	b	31	49	
260		4	b	30	48	
261		5	b	32	50	
262		6	b	30	48	
263		7	b	30	48	
264		8	b	32	50	
265	Create Time (8)	1	b	31	49	
266	17:07:15:03	2	b	37	55	
267		3	b	30	48	
268		4	b	37	55	
269		5	b	31	49	
270		6	b	35	53	
271		7	b	30	48	

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
272		8	b	33	51	
273	Time Type (1) Zulu	1	b	00	0	
274	Reserved (7)	1	b	FF	255	
275		2	b	FF	255	
276		3	b	FF	255	
277		4	b	FF	255	
278		5	b	FF	255	
279		6	b	FF	255	
280		7	b	FF	255	
281	Vendor Unique (8)	1	b	FF	255	
282		2	b	FF	255	
283		3	b	FF	255	
284		4	b	FF	255	
285		5	b	FF	255	
286		6	b	FF	255	
287		7	b	FF	255	
288		8	b	FF	255	
289	UNUSED	UNUSED		FF	255	
290	UNUSED	UNUSED		FF	255	
291	UNUSED	UNUSED		FF	255	
292	UNUSED	UNUSED		FF	255	
293	UNUSED	UNUSED		FF	255	
294	UNUSED	UNUSED		FF	255	
295	UNUSED	UNUSED		FF	255	
296	UNUSED	UNUSED		FF	255	
297	UNUSED	UNUSED		FF	255	
298	UNUSED	UNUSED		FF	255	
299	UNUSED	UNUSED		FF	255	
300	UNUSED Block Boundary	UNUSED		FF	255	
301	Magic Number (8)	1		46	70	"F"
302		2		4F	79	"O"
303		3		52	82	"R"
304		4		54	84	"T"
305		5		59	89	"Y"
306		6		74	116	"t"
307		7		77	119	"w"
308		8		6F	111	"o"
309	Revision Number (1)	1		01	1	Edition 1
310	Shutdown (1)	1		FF	255	N/A
311	Number of File Entries (2)	1		00	0	2 files
312		2		02	2	
313	Reserved (4)	1		FF	255	
314		2		FF	255	
315		3		FF	255	
316		4		FF	255	

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
317	Volume Name (32)	1		4E	78	"N"
318		2		41	65	"A"
319		3		44	68	"D"
320		4		53	83	"S"
321		5		54	84	"T"
322		6		45	69	"E"
323		7		53	83	"S"
324		8		54	84	"T"
325		9		52	82	"R"
326		10		4D	77	"M"
327		11		4D	77	"M"
328		12		31	49	"1"
329		13		00	0	EOS Null
330		14		00	0	EOS Null
331		15		00	0	EOS Null
332		16		00	0	EOS Null
333		17		00	0	EOS Null
334		18		00	0	EOS Null
335		19		00	0	EOS Null
336		20		00	0	EOS Null
337		21		00	0	EOS Null
338		22		00	0	EOS Null
339		23		00	0	EOS Null
340		24		00	0	EOS Null
341		25		00	0	EOS Null
342		26		00	0	EOS Null
343		27		00	0	EOS Null
344		28		00	0	EOS Null
345		29		00	0	EOS Null
346		30		00	0	EOS Null
347		31		00	0	EOS Null
348		32		00	0	EOS Null
349	Forward Directory Link (8)	1		00	0	
350	Block 2	2		00	0	
351	I.e. this is last dir blk	3		00	0	
352	Points to itself	4		00	0	
353		5		00	0	
354		6		00	0	
355		7		00	0	
356		8		02	2	
357	Reverse Directory Link (8)	1		00	0	
358	Block 1	2		00	0	
359		3		00	0	
360		4		00	0	
361		5		00	0	
362		6		00	0	

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
363		7		00	0	
364		8		01	1	
365	File Name (56)	1	c	4E	78	"N"
366		2	c	41	65	"A"
367		3	c	44	68	"D"
368		4	c	53	83	"S"
369		5	c	54	84	"T"
370		6	c	45	69	"E"
371		7	c	53	83	"S"
372		8	c	54	84	"T"
373		9	c	46	70	"F"
374		10	c	49	73	"I"
375		11	c	4C	76	"L"
376		12	c	45	69	"E"
377		13	c	63	99	"c"
378		14	c	68	104	"h"
379		15	c	61	97	"a"
380		16	c	72	114	"r"
381		17	c	6C	108	"l"
382		18	c	69	105	"i"
383		19	c	65	101	"e"
384		20	c	00	0	EOS Null
385		21	c	00	0	EOS Null
386		22	c	00	0	EOS Null
387		23	c	00	0	EOS Null
388		24	c	00	0	EOS Null
389		25	c	00	0	EOS Null
390		26	c	00	0	EOS Null
391		27	c	00	0	EOS Null
392		28	c	00	0	EOS Null
393		29	c	00	0	EOS Null
394		30	c	00	0	EOS Null
395		31	c	00	0	EOS Null
396		32	c	00	0	EOS Null
397		33	c	00	0	EOS Null
398		34	c	00	0	EOS Null
399		35	c	00	0	EOS Null
400		36	c	00	0	EOS Null
401		37	c	00	0	EOS Null
402		38	c	00	0	EOS Null
403		39	c	00	0	EOS Null
404		40	c	00	0	EOS Null
405		41	c	00	0	EOS Null
406		42	c	00	0	EOS Null
407		43	c	00	0	EOS Null
408		44	c	00	0	EOS Null

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
409		45	c	00	0	EOS Null
410		46	c	00	0	EOS Null
411		47	c	00	0	EOS Null
412		48	c	00	0	EOS Null
413		49	c	00	0	EOS Null
414		50	c	00	0	EOS Null
415		51	c	00	0	EOS Null
416		52	c	00	0	EOS Null
417		53	c	00	0	EOS Null
418		54	c	00	0	EOS Null
419		55	c	00	0	EOS Null
420		56	c	00	0	EOS Null
421	File Start Address (8)	1	c	00	0	
422	Block 741,000	2	c	00	0	
423	0x0B4E88	3	c	00	0	
424		4	c	00	0	
425		5	c	00	0	
426		6	c	0B	11	
427		7	c	4E	78	
428		8	c	88	136	
429	File Block Count (8)	1	c	00	0	
430	157,400 Blocks	2	c	00	0	
431	0x0266D8	3	c	00	0	
432		4	c	00	0	
433		5	c	00	0	
434		6	c	02	2	
435		7	c	66	102	
436		8	c	D8	216	
437	File Size (8)	1	c	00	0	
438	47,220,000 bytes	2	c	00	0	
439	0x02D08520	3	c	00	0	
440		4	c	00	0	
441		5	c	02	2	
442		6	c	D0	208	
443		7	c	85	133	
444		8	c	20	32	
445	Create Date (8)	1	c	30	48	
446	10/3/2002	2	c	33	51	
447		3	c	31	49	
448		4	c	30	48	
449		5	c	32	50	
450		6	c	30	48	
451		7	c	30	48	
452		8	c	32	50	
453	Create Time (8)	1	c	30	48	

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
454	08:09:59:07	2	c	38	56	
455		3	c	30	48	
456		4	c	39	57	
457		5	c	35	53	
458		6	c	39	57	
459		7	c	30	48	
460		8	c	37	55	
461	Time Type (1) Zulu	1	c	00	0	
462	Reserved (7)	1	c	FF	255	
463		2	c	FF	255	
464		3	c	FF	255	
465		4	c	FF	255	
466		5	c	FF	255	
467		6	c	FF	255	
468		7	c	FF	255	
469	Vendor Unique (8)	1	c	FF	255	
470		2	c	FF	255	
471		3	c	FF	255	
472		4	c	FF	255	
473		5	c	FF	255	
474		6	c	FF	255	
475		7	c	FF	255	
476		8	c	FF	255	
477	File Name (56)	1	d	4E	78	"N"
478		2	d	41	65	"A"
479		3	d	44	68	"D"
480		4	d	53	83	"S"
481		5	d	54	84	"T"
482		6	d	45	69	"E"
483		7	d	53	83	"S"
484		8	d	54	84	"T"
485		9	d	46	70	"F"
486		10	d	49	73	"I"
487		11	d	4C	76	"L"
488		12	d	45	69	"E"
489		13	d	64	100	"d"
490		14	d	65	101	"e"
491		15	d	6C	108	"l"
492		16	d	74	116	"t"
493		17	d	61	97	"a"
494		18	d	00	0	EOS Null
495		19	d	00	0	EOS Null
496		20	d	00	0	EOS Null
497		21	d	00	0	EOS Null
498		22	d	00	0	EOS Null

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
499		23	d	00	0	EOS Null
500		24	d	00	0	EOS Null
501		25	d	00	0	EOS Null
502		26	d	00	0	EOS Null
503		27	d	00	0	EOS Null
504		28	d	00	0	EOS Null
505		29	d	00	0	EOS Null
506		30	d	00	0	EOS Null
507		31	d	00	0	EOS Null
508		32	d	00	0	EOS Null
509		33	d	00	0	EOS Null
510		34	d	00	0	EOS Null
511		35	d	00	0	EOS Null
512		36	d	00	0	EOS Null
513		37	d	00	0	EOS Null
514		38	d	00	0	EOS Null
515		39	d	00	0	EOS Null
516		40	d	00	0	EOS Null
517		41	d	00	0	EOS Null
518		42	d	00	0	EOS Null
519		43	d	00	0	EOS Null
520		44	d	00	0	EOS Null
521		45	d	00	0	EOS Null
522		46	d	00	0	EOS Null
523		47	d	00	0	EOS Null
524		48	d	00	0	EOS Null
525		49	d	00	0	EOS Null
526		50	d	00	0	EOS Null
527		51	d	00	0	EOS Null
528		52	d	00	0	EOS Null
529		53	d	00	0	EOS Null
530		54	d	00	0	EOS Null
531		55	d	00	0	EOS Null
532		56	d	00	0	EOS Null
533	File Start Address (8)	1	d	00	0	
534	Block 899,000	2	d	00	0	
535	0x0DB7B8	3	d	00	0	
536		4	d	00	0	
537		5	d	00	0	
538		6	d	0D	13	
539		7	d	B7	183	
540		8	d	B8	184	
541	File Block Count (8)	1	d	00	0	
542	1,397,821 blocks	2	d	00	0	
543	0x15543D	3	d	00	0	
544		4	d	00	0	

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
545		5	d	00	0	
546		6	d	15	21	
547		7	d	54	84	
548		8	d	3D	61	
549	File Size (8)	1	d	00	0	
550	419,346,300 bytes	2	d	00	0	
551	0x18FEB77C	3	d	00	0	
552		4	d	00	0	
553		5	d	18	24	
554		6	d	FE	254	
555		7	d	B7	183	
556		8	d	7C	124	
557	Create Date (8)	1	d	30	48	
558	10/3/----	2	d	33	51	
559		3	d	31	49	
560		4	d	30	48	
561		5	d	2D	45	
562		6	d	2D	45	
563		7	d	2D	45	
564		8	d	2D	45	
565	Create Time (8)	1	d	30	48	
566	09:59:----	2	d	39	57	
567		3	d	35	53	
568		4	d	39	57	
569		5	d	2D	45	
570		6	d	2D	45	
571		7	d	2D	45	
572		8	d	2D	45	
573	Time Type (1) Zulu	1	d	00	0	
574	Reserved (7)	1	d	FF	255	
575		2	d	FF	255	
576		3	d	FF	255	
577		4	d	FF	255	
578		5	d	FF	255	
579		6	d	FF	255	
580		7	d	FF	255	
581	Vendor Unique (8)	1	d	FF	255	
582		2	d	FF	255	
583		3	d	FF	255	
584		4	d	FF	255	
585		5	d	FF	255	
586		6	d	FF	255	
587		7	d	FF	255	
588		8	d	FF	255	
589	UNUSED	UNUSED		FF	255	

Byte Number (1-600)	Element	Element Byte Number	File	HEX	DEC	
590	UNUSED	UNUSED		FF	255	
591	UNUSED	UNUSED		FF	255	
592	UNUSED	UNUSED		FF	255	
593	UNUSED	UNUSED		FF	255	
594	UNUSED	UNUSED		FF	255	
595	UNUSED	UNUSED		FF	255	
596	UNUSED	UNUSED		FF	255	
597	UNUSED	UNUSED		FF	255	
598	UNUSED	UNUSED		FF	255	
599	UNUSED	UNUSED		FF	255	
600	UNUSED Block Boundary	UNUSED		FF	255	

ACQUISITION GUIDANCE

1. Scope. This Annex provides guidance for items to be included in a technical specification when purchasing an Advanced Data Storage System (ADSS). The annex structure consists of a short introduction followed by two Appendices: Appendix 1, an Airborne Recorder Acquisition Specification outline and Appendix 2, a Ground Station Interface Acquisition Specification outline.

The intent for future data storage system capabilities go far beyond the requirements for downloading acquired data to a ground station from an RMM via a NADS interface. There are many alternatives that would allow the NADS interface to meet its minimum requirements while providing a much more extensive capability to programs that specify additional capability. In addition, mechanical and electronic interfaces used for system download may use any portion of the NADSI interface and capability via additional connectors and couplers when operating with their native ground station.

It should be noted that the basic concept of this architecture includes provisions for removing the memory module from the platform for replay in the ground station. This concept is the most stressing of the operational scenarios. The ability to remove the memory can involve removal of the portion of the recorder that contains the memory media, or in some designs can include removal of the entire recorder, provided that this can be done within the timelines provided by the specific application. In addition, in some application scenarios, the data will be downloaded directly at the acquisition platform, using portable download equipment that can be transported to a ground station, or in the case of carrier operations and other applications with limited distances, may be directly connected to the ground station. As the program acquisition office develops the specification, consideration should be made to ensure the interoperability with allied forces, while meeting the requirements of the application. The specification outlines provided herein, should be used as guidance for developing the acquisition specification, which would be tailored to the application.

2. Airborne Advanced Data Storage System Architectures. There are a number of architectural approaches implemented in avionics data recorders that provide a range of mission capabilities and performance. These can be grouped into the four general Advanced Data Storage System categories briefly summarized below and in Table C-1:

1. Legacy magnetic tape recorder emulation: simulates writing/reading data to magnetic tape. Typically provides direct data connection between the airborne sensor/data source and the recorder. Control of the recorder is typically through a separate interface (RS-422, MIL-STD-1553, etc.). The recorder controls writing mission data to the media. The recorder's host controller maintains an external directory of recordings that is written to the media following the mission.
2. Intelligent Peripheral: uses random access solid state or rotating media to support features such as multiple independent write and read data interfaces and simultaneous write and read operations. Typically controls assignment of write data addresses and generates an internal directory of written files. Typically implements a separate control interface.
3. Direct Access Storage Device (DASD): provides a direct connection to the system controller for both data and control. The system controller conveys sensor data into explicitly addressed memory locations within the recorder.
4. File Server: similar to DASD however the system controller uses a data write/read protocol using logically named files and offsets within those files. The recorder manages the placement of the data comprising these files into its memory space.

TABLE C-1 Airborne ADSS Architectures & Characteristics				
Data Storage Device Characteristic	**Mag. Tape Emulation**	**Intelligent Peripheral**	**DASD**	**File Server**
Sequential access media	**X**			
Fast, random access media		**X**	**X**	**X**
Host maintains directory via recorder queries; Recorder assigns media write addresses	**X**	**X**		
Recorder maintains directory and assigns media write addresses		**X**		**X**
Host maintains directory and assigns media write addresses			**X**	
Provides separate data and control interfaces	**X**	**X**		
Provides a common data and control interface			**X**	**X**
Supports single channel record or play operation	**X**	**X**	**X**	**X**
Supports multiple, independent record and play interfaces		**X**		
Support multiple data inputs/outputs via multiplexing mission data external to recorder	**X**	**X**	**X**	**X**
Supports partitioning storage capacity between record channels on mission basis		**X**	**X**	**X**
Supports simultaneous record and play at independent data rates		**X**	**X**	**X**
Supports record data interface handshake conventions to identify valid data	**X**	**X**		
Supports play data interface flow control	**X**	**X**		
Supports play data access based on mission time, event marks, etc.	**X**	**X**	**X**	**X**
Supports data block oriented protocol transfers			**X**	
Supports file oriented protocol transfers				**X**

2.1 Airborne Recorder Acquisition Specification Outline. An airborne recorder acquisition specification outline is contained in Appendix 1, SPECIFICATION TEMPLATE FOR ACQUISITION PLATFORM ADVANCED DATA STORAGE SYSTEM CHARACTERISTICS. This outline provides suggested areas of specification for an airborne Advanced Data Storage System (ADSS) and the guidelines for the scope and depth of these specifications. Each section is organized relative to content. This outline provides all of the elements of a specification but should be tailored to the specific application. Some parameters may not be appropriate for a given application. The outline is based on a review of several specifications for recording systems intended to incorporate the STANAG 4575 interface and function in the NATO environment as outlined in the CONOPS of ANNEX A to this AEDP. Most of the requirement items recommended for inclusion are common to the sample specifications considered, although the ordering, grouping and detail provided varied considerably.

3. Ground Station Interface Acquisition Specification Outline. The ground station is intended to support data download from any RMM through the NADS Interface. This may require the development of device driver software that will allow the direct connection and control of the RMM by the processor. The ground station must also meet the physical and electrical requirements of the RMM interface as stated in STANAG 4575. A Template for a Specification to assist Ground Stations in meeting NADS Interface requirements, including specific Driver recommendations is provided in Appendix 2, SPECIFICATION TEMPLATE FOR GROUND STATION TO MEET NADS INTERFACE REQUIREMENTS. It should be noted that this section addresses only the aspects of the Ground Station that are impacted by the NADS Interface, and does not address the other functional requirements essential to operation of a ISR ground station.

3.1 Required Drivers Based on the results of the first phase testing program conducted by the NADS TST during the STANAG 4575 development, it was determined that some Ground Station processor operating systems may require a driver be developed to allow download of data from the RMM. (See paragraph 1.1 of Annex F, Testing of NADS Interface with CIGSS Test Van at NAWC, China Lake, CA; 3 May 2001.)

3.2 Application Scenario Indicated Functionality. The interface should provide the functionality to download the data contents of the RMM. This implies that the ground station will determine the logical block size, access the directory of the RMM data files, and be able to select and download individual files, file segments, or all of the files.

3.3 RMM Variability. STANAG 4575 defines the general requirements to support the RMM operation in a ground station. These requirements apply to a wide range of RMM designs, using various technologies and a wide range of specific requirements within those general requirements of the STANAG. Consideration should be given to factors relating to handling, positioning and normal safety precautions for these devices when transported and used in a ground station.

3.4 Interface Connections. The flying lead used in the ground station should be of adequate length and appropriate placement to allow easy connection to the RMM in the designed space and location. The length of the flying lead should be kept to a minimum in accordance with good engineering design practice. STANAG 4575 allows the use of both Mil Circular and D-sub connectors. The ground station must provide a method of connection for both types of connectors.

3.4.1 Optical vs. Copper Connectors. Investigation into optical vs. copper connector reliability determined that optical connections and cable are less reliable in an adverse environment or in an application which requires frequent mating and un-mating, especially in a dirty environment. Since there are in-line converters available to change from copper to optical and back, copper was chosen as the NADS interface connection with the belief that a copper to optical converter could be used whenever necessary. Commercially available Fibre Channel Media Interface Adapters (MIA) typically use 9-pin D-subminiature connectors for the copper interface. MIA pin assignments include voltage and ground pins for powering MIA-internal electrical-to-optical conversion electronics. Neither of the NADSI connector options is directly compatible with standard MIA units. It will be necessary for programs wishing to convert to optical fiber to develop custom conversion cabling and means for powering the associated electrical-to-optical conversion electronics.

3.5 Power. STANAG 4575 requires that power to operate the RMM be supplied by the ground station when the RMM is removed from the ADSS on the acquisition platform and connected directly via the NADS Interface to the ground station. Since in many case STANAG 4575 power voltages (+3.3VDC, +5.0VDC, +12.0VDC) will be directly connected to the RMM's internal electronics, it is imperative that these voltage be well regulated, noise-free and carefully applied to the unit. Design considerations for the STANAG 4575 power supply system are discussed by topic below.

3.5.1 Output Current: The maximum STANAG 4575 currents versus voltage are shown in the Table C-2. It is recommended that the power supplies be rated to supply at least 50% more current than these requirements in order to achieve high power supply reliability and long life.

TABLE C-2
Maximum STANAG 4575 Currents vs. Voltage

Voltage	STANAG 4575 Current Requirement	Recommended P.S. Current Rating
+3.3 VDC	15 A	22.5 A
+5.0 VDC	10 A	15 A
+12.0 VDC	13.5 A	20 A
+28 VDC	5 A	7.5 A

3.5.2 Voltage Regulation: The regulation of the +3.3V, +5.0V and +12.0V power supplies should be rated at +/- 5% under full load conditions. The regulation of the +28V power supply should be rated at +/- 10% under full load conditions.

3.5.3 Output Noise and Ripple: Output noise and ripple on the +3.3V, +5.0V and +12.0V power supplies should be rated at 2% or less of the regulated output voltage under full load conditions.

3.5.4 Over Voltage Output Protection: The power supply outputs should be protected against over voltage conditions with adjustable or preset crowbar limits of nominally 110% of the regulated output voltage.

3.5.5 Load Short Circuit Protection: The power supply outputs should be internally protected against short circuit loads.

3.5.6 Remote Sense: The STANAG 4575 power cable is expected to produce voltage drops in both the voltage and return wires. To offset these losses the NADSI power connectors provide remote sense pins for the +3.3V, +5.0V and +12.0V voltages and their returns. The power supplies must be capable of offsetting wiring voltage losses that are proportional to the load current, the number of wire pairs, the wire gauge (resistivity per foot) and length. See comments below on power cable length. In order to determine the required power supply remote sense capabilities it will be necessary to calculate the expected wire losses. It is recommended that power supply vendor's remote sense application notes be consulted during design of the power supply system.

3.5.7 Power Cable Length: In general wire gauge #22 is the maximum size compatible with the 37-pin 38999 connector. The 50-pin D-sub may support #20 or #18 gauge wire. It is important that all of the power wires in both connectors be populated with maximum gauge stranded copper wire. In general 19 stranding provides the lowest resistance per foot in each gauge. It is important to implement the shortest power cable that is practical, to calculate the resulting voltage drops in the cable and to ensure that the losses are within the regulation capabilities of the selected power supplies using their remote sensing. If a practical cable length cannot be met, it may be possible to use a transition cable approach with the longer length implemented with lower gauge wire (see figure C-1 below).

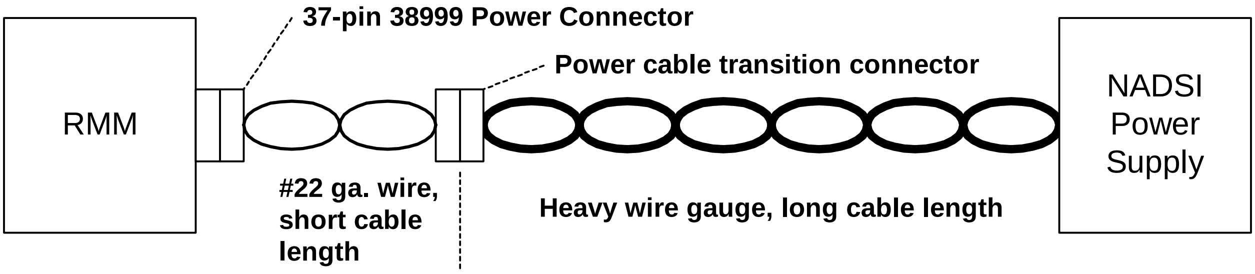


Figure C-1 - Example Transmission Cable Approach

3.5.8 Soft Start Voltage Application: In general the STANAG 4575 power supply voltages will be connected to RMM electronics containing a significant amount of bypass capacitance. It is important that the power supplies provide a “soft start” feature to insure inrush current is limited. The power supply voltages should be established with a controlled, continuously increasing voltage rise that is neither too fast nor too slow. It is recommended that each power supply transition from OFF to 90% of its regulated voltage in no less than 0.5 milliseconds under no load conditions. It is recommended that each power supply transition from OFF to 90% of its regulated voltage in no more than 5.0 milliseconds under full load conditions.

3.5.9 Power ON Overshoot: The power supply overshoot during the power ON transition should be no more than 50 millivolts for the +3.3V, +5.0V and +12.0V voltages. An overshoot of up to 500 millivolts is acceptable on the +28V voltage.

3.5.10 Power Interlock: The STANAG 4575 power connector must be fully mated to the RMM prior to the application of power to avoid damaging the unit. It is important that the power supply design properly utilize the interlock feature that has been defined for the STANAG 4575 power connectors. This interlock consists of a short circuit between two pins within the connector. The power supply design must sense a continuous short circuit between these pins for a minimum of 5 seconds before applying power. This time was arbitrarily estimated as the maximum time required to firmly attach either power connector to the RMM following initial connector contact. Any loss of interlock continuity must restart the 5-second time interval (clumsy operator provision). Should interlock continuity be lost after power has been applied to the RMM, power should be automatically disconnected immediately and only reconnected following 5 continuous seconds of continuity. Implementing this interlock will require logic within the power supply system that is separately powered.

3.5.11 Power System Protection: It is recommended that primary power source to the STANAG 4575 power supply system be protected with either a fuse or circuit breaker.

3.5.12 Power Safety: The power supply system and all of its cabling should be designed to eliminate any risk to the operating personnel.

3.5.13 Simulated RMM Load Fixture: It is highly recommended that a simple resistive load fixture be developed that can be connected to the power cable via either the 50-pin D subminiature or 37-pin 38999 connector. The power supply loads should be designed to draw the maximum currents as specified in STANAG 4575. Voltage test points should be provided for rapid measurement. This load fixture would be useful for initially verifying the operating characteristics of the NADSI power supply and as a quick safety check prior to connection to each RMM. It will be important to accurately measure each voltage at the load to ensure that the remote sense circuitry is operative.

SPECIFICATION TEMPLATE FOR ACQUISITION PLATFORM ADVANCED DATA STORAGE SYSTEM CHARACTERISTICS.

1. SCOPE.

1.1 Introduction. Introduce and name the equipment covered and state the purpose for the specification.

1.2 Functional requirements. Describe the system in moderate detail, providing component modular nomenclature and function of each module within the system.

1.3 Organization of the Specification. Describe the organization of the specification to follow.

2. Applicable or Referenced Documents. Some examples of Applicable or Referenced Documents are contained in section 4 of the Overview on page 3 of this document.

3. Requirements / Definitions

3.1 Advanced Data Storage System (ADSS) Definition. Describe the total storage system being addressed by the specification. This might include the airborne recorder with the RMM and a description of planned CONOPS. Required partitioning of the ADSS, specific RMM and native system docking requirements should be included.

3.1.1 Interface Definition and Characteristics. Describe and show by Block diagrams the various interfaces associated with program requirements.

3.1.1.1 Mechanical Interface. The mechanical interface for the RMM should be clearly defined using drawings and descriptions showing size, weight and dimensional data for all hardware and connector placement. Description of removal and insertion procedure and clearances for the RMM is described, as well as time requirements and power interlock considerations. Physical interface and accessibility as well as connect/disconnect restrictions of the NADSI high-speed download port are also described. Some of these parameters can also be covered under Physical Characteristics.

3.1.1.2 Environmental Interface.

3.1.1.2.1 ADSS Cooling Requirements. If cooling is required for the ADSS, the cooling method to be used (Conduction forced air, Conduction to liquid cooled surface, Convection, etc) should be defined with the temperature limits for which the ADSS will be able to operate clearly defined. Appropriate standards such as MIL-HDBK-5400 should be referenced here. Thermal analysis requirements and critical operating temperature ranges should be defined, as well as heater requirements for some technologies and requirements for heat transfer from a sealed RMM.

3.1.1.3 Electrical Interface. The Electrical Interface information for the high-speed download NADS 4575 port of the RMM will be taken directly from Annexes B & C of STANAG 4575. The information below is guidance for preparing specifications defining the electrical interfaces between the aircraft and the ADSS.

3.1.1.3.1 Power Interfaces. Typical parameters that should be specification items include:

1. Total power consumption including heaters if used. Specifications on power dissipation levels at various modes or data rates may also be required.
2. Main input power requirements such as voltages, currents, frequency and phase if AC, and transient tolerances with references to appropriate standards such as MIL-STD-704.
3. Protective devices required such as fuses, transient voltage suppressors and thermal cut off switches.

4. Power Interrupt requirements such as how long the unit should continue to operate when input power drops below the required level.

5. Power control, power interlock, sequencing instructions and power up current profile are also found in some specifications to meet specific program requirements.

3.1.1.3.2 Control / Status Interface. Specifications for the Control and Status interfaces should list all protocols that will be used (e.g. MIL-STD-1553, RS-422, RS-232, SCSI over Fibre Channel, etc.) and the order of desired preference. If there is an override preference between the STANAG 4575 and the commands on the ADSS bus, it should be so indicated. The Control bus protocol, control commands, status messages and error-handling protocol should be clearly defined. Non-interference requirements between the native and NADSI interface should be identified.

3.1.1.3.3 Data Interfaces. The Data Interface specification should clearly define the number of data interfaces and kind and number of ports for each. For example, two separate data input interfaces and two or more separate data output interfaces may be required. Additional capabilities to consider might include:

1. The capability to map a certain portion of the memory capacity to one particular input port or the ability to restrict that mapping such that the memory capacity will not be pre-assigned to a specific input port.
2. The capability for all output ports to access all previously recorded data.
3. The capability of operating input and output ports at independent data rates.
4. Simultaneous record and playback capability.
5. Simultaneous independent record and data file recovery.
6. Individual file recovery and replay.
7. Data flow control.
8. Event marking.
9. Time stamping.

The capability to record/reproduce data via the NADSI interface as the primary interface to the recorder should be considered.

3.1.1.3.3.1 Input Data Interface and Data Rate. The input data interface protocol should be clearly defined (SCSI, Fibre Channel, DCRsi eight bit parallel, etc.) with references provided to appropriate standards. Interface connectors should be clearly defined with part numbers, diagrams and tables defining pin-outs and associated signal names.
Data Rates for each of the input interfaces should be specified independently for maximum capability as well as capability when operating simultaneously with the other input interfaces. The method or command by which the data rate for the interfaces is controlled should also be specified here.

3.1.1.3.3.2 Output Data Interface and Data Rate. The output data interface should also be clearly defined as to types and protocols to be used, providing references to appropriate standards. Interface connectors should be clearly defined with part numbers, diagrams and tables defining pin-outs and associated signal names. The capability for selective and general dubbing of data to external equipment should be specified if required.

Data Rates for each of the output interfaces should be specified independently for maximum capability as well as capability when operating simultaneously with the other output interfaces. The method or command by which the data rate for the interfaces is controlled should also be specified here. If required, the rate for dubbing should be specified here.

3.2 Characteristics.

3.2.1 Performance.

3.2.1.1 Non-Volatility. In the first NADS TST meeting, the group accepted that non-volatile storage was to be used in principle. Nonvolatile (sometimes written as "non-volatile") storage (NVS) can be implemented using a large number of different memory technologies. These include semiconductor, optical, magneto-optical, and magnetic memories. In this section, the author would define the length of time that implies non-volatility, any restriction on the techniques that can be used to provide this function (such as acceptability of batteries), and the requirements for proper erasure of the storage media. Since non-volatility can be influenced by environmental conditions, storage and transportation of NVS media should also be addressed.
Note – Declassification is addressed separately in AEDP-3.

For some data storage media types there may be as many as three non-volatility specifications:

1. The length of time that recorded data must be accurately retained in memory when used in the normal operational scenario. This time could range from hours to years and the data must be fully recoverable at the original error rate. The media storage environment, conditions and handling should be specified, which may include intermittent operation (or the inability to operate) of the memory element (such as for disk or tape) or for checking or changing batteries.
2. The minimum write/re-write cycles that allow full retention of the data and provide the full memory capacity originally specified. The number of write/read/erasure cycles can affect both the error rate and the retention of user data. In addition, some portions of the memory may be re-written much more often than others, causing data loss earlier than the bulk of the memory unit. These issues must be considered when specifying the time over which the NVS requirement must be maintained for all memory elements.
3. As portions of the memory become defective, remapped or unreliable over time, volatility becomes dependent on data location within the memory and the overall memory capacity is reduced. In time, the Non-memory portions of the system can contribute significantly to memory loss or become the dominant failure mode. The system/media operational lifetime over which the NV requirement must be maintained should be specified based on the overall performance and capacity requirements.

3.2.1.2 RMM Capacity. Required user data storage capacity for the RMM should be specified in this section. Since capacity of memory modules in Advanced Data Storage systems is constantly increasing, users may elect to specify current minimum acceptable memory capacity with design goals for future growth and acceptable upgrade methods. For example upgrades may exclude any mechanical, electrical or software/firmware redesign and allow growth only by adding additional memory. (There is a difference in usage of the capacity multipliers commonly used to define memory. Traditional mass memory devices have defined “megabyte” to mean 10^6=1,000,000. Computer system memories usually are stated in terms of a “megabyte” as meaning 2^{20}= 1,048,576. To avoid ambiguity, the specification should clearly state which of these applies to this procurement.) In terms of STANAG 4575, megabytes refers to 10^6 bytes.

Data storage technologies using portions of the user data space to perform “circular buffer” operation, where the recorder automatically over-writes the “oldest” mission data when its storage capacity is reached, then users should specify the minimum amount of mission data that must be retained in this mode of operation.

3.2.1.3 Time.

3.2.1.3.1 Access Time. Access time is that time from when a command is issued until the actual operation begins. It should be specified precisely for both write and read operations, in order to clearly define the requirements and permit later verification of compliance. The access time needs to be measured over a broad range of data addresses that are possible to be accessed and should be specified as a minimum, maximum and average measured value. It is usually important to be aware of the events in the timeline of the interface to the data storage system, however, the access time is an overall value, which includes all steps in a write or read operation.

3.2.1.3.1.1 Read Access Time. Read access time is the time from the transmission of the last byte of the command to access data until the time that the first byte of data has been transferred to the host. Average and maximum times should be specified.

3.2.1.3.1.2 Write Access Time. Write access time is the time from the transmission of the last byte of a command to write data (or a file) to the data storage device, until the time that the first byte of data is written (i.e. when the write operation begins) on/in the media. Average and maximum times should be specified.

3.2.1.3.1.3 Access Time Verification. Compliance to the specification for the read and write access times should be verified. This measurement includes the complete end-to-end time to initiate and begin the operation, regardless of intermediate steps. Care should be taken to use data addresses for this testing that are representative of the entire memory span and that the sequence of test addresses includes the full range of adjacent and distant addresses.

3.2.1.3.2 Startup Time. Startup time is considered to be the minimum time required for the storage device to accept all supported commands from the time when power is applied, assuming the drive temperature is within the operating range. Additional requirements for temperature extremes should also be inserted here, if applicable. . Startup time includes booting the recorder's software, performing its Operation Readiness Test (ORT), enabling Periodic Built In Test (PBIT) and entering the Initialized mode (ready for host commands over either its native or NADSI control interface.

3.2.1.3.3 Erasure Time. Some data storage technologies such as solid-state Flash memory require erasure before they can be re-written with new mission data. The recorder specification should identify the time allowed to perform bulk erasure of the RMM between missions. Declassification of mission data is discussed in AEDP-3. Applications requiring erasure of individual record sessions or files should provide guidance on the minimum and maximum amount of data expected to be recorded in a single session or file and the associated erasure time.

3.2.1.4 Modes of Operation – The method for selection of the modes of operation by the host system should be specified, e.g. by the control/status interface or by front panel, etc. One could also specify mode interdependencies and mode change times in this section. Some typical Modes of Operation that could be specified and example definitions and/or requirements are presented below in 3.2.1.4.1 thru 3.2.1.4.8.

The use of the term "Mode" is only descriptive. For example, there is not required to be either an "Initialize Mode" command issued by a system controller or an "Initialize Mode" response issued by an ADSS. The behaviors and responses associated with these modes are common and need to be considered in procurements, controlled by specifications, and defined in interface control documents. The recorder acquisition program may require:

1. Either strict adherence (emulation) to or compatibility with an existing recorder control protocol (minimize host software changes).

2. Use of an existing control protocol with specified enhancements to support new operational capabilities.

3. Definition of the recorder's required operational modes, functional capabilities and status reporting, allowing the ADSS supplier to tailor a custom control protocol to the application.

The recorder's control protocol should be fully documented in an Interface Control Document that defines the interface, protocol, operating modes and mode transitions. The recorder may be required to provide separate control and maintenance interfaces, each with their own protocol and operational modes.

3.2.1.4.1 Off Mode. The ADSS will be in the "OFF" mode when power is not applied.

3.2.1.4.2 Initialize Mode.

1. The Initialize mode will include the following functions:

   a. Application of Power
   b. ORT
   c. Initialization of the ADSS internal bus
   d. Initiation of thermal stabilization and continued thermal stabilization of the ADSS.
   e. PBIT

2. The Initialize mode will be entered automatically when input power is applied to the ADSS or when commanded by the host system.

3. Upon application of input power to the ADSS, it will automatically perform ORT and PBIT .

4. As a goal in this mode, the ADSS will minimize power consumption (e.g., operate only those circuits necessary for communication with the host system, power-supply control, BIT or heaters).

5. Means should be provided for the system controller to determine that the ADSS is initializing and not yet ready to respond to functions associated with the Operate Mode.

3.2.1.4.3 Operate Mode. A large number of different possible functions can be implemented to perform the processes of storing and retrieving data with an ADSS. The specific functions chosen should be selected that are appropriate for the overall system architecture that is being implemented. Specific examples of functions that could be used to implement the four possible architectural approaches described in section 2 of Annex C are provided in the sections below.

3.2.1.4.3.1 Legacy Tape Emulation Functions. Rotary magnetic tape recorders have historically been used in many Intelligence, Surveillance, and Reconnaissance (ISR) applications. These recorders write wideband mission data in transverse or helical tracks along a ribbon of magnetic tape housed in a removable cassette or cartridge. Longitudinal tracks along the edge of the tape may be written with additional low rate data that may be either played back along with the wideband data or used to search the tape for particular areas of interest. Advanced Data Storage Systems (ADSS) may be retrofitted into legacy magnetic tape recorder applications to gain advantages of their lower size, power and weight and improved reliability and environmental ruggedness. In these applications it may be required that the ADSS exactly emulate the previously used magnetic tape recorder in its interfaces, modes of operation and control protocol. In such cases it is important to supply hardware and control protocol Interface Control Documents (ICD) for the legacy magnetic tape recorder that define these details for the ADSS supplier. Figure C-1-1 provides a sample interface diagram for a typical application of an ADSS configured for Tape Recorder Emulation.

When emulating legacy magnetic tape recorders the ADSS must support data "record" or "play" modes. Due to the sequential access mode of magnetic tape, a simultaneous record and play mode is not supported, however, some tape emulators add enhanced features beyond the normal capabilities of tape systems. Typically the recorder supports only a single wideband record and a single wideband playback interface. Magnetic recorders generally implement dedicated record and playback data interfaces using 8-bit data word widths and differential emitter coupled logic (DECL) drivers and receivers. These data interfaces generally provide special signals that allow the host system to control the data that is recorded on a byte-by-byte basis and to control the flow of playback data (e.g.: in data link or on board review applications).

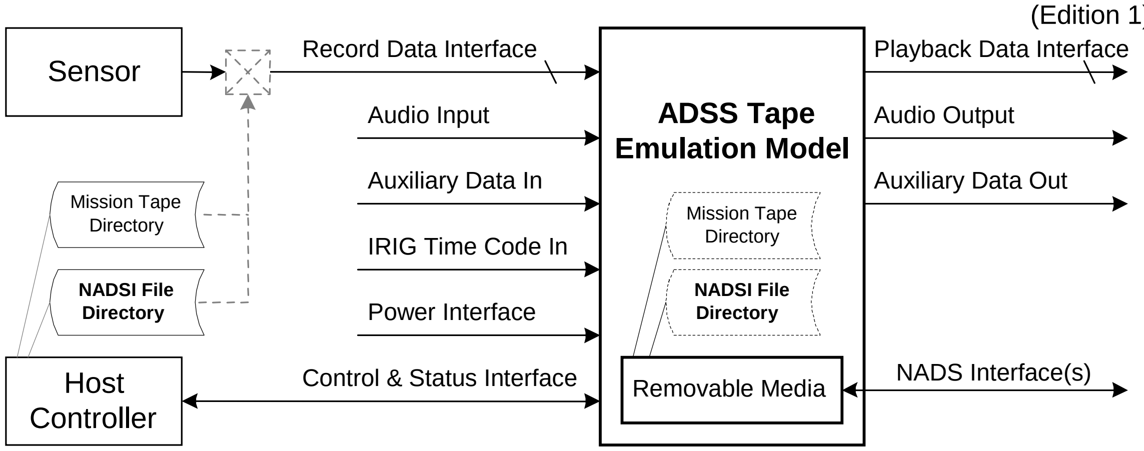


Figure C-1-1 - ADSS Tape Emulation Model

With magnetic tape emulation, the recorder is responsible for accepting record data and placing the data in logically sequential memory locations defined by the ADSS. Magnetic recorders generally support host queries for the current tape position during record (e.g.: current track set ID (TSID) or scan block) so that an external tape directory can be generated. In many legacy applications the detailed mission tape directory is downloaded to tape over the wideband record data channel at the end of the airborne mission. Supporting a NADSI compliant file directory in magnetic tape emulation mode would require either the ADSS to internally generate one or the external host to generate one and download it at the conclusion of the mission.

An attempt to show these optional techniques for the directory generation is provided in Figure C-1-1. The case where the directory is internally generated by the ADSS is depicted by the “NADSI File Directory” shown within the ADSS Tape Emulation Model block. The case where the directory is generated by the external host/RMS and written to the recorder through its normal Record Data Interface is depicted by the “NADSI File Directory” shown in the left hand side of the figure going to the normal Record Data Interface. The dashed lines and box were meant to indicate a method of time multiplexing between the host held file directories and sensor data being applied to the ADSS Record Data Interface.

Longitudinal tape channels are frequently used to record data such as voice annotation, time code, platform data, event marks, rotary head scan number, etc. These channels may be used to search for specific wideband data segments of interest. Alternately the recorder may provide a tape footage counter used to locate data segments. Magnetic tape requires erasure before reuse. However erasure heads are generally implemented within the tape transport and are automatically energized during Record mode such that a separate Erase command is not required. These recorders may also support standard avionics test modes such as Operation Readiness Test (ORT), Periodic Built-In Test (PBIT) and Initiated Built-In Test (IBIT) although much of the provided status is associated with tape transport mechanisms which may not apply to the ADSS.

Primary operational commands for magnetic tape emulation ADSS include: Record, Play, Stop, Fast-Forward, Rewind and Search. The following sections provide recommended requirements for these modes.

3.2.1.4.3.1.1 Record Function. The ADSS will record user data at a host controlled data rate. The record command will be rejected (with cause) if the installed RMM is write-protected. The ADSS will be able to sustain recording at data rates up to the maximum specified rate. If record data will be provided in bursts, the peak input data rate should be clearly defined. The ADSS will provide a “Record” status indication to the host system over the control/status interface in accordance with the ICD.

3.2.1.4.3.1.2 Play Function. The ADSS will playback the previously recorded data requested by the host system. A host system may request either playback of a specific data segment or playback starting from a specific memory location. Only the data requested by the host system will be outputted. The playback data rate will be controlled by the host and will support data rates up to the maximum specified. Requirements for the ADSS to support playback data flow control mechanisms should be stated. The maximum time between the play command and the ADSS beginning to output the requested data may be specified. The ADSS will provide a “Play” status indication on the control/status interface to the host system in accordance with the ICD.

3.2.1.4.3.1.3 Stop Function. This function is invoked to end any of the other functions, e.g., record, play, fast-forward, rewind or search. This function may also be used to return the system to the Operate mode, where the ADSS is ready to accept new functional commands.

3.2.1.4.3.1.4 Auxiliary Channel Function. Requirements for record and playback of other channels such as voice annotation, time code, platform data, event marks, rotary head scan number, etc. should be clearly stated. Requirements for these tracks to be readable during playback or simulated fast-forward, rewind or search modes should also be clearly stated.

3.2.1.4.3.1.5 Fast-Forward, Rewind and Search Function. The legacy approach for positioning tape for playback of a particular data segment should be clearly defined. This is particularly important if external equipment such as a time code reader is used in the tape positioning control loop. If Search commands will be issued that contain parameters such as time code, TSID or scan blocks this should be clearly stated.

3.2.1.4.3.1.6 File Directory. Detailed requirements for both the legacy mission file directory and the NADSI file directory should be provided. For directories generated external to the ADSS the methods for extracting ADSS record addresses and for eventually storing the directory on the ADSS media should be provided. If the NADSI file directory is to be generated by the ADSS the method of providing individual file entry annotation (file name, create data, create time, etc.) should be defined.

3.2.1.4.3.2 Intelligent Peripheral. When the application is not restricted to emulating a legacy magnetic tape recorder, the ADSS can take full advantage of its advanced data storage media to offer expanded mission record and playback capabilities. Figure 3.2-2 shows a general block diagram of the ADSS Intelligent Peripheral configuration. One key attribute of this architecture is that the random access memory can be configured to support multiple concurrent record and playback data interfaces. Such a recorder can support recording from multiple input sensors while playing back mission critical data to a data link or to an onboard reviewer’s display. In general each record and playback interface will support its own clock source and data flow control signals to support completely independent operation. The ADSS bulk memory can also be user allocated on a mission to mission basis to best suit the individual mission profile. In general the recorder assigns addresses for all recorded data and supports playback data requests using the logical block addressing mandated by the NADSI SCSI control protocol. This architecture provides the recorder “intelligence” required for generating the NADSI file directory with either default file annotation or host annotation of files through an expanded control protocol. Figure C-1-2 shows the NADSI File Directory being generated internal to the ADSS with the support of commands from the external host/RMS (supply file name, time, date). A separate host/RMS generated mission file directory is shown time multiplexed over the native Record Data Interface.

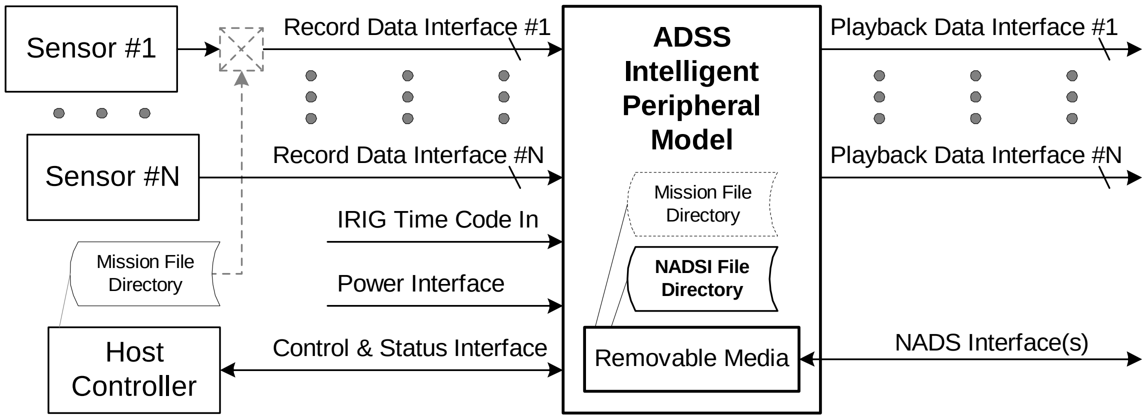


Figure C-1-2 - ADSS Intelligent Peripheral Model

Similar to the Tape Recorder Emulation model, the Intelligent Peripheral provides separate data and control interfaces. This allows the record data interfaces to be connected directly to the mission sensors, radar system or data compression suite without additional data buffering or multiplexing. The ADSS may also accept auxiliary inputs such as IRIG time code, event marks, voice annotation or platform data for recording or time-stamping the sensor data. These recorders support standard avionics test modes such as ORT, PBIT and IBIT. The Intelligent Peripheral architecture also facilitates placement of the NADSI mandated Fibre Channel interface (with its software) on the removable memory unit.

Primary operational commands for intelligent peripheral include: Record, Stop Record, Play, Stop Play, Erase and File Directory request. The following sections provide recommended requirements for these modes.

3.2.1.4.3.2.1 Record Function. The Intelligent Peripheral ADSS Record (Write) command may provide parameter fields to allow independently initiating a record operation on any of its multiple record data interfaces. The ADSS will record user data at a host controlled data rate. The record command will be rejected (with cause) if the installed RMM is write-protected. The ADSS will be able to sustain recording at data rates up to the maximum specified rate. If record data will be provided in bursts, the peak input data rate should be clearly defined. The ADSS will provide a “Record” status indication to the host system over the control/status interface in accordance with the ICD.

3.2.1.4.3.2.2 Play Function. The Intelligent Peripheral ADSS Play (Read) command may provide parameter fields to allow independently initiating a playback operation on any of its multiple playback data interfaces. The ADSS will playback the previously recorded data requested by the host system. A host system may request either playback of a specific data segment or playback starting from a specific memory location. Only the data requested by the host system will be outputted. The playback data rate will be controlled by the host and will support data rates up to the maximum specified. Requirements for the ADSS to support playback data flow control mechanisms should be stated. The maximum time between the play command and the ADSS beginning to output the data may be specified. The ADSS will provide a “Play” status indication on the control/status interface to the host system in accordance with the ICD.

3.2.1.4.3.2.3 Simultaneous Record and Playback Function. Applications requiring simultaneous record and playback operation should specify the maximum data rates required in each operation. The required proximity of the playback data in ADSS memory to the on-going record data process should also be stated. If multiple channels are configured, specifications should clearly state the record / replay requirements of each. For instance, if multiple record channels are to be replayed through a single play channel, specifications should clearly state the record / replay requirements of each possible combination.

3.2.1.4.3.2.4 Stop Record Function. An ADSS providing multiple record data interfaces or a simultaneous record and playback function requires a Stop Record command so that the host can specify the exact function to be terminated.

3.2.1.4.3.2.5 Stop Play Function. An ADSS providing multiple play data interfaces or a simultaneous record and playback function requires a Stop Play command so that the host can specify the exact function to be terminated.

3.2.1.4.3.2.6 Erase Function. An ADSS using solid state Flash memory may require a separate bulk erasure mode to prepare the memory for the next mission.
(Note: ADSS declassification is addressed in AEDP-3.)

3.2.1.4.3.2.7 Auxiliary Channel Functions. Requirements for record and playback of other channels such as voice annotation, time code, platform data, event marks, rotary head scan number, etc. should be clearly stated. Special requirements such as time-stamping sensor data should also be clearly defined.

3.2.1.4.3.2.8 File Directory. If the application will be generating a mission file directory external to the recorder, an approach should be specified for determining the ADSS assigned record addresses and for eventually storing the directory to the ADSS. The method of providing individual file entry annotation (e.g.: file name, create data, create time, etc.) for the recorder's NADSI file directory should be defined if the specified default parameters are not acceptable.

3.2.1.4.3.3 DASD Functions. A direct access device is always given the specific addresses at which all data is to be accessed from. A data access command, such as “read” or “write” from the system controller specifies both the starting address as well as the number of memory addresses to be read or written. Because this type of ADSS does not interface directly to the sensors, the number of channels of sensor data and their types are not directly defined by the ADSS. The system controller conveys sensor data with “read” and “write” commands. The data associated with these commands can come from any type or combination of sensors. Also, a DASD device permits “read” and “write” commands to occur in any sequence and to access any region of memory. The tradeoff of this flexibility in handling arbitrary sensor data is that the system controller must be more complex than that of a tape emulation type of ADSS and any required signal conversion or signal processing must be performed outside of the ADSS. Figure C-1-3 provides an interface diagram for an ADSS configured as a DASD.

3.2.1.4.3.3.1 Read Function. The ADSS will accept “READ” commands in accordance with the protocol selected for use (e.g., SCSI).

3.2.1.4.3.3.1.1 Read Data Rate. The procuring authority specifies the channel rate (its intrinsic data carrying capability) directly by specifying the channel type. The host controls the data transfer rate by the rate at which it issues data access commands. The procuring authority specifies the transfer rate the media must support by defining the characteristics of the read data rate.

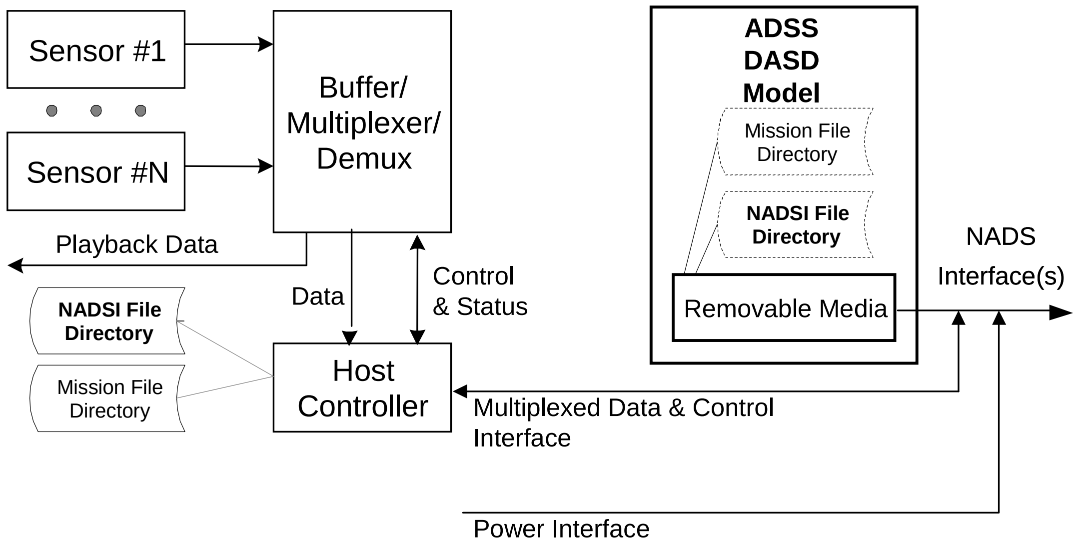


Figure C-1-3 - Interface Diagram for DASD Configured ADSS

The ADSS will transfer data through its system interface at a burst rate equal to the capacity of the required channel type. It will be capable of a minimum sustained transfer rate of “X” megabytes per second measured for a total transfer of “Y” megabytes with individual read transfers greater than “Z” kilobytes per transfer. The minimum size of each transfer needs to be specified so as to make sure that efficient use is being made of the data channel and that the required performance is a measure of the ADSS and not of the channel itself. The total transfer size needs to be specified in order to quantify the meaning of the word “sustained” in the transfer rate specification. It may also be necessary to specify that read cache memory is not to be used by the ADSS when measuring this data rate so that the measurement correctly reflects the intrinsic media capabilities.

The DASD type of ADSS understands only blocks of data, not files; therefore it is not necessary or possible to specify “file-handling” performance.

The previously specified access time measurement, combined with the Read data rate will allow for system performance predictions to be made.

3.2.1.4.3.3.2 Write Function - The ADSS will accept “WRITE” commands in accordance with the protocol selected for use (e.g., SCSI).

3.2.1.4.3.3.2.1 Write Data Rate. The procuring authority specifies the channel rate (its intrinsic data carrying capability) directly by specifying the channel type. The host controls the data transfer rate by the rate at which it issues data access commands. The procuring authority specifies the transfer rate the media must support by defining the characteristics of the write data rate.

The ADSS will transfer data through its system interface at a burst rate equal to the capacity of the required channel type. It will be capable of a minimum sustained transfer rate of “X” megabytes per second measured for a total transfer of “Y” megabytes with individual write transfers greater than “Z” kilobytes per transfer. The minimum size of each transfer needs to be specified so as to make sure that efficient use is being made of the data channel and that the required performance is a measure of the ADSS and not of the channel itself. The total transfer size needs to be specified in order to quantify the meaning of the word “sustained” in the transfer rate specification. It may also be necessary to specify that write cache memory is not to be used by the ADSS when measuring this data rate so that the measurement correctly reflects the intrinsic media capabilities.

This type of ADSS understands only blocks of data, not files; therefore it is not necessary or possible to specify “file-handling” performance.

The previously specified access time measurement, combined with the Write data rate will allow for system performance predictions to be made.

3.2.1.4.3.4 File Server Functions. A File Server device accepts data access commands, such as “read” or “write” from the system controller over a network interface. Unlike a DASD device, a file server uses these commands with a reference to a file identifier and a block offset into that file. This combines some of the features of tape emulation and of a DASD device. Like a tape emulation ADSS, a file server does not need to convey actual data address locations to the system controller in order to function. And, like a DASD device, the system controller does know exactly where it put all of its data, but it knows those locations only at a higher level of abstraction. This type of ADSS does not interface directly to sensors, therefore number of channels of sensor data and their types are not directly defined by the ADSS. The system controller conveys sensor data with “read” and “write” commands. The data associated with these commands can come from any type or combination of sensors. Also, a File Server device permits “read” and “write” commands to occur in any sequence and to access any file in memory. The tradeoff of this flexibility in handling arbitrary sensor data is that the system controller must be more complex than that of a tape emulation type of ADSS and any required signal conversion or signal processing must be performed outside of the ADSS. Figure C-1-4 provides an interface diagram for an ADSS configured as a File Server.

A file server has the advantage of being easily shared by more than one system controller. The permissions for read and write access to various files can be used to prevent one system controller corrupting another controller’s data.

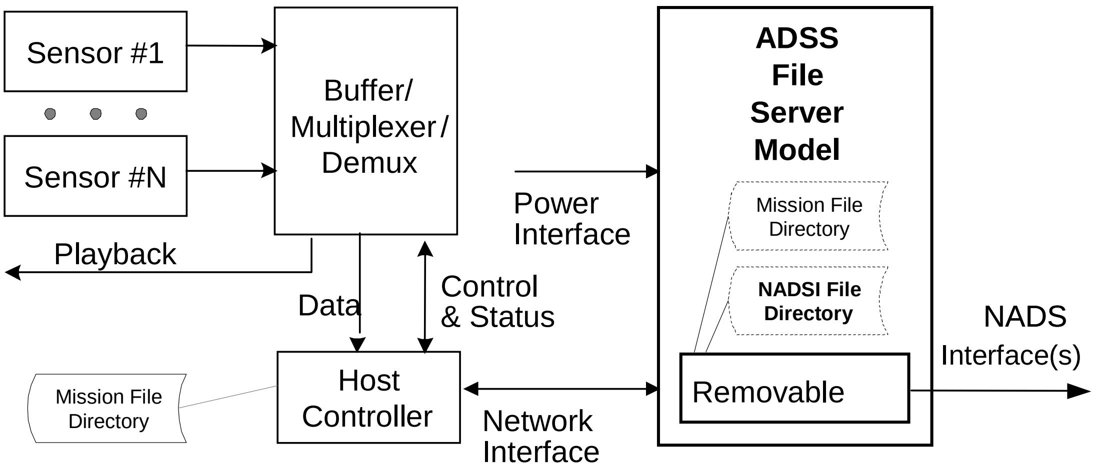


Figure C-1-4 - Interface Diagram for File Server Configured ADSS

3.2.1.4.3.4.1 Read Function. The ADSS will accept “READ” commands in accordance with the protocol selected for use (e.g., NFS over TCP/IP on Fibre Channel).

3.2.1.4.3.4.1.1 Read Data Rate. The procuring authority specifies the channel rate (its intrinsic data carrying capability) directly by specifying the channel type. The host controls the data transfer rate by the rate at which it issues data access commands. The procuring authority specifies the transfer rate the media must support by defining the characteristics of the read data rate.

The ADSS will transfer data through its system interface at a burst rate equal to the capacity of the required channel type. It will be capable of a minimum sustained transfer rate of “X” megabytes per second measured for a total transfer of “Y” megabytes with individual read transfers greater than “Z” kilobytes per transfer. The minimum size of each transfer needs to be specified so as to make sure that efficient use is being made of the data channel and that the required performance is a measure of the ADSS and not of the channel itself. The total transfer size needs to be specified in order to quantify the meaning of the word “sustained” in the transfer rate specification. It may also be necessary to specify that read cache memory is not to be used by the ADSS when measuring this data rate so that the measurement correctly reflects the intrinsic media capabilities.

This type of ADSS understands only blocks of data associated with files; therefore it is necessary to specify “file-handling” performance. This includes the number of different files that can be “open” for access at any one time, and the time delay for gaining first access to a file.

The previously specified access time measurement, combined with the Read data rate will allow for system performance predictions to be made.

3.2.1.4.3.4.2 Write Function. The procuring authority specifies the channel rate (its intrinsic data carrying capability) directly by specifying the channel type. The host controls the data transfer rate by the rate at which it issues data access commands. The procuring authority specifies the transfer rate the media must support by defining the characteristics of the write data rate.

The ADSS will transfer data through its system interface at a burst rate equal to the capacity of the required channel type. It will be capable of a minimum sustained transfer rate of “X” megabytes per second measured for a total transfer of “Y” megabytes with individual read transfers greater than “Y” kilobytes per transfer. The minimum size of each transfer needs to be specified so as to make sure that efficient use is being made of the data channel and that the required performance is a measure of the ADSS and not of the channel itself. The total transfer size needs to be specified in order to quantify the meaning of the word “sustained” in the transfer rate specification. It may also be necessary to specify that write cache memory is not to be used by the ADSS when measuring this data rate so that the measurement correctly reflects the intrinsic media capabilities.

This type of ADSS understands only blocks of data associated with files; therefore it is necessary to specify “file-handling” performance. This includes the number of different files that can be “open” for access at any one time, and the time delay for gaining first access to a file. The time to create a single file and the file creation rate should both be specified.

The previously specified access time measurement, combined with the Write data rate will allow for system performance predictions to be made.

3.2.1.4.4 Terminate Mode. A Terminate mode may be required by the ADSS that must perform overhead functions prior to removing power. In the terminate mode, the ADSS could perform all overhead functions (e.g., transfer of internal ADSS directory information from volatile to non-volatile storage, storage media releases, ADSS door actuators, etc.) required prior to power removal, prior to physical removal of the Removable Memory Module from the Interface Unit, and/or prior to download of the recorded data through the STANAG 4575 defined interface. The ADSS could also perform PBIT functions during this mode. The ADSS should provide a positive “Terminate” status indication on the control/status interface to the host system in accordance with the ICD.

3.2.1.4.5 Declassify Mode. Declassification is a decision process that relies on the capability to perform a number of technical and procedural steps related to the storage media. Guidance and details for technology specific approaches are provided in AEDP-3.

3.2.1.4.6 Format/re-Initialize Mode. If the RMM requires Formatting or re-Initialization subsequent to Power-up Initialization for any reason, requirements for that mode would be included here. These requirements could include: authority for re-initialization, time allowed, modes of operation affected and effected, and positive status indications to host including memory space available. Cautions may also be expressed here e.g., “the RMM will not routinely require formatting or re-initialization prior to re-use”.

3.2.1.4.7 Host Initiated BIT Mode (IBIT). This mode is used to extensively test the ADSS functions by using fault-detection and fault-isolation tests that are not possible during PBIT and require interruption of the normal system operation, including recording and playback of internally generated data or that require operator intervention.

3.2.1.5 Bit Error Rate (BER). The Bit Error Rate should be specified for the playback of the RMM stored data through any ADSS-to-host interface or via the STANAG 4575 defined interface. The BER specified should apply to all defined operating environmental conditions and apply to the RMM using new, erased or declassified previously recorded media. The BER should also be specified for Crossplay in both directions between all Interface Units and all memory modules. The BER is directly applicable to user's data, regardless of any processing or conversions performed internal to the ADSS or RMM.

3.2.1.5.1 Seek Error Rate. Seek Error Rate is unique to RMMs with electromechanical positioning and is usually specified as one addressed track positioning error in a given number of seeks.

3.2.1.6 Functional Requirements.

3.2.1.6.1 ADSS Initialization. This specification section should provide requirements for the initialization of the ADSS such as:

1. When it must initialize, e.g. upon power-up, upon receipt of a System Reset command.
2. How long it should take to initialize the "state" or "mode" the ADSS should transition to when it has finished initializing, e.g. the Initialized mode.
3. What recorder self-tests must be performed during recorder initialization, e.g. ORT.
4. What recorder status should be available following initialization, e.g. ORT, PBIT.
5. Any other special requirements, e.g. that the ADSS should be able to initialize with or without the RMM in the system as required.

A NADSI compliant recorder must support download of mission data when its standalone RMM is powered through its NADS Interface (scenario #2; see Annex A, par. 2.4). Therefore the recorder's RMM, when powered by the NADS Interface, must automatically initialize into a mode enabling its NADSI fibre channel data/control interface.

A NADSI compliant recorder must also support download of mission data when mounted to its IU within the aircraft and powered by the aircraft (scenario #3). Therefore the recorder must support commands through its normal airborne control interface that enable the recorder's NADSI fibre channel data/control interface to be the priority data and control interface. This could be a System Reset command from the airborne host that initializes the recorder and allows it to "discover" the active control interface (native or NADSI) or a command could be issued to the recorder to activate the NADSI port. Cycling aircraft power to the ADSS may also enable NADSI in scenario #3.

To avoid data corruption, the airborne host should not issue further commands to the recorder that could cause alteration of the contents of the RMM memory during NADSI port operations. To maintain optimum download speed, consideration should be given to the commands that are issued by the airborne host to the recording system during NADSI operation.

3.2.1.6.2 Data Access. This section of the specification should clearly delineate the responsibility for creating and recording the directory and establishing the NADSI file structure within the RMM. The nature of advanced data storage systems allows the storage architecture to vary from system to system and technology to technology. In the case where the RMM is a memory element only, incorporated into the airborne host system (e.g. the RMS) as compared to being the recorder itself (e.g. the ADSS), additional burdens are placed on the system to assure proper directory and file structure implementation in accordance with NADSI requirements for subsequent data access. This section of the specification should define how the mission data is inserted in files and the NADSI directory is created and stored (i.e. the data is organized and cataloged) in the RMM. Two alternative approaches to accomplish this are:

1. The NADSI File Directory may be created by the airborne host system external to the RMM and recorded in the RMM for use during subsequent file download via the NADSI port. This approach will require the system to operate with the RMM to assign file locations for the RMM. These file locations will then be recorded in the directory data.

2. The airborne host may issue record/write commands to the ADSS and could transmit the data files directly to the ADSS, which takes the responsibility for NADSI compliance. The ADSS would store the data in the NADSI files in the RMM and then create the directory, which incorporates the file locations. The NADSI directory is then stored in the RMM. The host can query the ADSS to determine where the data is written or extract the whole directory.

3.2.1.6.2.1 Data Access Notes. The RMM's file directory and the file structure is an essential part of allowing efficient ground/shipboard data access. There are additional capabilities inherent in the advanced data storage technologies that are enhanced by the directory and file structure. The specification of the airborne system should not inhibit these capabilities. The following should be considered:

1. The recorder supports auxiliary channels for recording time code, event marks, scan block IDs, etc. which are used to identify playback data of interest.

2. For an ADSS with multiple RMMs, an explanation of the expected operation of the system in the event of a single RMM failure or the use of only one RMM should be defined.

3.2.1.6.3 Write Protect. It may be desirable to incorporate a write-protect feature for the removable memory module to prevent inadvertent media erasure or overwrite. In addition, where applicable to the device type, it may be desirable for the host system to have the capability to command that individual files are write protected or the capability to override write protect of individual files.

3.2.1.6.4 Time Stamping Data. If data time stamping is required, the method (e.g.: time correlated auxiliary track, formatted in with data, etc.), the clock source (recorder external (IRIG/GPS) or internal (settable RTC)) and the time precision and periodicity should be specified.

3.2.1.6.5 Built-In-Test (BIT). The ADSS system should incorporate a minimum Built-In Test (BIT) capability as defined in this section. The purpose of this BIT capability is to determine the operational suitability ability of the ADSS and any connected RMM(s) and to perform fault detection/isolation. BIT functions could also be used to provide information to allow the system to establish and implement degraded modes of operation. BIT functions are normally organized as Operational Readiness Test (ORT) BIT, Periodic BIT (PBIT), and Initiated BIT (IBIT). Additional BIT capability can be defined in the system procurement specification for the specific application.

The RMM must be inserted into the ADSS system in order to test the performance of any RMM dependent BIT function. All RMM(s) should be capable of supporting BIT when more than one RMM is installed in the ADSS system.

The ADSS should be able to test those functions that are not dependent upon the presence of an RMM and report appropriate status when an RMM is not present.

Built in Test or BIT should accomplish failure detection and isolation without the assistance of support test equipment.

3.2.1.6.5.1 Minimum BIT. As a minimum, the ADSS should be capable of performing a test of its own basic operation, whether or not an RMM is present or functional. The ADSS BIT should also be able to determine the presence of RMM(s) and their status.

BIT or other system functions should be provided to identify status information such as usable capacity of RMM memory, and to support modifications to error management parameters such as numbers and types of retries, and locations of defective media areas- as is appropriate to the media and the system.

3.2.1.6.5.2 BIT Performance. The specification should provide BIT performance levels by indicating what percentage of ADSS functional failures should be detected for each type BIT and it should also specify a maximum percentage for false failure detection. For example:

1. For Initiated BIT, fault detection of at least X% of all faults. For Periodic BIT, fault detection of at least Y% of faults that affect the equipment performing current mission functions.
2. For Initiated BIT, fault isolation to a line replaceable assembly for at least U% of detected faults.
3. For Initiated BIT, the false alarm rate (percentage of BIT fault reports subsequently determined to be erroneous) will not exceed V%. This will be achieved by carefully screening out failure indications caused by transients. A false alarm is defined as a fault callout where no fault exists. BIT failure reports due to cables, wires, harnesses, etc., not located within a line replaceable assembly are not considered false alarms.
4. It is desirable to provide a wraparound capability so that failures in equipment interfaces can also be detected and isolated without auxiliary test equipment external to the aircraft.

3.2.1.6.5.3 Operational Readiness Test (ORT). The ORT is an automatic test at start-up that verifies that all functions, such as power supplies, clocks and connections are proper and operating. It would be used for confirming the operational capability of the equipment status when the equipment enters the "ON" state.

1. ORT BIT will include the testing of all WRA(s) circuitry and the equipment backplane(s).
2. ORT BIT will be performed whenever input power is reapplied to the equipment.
3. ORT BIT duration should be specified.

ORT should also verify the presence and functionality of any connected RMMs. It should verify that each RMM is operating, providing the available memory capacity and should verify the ability to read and write data**.** It could also detect and report if there are any problems with identifying error blocks that have been masked. The ORT may be accomplished in multiple steps rather than at initial start-up if required, e.g., if no RMM is present -or ready- at initial power-up.

3.2.1.6.5.4 Initiated BIT (IBIT). The IBIT should perform a full comprehensive test that includes a determination of the available memory. Initiated BIT will include the full complement of WRA tests and backplane tests that can be performed while the equipment is installed in the vehicle. IBIT tests are permitted to interfere with the normal operation of the ADSS.

3.2.1.6.5.5 Periodic BIT (PBIT). The PBIT will be a non-intrusive test run in the background whenever power is applied to the ADST system. The frequency of the additional PBIT test (beyond power-up test) should be as defined in the procurement specification. It is used to determine the health of the equipment without interfering with equipment tactical operations. Periodic BIT will include autonomous module tests, backplane tests and equipment health checks.

1. Periodic BIT should be state preserving and should execute during equipment operation as a background task.

2. Periodic BIT will begin testing automatically when the WRA completes initialization. Periodic Bit status will be made available to external equipment by interrogation of the ADSS.

3.2.1.6.5.6 Maintenance BIT (MBIT). MBIT may be distinct tests or may be a subset of the IBIT functions. These tests are specifically intended to support maintenance operations and may include tests that detect and map out defective areas of the memory on the RMM to maintain bit error rate. This type of a test usually requires that the complete memory be overwritten upon initiation of MBIT and at the completion the RMM is completely erased and is ready for the next use. The time required for the complete process to be completed for all RMMs should be specified.

3.2.1.6.5.7 BIT Reporting. BIT data should be reported as requested by external equipment. Reported BIT data should allow determination of specific loss of equipment functionality. BIT should report current status over the control/status interface and/or BIT discrete in all modes of operation.

3.2.1.6.5.8 Fail-Safe Operation. The circuits and devices that provide self-test functions should be designed in such a manner that any failure of the self-test circuitry should not functionally degrade the equipment with which it is associated.

3.2.1.6.5.9 BIT Fault Recording. BIT data for the latest N detected faults should be stored in equipment non-volatile memory for retrieval at a later time. Time of failure should be stored with the BIT data.

3.2.1.6.5.10 Discrete Warnings and Indicators. If a BIT indicator is appropriate for the specific ADSS program then the following features should be considered:

1. Placement of the indicator on each line removable assembly.
2. Event types that will cause the indicator to be set and to be reset (e.g., power cycling, IBIT results).
3. Ability to control the state of the indicator via the system control interface.
4. The color and brightness of the indicator and whether or not it must be viewable without power applied.

3.2.2 Physical.

3.2.2.1 ADSS. The ADSS weight, center of gravity, dimensions, mounting, cooling, markings, etc should all be clearly specified as required for the particular application. The requirements and procedures for the removal and insertion of the RMM into the ADSS must be specified.

3.2.2.2 RMM. The RMM weight, center of gravity, dimensions, mounting, cooling, markings, etc should all be clearly specified as required for the particular application. The requirements and procedures for access to the RMM must be specified.

3.2.3 Reliability. A primary consideration for use of an ADSS is increased reliability and data integrity. Reliability requirements should address long-term use and consider data recovery (e.g. disk replacement in a RAID system). Specific requirements for Mean Time Between Failures (MTBF) should be established for the ADSS when operated in any combination of modes, service life, or natural environments. Predicted MTBF levels should also be established and can be based on MIL-HDBK-217 or industrial standard alternatives. An expected standard service life for the ADSS may also be specified under the environments and design described within the spec. It would also be very important to specify the expected number of RMM removal and insertion cycles with the ADSS without degradation to the performance of the system.

3.2.4 Maintainability. There are numerous maintainability issues that should be considered in drafting the specification for the ADSS. Overall maintainability design guidance can be found in MIL-HDBK-2084 and MIL-STD-1472. Some of the areas that should be considered include Preventative and Scheduled maintenance, Fault Isolation procedures including use of the various BIT modes, Mean Time to Repair (MTTR), Modular Design concept, Handling Provisions, Adjustments and Alignments allowances, Tools and Test Equipment, etc.

3.2.5 Transportability.

3.2.5.1 ADSS Transportability. Specifications should provide transportation environmental requirements such that the ADSS will survive during transport without damage or performance degradation.

3.2.5.2 RMM Transportability. The RMM will be removed from the data acquisition platform and taken to the ground station for data recovery in many cases. The specifications should address the conditions it must withstand during removal, transport and insertion into the ground station system.

3.2.6 Safety and Cautions. This paragraph should provide requirements and address issues related to safety and cautions in connecting to and handling the RMM. Since the NADS Interface incorporates a power connector and data can be downloaded from the NADSI port while the RMM is installed in the aircraft, specific cautions and safeguards should be highlighted. Specifically, when the RMM is mounted and powered in the aircraft, the power pins on the NADSI may have voltage supplied to them by the ADSS. These pins are male because the ground station connector supplying power (when the RMM is connected to the DCGS) was chosen to be female. There is the potential for high current flow if these pins are shorted. Appropriate connector covers should be installed when the RMM is in the ADSS/aircraft and the NADSI connector has the potential to be powered. Procedures and training should address this potential hazard.

3.2.7 Other Characteristics. Other characteristics to be specified could include (but are not limited to) Environmental, EMI, Design & Construction, Human Engineering, Interchangeability, Security and Computer Resources.

4. Quality Assurance Requirements.

4.1 General. In this area, quality conformance requirements should be specified along with methods of verification, inspection, analysis and demonstration. Also, ADSS and RMM functional and performance acceptance tests including NADS Interface Certification tests would be contained in this section.

SPECIFICATION TEMPLATE FOR GROUND STATION TO MEET NADS INTERFACE REQUIREMENTS

1. SCOPE.

1.1 Introduction. Introduce and name the equipment covered and state the purpose for the specification.

1.2 Functional Requirements. Describe the system in moderate detail, providing component modular nomenclature and function of each module within the system.

1.3 Organization of the Specification. Describe the organization of the specification to follow.

2. Applicable or Referenced Documents. Some examples of Applicable or Referenced Documents are contained in section 4 of the Overview on page 3 of this document.

3. Recommended Ground Station NADSI Capabilities.

3.1 Ground Station Data Download System Definition. Describe the total ground station data download system being addressed by the specification and a description of planned CONOPS.

3.1.1 Interface Definition. Describe and show by Block diagrams the various interfaces associated with program requirements.

3.2 Characteristics. The following characteristics should be described for the NADS Interface in a ground station:

3.2.1 Recommended Minimum Capabilities Details. Minimum capabilities details of the presentation of information, and the interaction of the user with the computer download process should be in accordance with the appropriate program Human Computer Interface specifications. As a minimum, the system should provide the following functionality to the user:

1. Ability to detect the presence of a new NADS compliant device (once cabling and power on self test is complete). The detection of a new device may be performed automatically, or following user initiation. Some systems may require that the SCSI upper layer protocol (ULP) be re-initialized via a complete system re-boot, and others may perform the discovery operation by a software "probe" of the interface system. The exact device discovery requirements need to be specified by the procurement office.
2. Ability to select the NADS device, prepare and test the device for download operations.
3. Ability to download and list the file contents of the NADS device.
4. Ability to select logical blocks or one or more individual data files for download to the ground station system.
5. Ability to select all data files for download to the ground station systems.
6. Automatic, or operator selected download of a file or sequence of files

3.2.1.1 Automatic Or Selected File Download. Download of a file or sequence of files requires a ground station utility that:

1. Has determined the NADS device's Logical Block (LB) size.
2. Has downloaded and stored the NADS device's File Directory (this may require reading only LB #1 or reading multiple logical blocks if forward links are indicated).

3. Interprets the LB address range of the selected file and composes one or more SCSI Read commands based upon the file size, the NADS device's LB size and the ground station RAM assigned to temporarily store mission data.

4. Has determined the LB size of the target hard drive or RAID peripheral and its available address range for writing data (normally handled by a file system call to the host operating system).

5. Has confirmed adequate space available to download mission files.

6. Composes file system / peripheral Write commands based upon the peripheral's parameters and the size of mission data segment held in ground station RAM.

7. Is capable of creation of the hard drive/RAID's file, with support for either automatic hard drive/RAID file naming (e.g. use NADS file name) or prompt operator for file name.

8. Does not preclude the exploitation of mission data directly from the RMM

3.2.2 Optional Capabilities / Recommendations. Dependent upon the procurement specification, the following additional NADS Interface related capabilities may be specified for the ground station application, but may not be available with all RMMs that could be attached to the ground station:

1. Ability of the user to select the target directory for file download.

2. Ability to make a hard /soft copy print of the directory listing of the NADS device.

3. Ability to display the progress of any data transfer operations to or from the NADS device (specific indication details would be specified within the program HCI style guide).

4. Ability to interrupt, resume or cancel a data transfer operation.

5. Ability to list supported command set for specific NADS device. i.e. provide the operator with feedback on the ability of the NADS device to accept further NADS compliant commands.

6. Ability to copy the entire contents of the NADS device into a single file in the ground station. This functionality may be useful for recovery of data should the system be unable to decipher the directory listing due to airborne equipment failure. (Corruption of NADS file table due to power failure etc)

3.2.2.1 Incremental Download of Multiple files. The software interface between the NADS device and the host operating system will take the form of a self-contained device driver, or compilable software module library. The simplest implementation for a NADS software interface is usually through a user level software application, utilising specific NADS library code.

Most host computer systems natively support Fibre Channel devices, and more specifically the SCSI command protocol over a Fibre Channel connection through the use of low-level device drivers supplied with the specific Fibre Channel interface hardware or through native support by the operating system. It is recommended that any additional NADS interface software be a non-blocking implementation, allowing simultaneous access by one or more user applications, or user application threads. The reason for this recommendation is the desire to obtain the maximum throughput and utility from the functionality offered by the new breed of NADS compliant random access media.

Most operating systems used in ISR ground stations support multi-tasking and/or multi-threaded operations, and it is advised that any NADS software implementations continue to support multi-tasking and threading operations. An example download scenario could see a NADS device with several data files being read by a ground station. One of the files is a large multi-gigabyte compressed data file, and several of the other files are smaller auxiliary data files. After reading one of the auxiliary data files, the ground station begins to open and read the large compressed data file, transferring several blocks of compressed data before de-compression begins, at which time download is paused. The NADS device is therefore available for transfer of data from other data blocks whilst the decompression takes place. Depending upon the implementation of the NADS device driver, and whether the driver is blocking or non-blocking, NADS device may or may not be available for continued download of alternate data whilst the main data transfer has paused. Historically tape recorders have been unable to re-position and transfer alternate data without incurring a throughput penalty, however random access media offers the ability to near simultaneously serve several streams of user data from the device (for example imagery from more than one sensor).

3.2.2.2 Declassification. The ability to erase / declassify / purge data from the NADS device (assuming system security policy permits this operation and the NADS device supports this operation) is a highly desirable capability. Declassification procedures for disk and solid state devices are provided in the NATO AEDP 3 document. It is assumed that host ground stations will not be required to declassify RMMs received from non-native systems, or RMMs from other NATO nations. However the functionality to achieve declassification through the NADS interface may be specified, should the NADS interface be the only, and hence prime interface for a host ISR system. See AEDP-3 for further guidance.

3.2.2.3 NADS As The Primary Interface. Should the ISR system wish to use the NADS interface as the primary interface for the data recorder, then further functionality may be required to support the re-commissioning of the recorder prior to re-use within the airborne ISR system.

3.2.3 Power Supply Characteristics. Specific power supply interface requirements for NADS devices are listed in STANAG 4575 Annex C section 3. In addition, detailed guidance regarding power supply considerations are provided in Annex C of this document at paragraph 3.5.

3.3 Performance. Data Integrity and Performance of the download port should not be degraded by the ground station, its interface implementation or other influences of ground station operation.

3.4 Physical.

3.4.1 Mounting/Support. Describe the physical environment and how the RMM to be downloaded will be supported in accordance with STANAG 4575. Also, describe how the physical assemblies that will constitute the NADSI port, interface board, power supplies, connectors will be mounted and supported so as to be assessable and provide the shortest cable run to the connected RMM.

3.4.2 Connector Selection. Describe how both the circular and D-sub connectors will be accommodated. If the flying leads use connectors on both ends, describe the requirements for the panel mounted connectors and caps (if required).

3.4.3 Flying Leads. Describe the cable and connector approach, including cable length, routing and storage when not in use. Address the use of adaptors and/or cable extensions.

3.4.3.1 Safety and Cautions. This paragraph should describe the requirements and address issues related to safety and cautions when connecting to the RMM via the NADSI or its native interface in a ground station. When the RMM's NADS Interface is used to download data in the ground station, the ground station will provide power using flying leads from the system. The power supplies have the potential to provide high currents and the procedures should include the method and sequence for proper connection and appropriate cautions. When the RMM is used in a docking tray in its native system the power pins of the NADSI connector may have voltages applied. Cautions related to covering the NADSI connector, including use of the connector cover should be specified.

3.4.4 Environmental. Describe the Cooling, EMI and Other Environmental requirements.

3.4.4.1 RMM Cooling Requirements in Ground Station. If there is a time requirement for the RMM to be cooled down or warmed after storage, it should be so indicated. Appropriate standards such as MIL-HDBK-5400 should be referenced.

3.4.4.2 EMI Requirements. The ground station requirements for both radiated and conducted EMI should be reflected in the NADSI specification. The NADSI hardware should not be effected by the electronic environment in the ground station. The EMI/RFI requirements should be applied to the NADSI with the flying leads attached to the RMM. The flying leads should be specified with the appropriate shielding and grounding.

3.4.4.3 Other Environmental Requirements.

3.5 Reliability. The inherent reliability of commercially available Fibre Channel interfaces is very good. The reliability of the NADS Interface hardware set should be specified to meet the reliability requirements of the system. The specification for the flying leads and connectors should take anticipated number of insertions, handling by ground system personnel and storage into consideration.

3.6 Maintainability. The location, mounting and connection of the NADS Interface should allow for access by ground station maintainers and technicians.

3.7 Transportability. When installed, the NADS Interface will be able to withstand moving of the ground station and transportation of the ground station using normal methods. The requirements fro other equipment in the ground station should be applied to the NADSI.

3.8 Storage. Describe how the NADS Interface and associated power supplies will be secured and stored when not in use. If the NADSI hardware set is not mounted in a rack or cabinet, it will be securely stored when not in use. When secured, it will withstand transportation of the ground system. The NADS Interface installation should be as compact and functional as possible within good engineering practice.

4. Quality Assurance Requirements

4.1 General. In this area, quality conformance requirements should be specified along with methods of verification, inspection, analysis and demonstration. Also, NADSI Ground Station functional and performance acceptance tests including NADS Interface Certification tests would be contained in this section.

COMPLIANCE TEST AND CERTIFICATION

1. Introduction.

1.1 Purpose. This Annex establishes the North Atlantic Treaty Organization (NATO) Advanced Data Storage Interface (NADSI) Compliance Test and Certification activities for achieving and sustaining NADSI compliance by all fielded and developmental advanced digital data storage implementations. This Compliance Test and Certification Guidance prescribes the NADSI Compliance Test and Certification policies, defines roles and responsibilities, and provides test-funding guidance within the Global NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA) Allied Engineering Documentation Publication (AEDP) Structure.

1.1.1 NADSI Testing Goals. The overall goal of NADSI testing is to maximize NATO-owned and national information system's interoperability in NATO operations. This will be accomplished by the following:

1. Verify standards syntactical correctness and unambiguous interpretation to ensure high quality NADSI documentation.
2. Ensure NADSI satisfies the information transfer requirements specified in STANAG 4575.
3. Ensure NATO-owned and national information systems implement the NADSI standard correctly and consistently.
4. Conduct NATO Compliance Tests to determine whether or not deviations from Standard Agreement (STANAG) 4575 exist and certify systems that implemented the standard correctly.
5. Conduct NATO-owned and national information systems interoperability evaluations to determine how/if different standard implementations have impacted interoperability.

1.1.2 Test Guidance Basis. This Guidance is established under the NATO Common Interoperability Standards (NCIS) Testing Concept and the NIIA AEDP Structure. This Guidance will allow developers, system designers, system managers, and budget planners to plan and perform NADSI testing. The NADSI Custodian is responsible for coordinating the use of national and NATO testing facilities in accordance with this Guidance.

1.2 Scope. This document applies to all NADS Interfaces and Data Storage Devices defined as meeting the NADSI standard. This document encompasses the following NADSI Compliance Test and Certification information:

1. Testing authorities
2. Testing responsibilities
3. Funding test services
4. Defining test criteria
5. Compliance test planning, execution, and reporting

1.2.1 Test Guidance Organization. Section 2 introduces the test criteria. The test execution section, Section 3, is divided into two parts. Part One addresses the test criteria for acquisition equipment, specifically the Removable Memory Module (RMM). Part Two provides the test criteria for the ground stations (GSs) side of the interface. Sections 4 and 5 provide the quality assurance requirements and reporting procedures. Section 6 defines the requirements for the test facilities.

1.3 Background. The interface and if applicable, the associated cable test are required of each manufacturer to certify compliance with the standard. In conjunction with the interface test, RMMs will be verified to comply with the requirements of the standard both for data transfer and interface performance. The same test method and equipment will be used for both tests.

On the opposite side of the interface, the GS must also be tested to certify compliance with the standard. This testing will confirm that the GS will be able to provide the proper commands to the RMM, provide the required power and receive the imagery and associated data for exploitation.

As stated in the NATO Policy for Command, Control, and Communications (C3) Interoperability, "there is a NATO requirement that automated data systems, whether NATO or nationally owned, used by the forces of NATO, be interoperable; the extent of the interoperability between specific systems is to be determined and agreed according to the information exchange requirements of cooperating forces."

The NATO Interoperability Management Plan (NIMP) provides the overall NATO strategy for the improvement of interoperability of information systems in support of C3. The strategy calls for the development of NCIS and their implementation on the interfaces of NATO-owned and national information systems that have requirements to interoperate in NATO operations. The NIMP establishes the NATO Interoperability Framework Testing Infrastructure (NIFTI) to coordinate the testing of NCIS standards. The NIMP also establishes the 5-year Rolling Interoperability Program (RIP). The NIFTI program provides input to the RIP on the status of Interoperability Milestones. This enables NATO to assess the “State-of-Interoperability” for NATO and national systems. The NADSI Custodian will provide feedback to NIFTI and the RIP.

1.4 References. Referenced documents for this Annex are contained in section 4, Applicable or Referenced Documents, on page 3 of this AEDP.

1.5 Applicability. To ensure STANAG 4575 quality and its successful implementation in NADSI systems, the Compliance Test and Certification guidance is applicable to tests performed during NADSI development, configuration management, implementation, and operational use. Nations, Major NATO Commands (MNCs), and NATO organizations responsible for the development, configuration management and implementation of NADSI are to conduct testing in accordance with this Plan. This Plan will be effective upon approval by all authorities.

Within the NCIS Testing Concept document, statements are made about the level of commitment of nations, MNCs, NATO organizations, and industries to adhere to testing implementations utilizing NCIS standards. The principal commitments in the use of this test program are summarized below:

1. NADSI Compliance and Interoperability Testing is mandatory for MNCs, NATO organizations, and Host Nations employing the NADSI in NATO-owned information systems to be used in NATO operations.
2. NADSI Compliance Testing and Interoperability Testing is highly recommended for nations employing the NADSI in national information systems to be used in NATO operations.
3. NADSI Compliance Testing is encouraged for nations implementing NADSI systems even when intended for national use only.
4. Industries that develop commercial-off-the-shelf (COTS) systems that implement the NADSI are recommended to submit their products for testing under the provisions of this Compliance Test and Certification Guidance. NATO and nations that acquire COTS to use in their information systems should insist on standards compliant products.

1.6 Authority. The following bodies have the responsibility for participating in the NADSI Test Program.

1.6.1 NATO Air Force Armaments Group (NAFAG) Air Group IV (AG IV). NAFAG AG IV has the responsibility for the development and configuration management of STANAG 4575. AG IV oversees the process whereby imagery systems achieve and sustain NADSI compliance through the NADSI Test Program. AG IV appoints the STANAG 4575 Custodian who will in turn manage the

Configuration and Testing of the NADSI STANAG. The custodian will review and approve test procedures for the NADSI Test Facilities.

1.6.2 NADSI Custodian. The AG IV NADSI Custodian is the delegated NATO authority for the management oversight of the NADSI Test Program. The testing of the standard is embedded in the development and configuration management procedures that are within the responsibility of the NADSI Custodian. Because of the close relationship of configuration management and testing, the Custodian will be responsible for the day-to-day oversight of the NADSI Compliance Test and Certification activities, and has responsibility for maintaining configuration control of the NADSI STANAG.

1.6.3 NATO C3 BOARD (NC3B) Interoperability Sub-Committee (ISC). The NC3B (ISC) has the overall responsibility for NATO interoperability of C3 systems. The NC3B (ISC) will coordinate the activities of the NADSI Test Program within the NATO Interoperability Framework Testing Infrastructure.

1.7 NADSI Test Policies and Procedures.

1.7.1 Test Policies. The Testing Policies for AG IV STANAGs identified in the NATO ISR Interoperability Architecture (NIIA) are contained in AEDP-2, Part II.

1.7.2 Test Procedures. Each NADSI Test Facility will maintain its particular test procedures available upon request as part of the test coordination. A test procedure will be provided to the NADSI Custodian for review and approval.

1.7.3 Test Program Responsibilities.

1.7.3.1 Test Coordination. The NADSI Owning Body or Vendor will coordinate directly with the NADSI Test Facility for test support. The NADSI Test Facility will provide schedule availability for tests and retests.

1.7.3.2 Test Schedules. The NADSI Test Facilities will maintain test schedules and provide current scheduling information to the NADSI Custodian.

1.7.3.3 Master Schedule. The NADSI Custodian will maintain a master test schedule and demonstration/exercise schedule.

1.7.3.4 Certified NADSI Systems. The NADSI Custodian will maintain a Certified NADSI System registry.

1.7.4 Test Program Resources.

1.7.4.1 NADSI Test Facilities. The NADSI Custodian will maintain a registry of accredited NADSI Test Facilities. The registry will include point of contact information, locations, and associated costs.

2. Introduction To Test Criteria. NADSI systems or subsystems will be tested in accordance with the test criteria documented herein. Although different testing facilities may be authorized to certify compliance and may use different test procedures and protocols, all facilities will use this common set of test criteria. Each facility will generate the necessary test procedures and the STANAG 4575 Custodian will approve the test procedures as part of the accreditation of the facility to perform STANAG compliance testing.

2.1 Compliance with AEDP-2, Volume II, Annex B. The testing program in this document complies with the policy contained in the Air Group IV (AG IV) directions contained in AEDP-2, Volume 2, Annex B. The policies and procedures defined therein are applicable to this test and certification program. However, minor deviations from the general guidance in AEDP-2 may be identified, and under such circumstances, the guidance provided herein takes precedence. All deviations will be approved by the Chairman of the ISRIWG and AG IV as provided in AEDP-2.

2.2 Overall Test Philosophy This program is intended to ensure that systems implementing the STANAG 4575 interface will, in fact, be interoperable once deployed in coalition operations. The test program provides for testing of both the removable memory modules from the airborne element of the recorder, and the ground station components of the interface required to download the data for exploitation and display. While the testing program is intended to be comprehensive relative to STANAG 4575 interface requirements, it will not include testing of the applications required to properly exploit and disseminate the information. The test program assumes that the format of the data recorded on the RMM is proper and that the applications to exploit the data are available in the ground station. This test program is therefore limited to verifying that the interface functionality is correct and operates in accordance with the requirements of the STANAG.

2.2.1 Basic Test Concept The testing concept embodied by this test program requires that all required features of the interface operate properly and that no optional features cause interface failure (in the sense of an interface lock-up or electrical overload). The test criteria will cover tests that examine each requirement in the STANAG. A test matrix is included in section 2.3. No system that fails one or more of the tests will be certified under the provisions of this program. However, since the purpose of the test and certification program is to ensure interoperability of systems in coalition operations, every effort will be made to provide the vendor an opportunity to fix the problems and bring the system or subsystem into compliance. If corrections or fixes are made, the certification facility will repeat the entire test sequence and the system or subsystem will be required to pass all tests without further changes to ensure that fixes did not cause other problems prior to certifying the system or subsystem.

2.2.2 Full Compliance Certification and Subsystem Compliance Certification. A key element of the test program is the use of two levels of compliance: full and subsystem compliance. Full compliance states that the system under test complies with all requirements outlined in STANAG 4575, as applicable to the unit under test (e.g. RMM or ground station). Failure of any applicable tests will preclude awarding the full compliance certification. Subsystem compliance testing provides a means for those vendors producing components intended for use in NADSI-compliant systems to have their units tested. However, because the component does not provide the complete functionality of the interface, it cannot be awarded the full compliance certification.

2.2.2.1 Subsystem Eligibility. The only subsystems that can be awarded subsystem compliance are:

1. Disk Drives – Disk Drives would not typically have the device drivers included that would properly record the files in the NADSI structure. If the files are properly written to the drives, the drives would then respond to the NADSI command set through the NADSI interface. However, if the host writes the files in some other format or structure, the NADSI interface would likely fail.
2. Power Supply – Power supplies can be tested against STANAG 4575 criteria, but none of the data protocol criteria would apply.
3. Power Connector and Cable - Power Connector and Cables can be tested in isolation to the STANAG 4575 criteria.

Other subsystem options can be considered for subsystem compliance testing with supporting justification and the approval of the 4575 Custodial Support Team.

2.2.2.2 Subsystem Testing. If a vendor wishes to apply for subsystem certification, he will state in the application the limits intended for the tests. The vendor, the STANAG Custodian, and test facility will agree on the subset of criteria that the unit will be tested against prior to beginning the testing. The testing will then be a pass/fail of the agreed subset. The process is the same as described with a full compliance test. The subsystem compliance certification will be provided if the subsystem passes all the agreed subsystem criteria.

The certification facility will clearly identify those tests against which the system or subsystem was tested on the completion certificate. The information will include a summary of the intended use of the unit that received the limited certification, and the details of the testing that was performed. The details will allow potential users to know what tests were performed. It will also give potential users a sense of the extent of additional functionality that will be required to obtain full certification. The same information will also be recorded in the registry so that potential users of the system or subsystem can know to what extent the system or subsystem was tested.

2.3 Classification of Tests. Requirements associated with STANAG 4575 compliance and interoperability have been captured in Table D-1. The Owning Body will verify that a specification requirement has been met as confirmed by satisfactory completion of internal (contractor) and external (customer) design and document reviews. Such reviews will have established a high degree of confidence that the requirement has been properly interpreted and implemented, and has been applied according to the methods, practices, and standards required by the STANAG 4575. Some requirements are directly related to a specific validation test. Other requirements are difficult and expensive to test and validate. The following identifies which requirements correspond to a direct test, and which requirements are better validated through design analysis. The method of verification required for each test category is described below:

2.3.1 Inspection (I). Verification that a specification requirement has been met by observation of overt characteristics (such as mechanical orientation, presence of a feature, or color) or by simple measurement of a physical property (such as length or weight).

2.3.2 Test (T). Verification that a specification has been met by means of quantitative measurement with standard or specialized external test equipment under the required operating conditions.

2.3.3 Demonstration (D). Verification that a specification requirement has been met by satisfactory demonstration of the required function when operating with a STANAG 4575-certified system or subsystem, or by observation of a higher-level test.

2.3.4 Analysis (A). Verification that a specification requirement has been met by analyzing the contributing subsystem tolerances, ranges, or limits followed by the allocation of such components among the subsystem in such a manner that the overall specification is assured. Analysis may be derived from equations, charts, graphs, and/or test data.

2.3.5 Not Applicable (N). No verifiable requirement exists. Tests are not applicable to this paragraph.

Table D-1; Testing Requirements Matrix.

Legend: **I** – Inspect **T** - Test **D** – Demonstration **A** – Analysis **N** – Not Applicable
G – Ground Station **R** – Removable Memory Module **B** – Both

STANAG Paragraph	Requirement	I	T	D	A	N
B 1.1	Data Transformation			B		
B 2.1	Physical and Signaling			B		
B 2.1.1	Transmitter			B		
B 2.1.2	Signaling Rate		B			
B 2.2	Command Protocol		B	B		
Table B-1	Required		B			
Table B-1	Prohibited		B			
Table B-1	Invokable		B			
Table B-1	Recommended (if implemented)		B			
Table B-1	Allowed (if implemented)		B			
B 2.2.1	Stream Devices			R		
B 2.3.1	Encryption			B		
B 3	File Structure Definition			B		
B 3.1	Data Hierarchy			R		
B 3.1.1	Directory			R		
B 3.1.2	Directory Block					B
B 3.1.3	File Entry					B
B 3.1.4	Data Files			R		
B 3.2	Directory			R		
Table B-2	Magic Number		R			
Table B-2	Revision Number		R			
Table B-2	Shutdown		R			
Table B-2	Number of File Entries		R			
Table B-2	Reserved		R			
Table B-2	VolName		R			

Table D-1; Testing Requirements Matrix.						
Legend: I – Inspect **T** - Test **D** – Demonstration **A** – Analysis **N** – Not Applicable **G** – Ground Station **R** – Removable Memory Module **B** – Both						
STANAG Paragraph	**Requirement**	**I**	**T**	**D**	**A**	**N**
Table B-2	Forward Link			R		
Table B-2	Reverse Link			R		
Table B-2	(N File Entries)		R			
B 3.2.1	Directory Fixed Fields				R	
B 3.2.2	Block Size			B		
B 3.2.3	Directory to Data File Link			R		
Table B-3	Name (56 Bytes)		R			
Table B-3	FileStartAdd (8 Bytes)			R		
Table B-3	FileBlkCnt (8 Bytes)			R		
Table B-3	FileSize (8 Bytes)		R			
Table B-3	Create Date (8 Bytes)			R		
Table B-3	Create Time (8 Bytes)			R		
Table B-3	Time Type (1 Bytes)		R			
Table B-3	Reserved (7 Bytes)		R			
Table B-3	Vendor Unique (8 Bytes)					B
B 3.2.4	File Entry Name		R			
B 3.2.5	File Entry Singularity			R		
B 3.2.6	Directory and Memory Region Relationships			R		
B 3.2.7	Empty Memory Reads					B
B 3.2.8	Contiguous Directory Entries			R		
B 3.2.9	Deleted Files		R			
B 3.2.10	Reserved Field		R			
B 3.2.11	Number of File Entries		R			
B 3.3	Data Definitions					B
B 3.3.1	Byte Order			R		
B 3.3.2	Character Set			R	R	
B 3.3.3	Naming Restrictions					B
B 3.3.3.1	Characters			R	R	
Table B-4	Prohibited Characters			R	R	
B 3.3.3.2	Names		B			
C 2	Interface Connectors	B	B			
C 2.1	D-sub Military Connector	B				
C 2.2	Circular Military Connector	B				
C 3	Power Input Interface		B			
	RMM Powered from GS		G			
	RMM Powered from Acquisition Platform					B
	Turn ON Time, no load, $\geq$ 0.5 mS (min)		G			
	Turn ON Time, full load, $\leq$ 5.0 mS (max)		G			
	Turn ON Voltage Overshoot, no load to full load $\leq$ 50mV (max) for 3.3, 5.0, & 12 VDC, $\leq$ 500mV (max) for28 VDC		G			
	Safety Interlock, GS 5 secs (MIN)		G			
Table C-1	Memory Unit Max Power Requirement		B			
C 4	GS Environment Requirements	B				
C 5.1	D-sub Pin Connections	B	B			
C 5.2	Circular Pin Connections	B	B			

Note: All criteria are pass/fail unless otherwise noted.

3. <u>Test Criteria</u>

3.1 <u>Part One: Acquisition Platform Equipment/RMM</u>.

3.1.1 <u>Test Objective</u>. To determine if the NADSI Acquisition Equipment/RMM can establish an interface to the NADSI Ground Station or Intermediate Terminal and transfer required data as specified in STANAG 4575.

3.1.2 <u>Required Documentation and Software</u>. The documents, software, and pretest procedures listed in 3.1.2.1 are required for performing the NADSI Acquisition Equipment/RMM Compliance Test and Certification.

3.1.2.1 Documents.

1. STANAG 4575
2. AEDP-6 and AEDP-2, Volume II, Annex B
3. Owning Body Test Requirements Document (if applicable)
4. NADSI Test Requirements Document
5. NADSI Test Facility Test Plan and Procedures

3.1.2.2 Software. The Owning Body or Vendor will be provided test data to be recorded to the RMM data storage unit prior to the test. The test data will be of sufficient size to require more than one Directory Block and will consist of test patterns and files of various file sizes and file types.

3.1.3 RMM Electrical and Command Protocol Requirement. The RMM interface will conform to the requirements of the Fibre Channel Private Loop Small Computer System Interface (SCSI) Direct Attach (FC-PLDA, ANSI/NCITS TR19-1998) with the exception that it conforms to the minimum set of commands in Table B-1 in Annex B of STANAG 4575, "Required" SCSI Commands, Features and Parameters.

3.1.3.1 Criteria.

1. The RMM interface will use an electrical transmitter (D).
   a. Fibre Channel/SCSI 3 Diagnostic Test - May be based on anomalies (D)
   b. The signaling rate will be 1.0625 Gbaud (T)

2. The RMM interface will provide SCSI Target functionality (T, D).

3. The RMM interface will implement or will not implement in accordance with STANAG 4575, SCSI commands, features, and parameters that are:
   a. Required (T)
   b. Prohibited (T)
   c. Invokable (T)
   d. Recommended (if implemented) (T)
   e. Allowed (if implemented) (T)

4. The interface does not use stream device or encryption protocols (D).

5. File (data) transfer from the RMM will be demonstrated (D).

3.1.4 RMM File Structure Requirement. The RMM interface will conform to the requirements of the Logically Sequential Access Mode defined in Paragraphs 3 through 3.3.3.2, Annex B of STANAG 4575.

3.1.4.1 Criteria.

1. Data Hierarchy (D)

   a. Directory (D)
      (1) One or more directory blocks of data will contain a list of all data files.
      (2) The directory will start at logical address zero of each block.

   b. Directory Block. The memory block will contain file entries and other metadata (N).
   c. File Entry. A fixed length data structure will describe files (N).
   d. Data Files. Data files will comprise user data stored in a monotonically increasing contiguous logical address (D).

2. Directory (D)
   a. Directory Blocks (Table B-2) (D).
      (1) Magic Number. The value is BCS "FORTYtwo" (hex – 0x464F52545974776F) (T)
      (2) Revision Number. Revision number of STANAG (T)
      (3) Shutdown. If set to 0xFF, then file system was properly shutdown.(T)
      (4) Number of File Entries. Number of file entries that follow (T)
      (5) Reserved. Bytes are reserved (T)
      (6) VolName. Filled with 0x00 for no name (T)
      (7) Forward Link. Block address of next block (D)
      (8) Reverse Link. Block address of directory block pointing to this address (D)
      (9) (N File Entries). One entry for each file (T)

   b. Directory Fixed Fields (A).
   c. Block Size. Varying block sizes (not defined) will be determined via SCSI protocol (D).
   d. Directory to Data File Link (Table B-2) (D).
      (1) Name (56 Bytes). File name (T)
      (2) FileStartAdd (8 Bytes). Zero based address of first block (D)
      (3) FileBlkCnt (8 Bytes). One based number that is the count consecutive address blocks (D)
      (4) FileSize (8 Bytes). The actual number of bytes contained in file (D)
      (5) Create Date (8 Bytes). DDMMYYYYBCS Character values (D)
      (6) Create Time (8 Bytes). HHMMSSss Character values (D)
      (7) Time Type (1 Bytes). A numeric code that qualifies the time and date values recorded in the "Create Date" and "Create Time" fields ((T)
      (8) Reserved (7 Bytes). Bytes are reserved (T)
      (9) Vendor Unique (8 Bytes). For vendors to utilize (N)
   e. File Entry Name. Each entry in a directory will have a unique name (T).
   f. File Entry Singularity. Multiple files entries will not refer to the same regions of memory (D).
   g. Directory and Memory Relationships (D).
   h. Empty Memory Reads (N).
   i. Contiguous Directory Entries. File entries and all fields in a directory block will be contiguous (D).
   i. Deleted Files. The corresponding file entry's File Block Count field will be marked with 0x00 (T).
   j. Reserved Fields. Reserved fields not used will be filled with 0xFF (T)
   k. Number of File Entries. The numerical value placed in the Number of File Entries field of a Directory Block will equal the number of active File Entries plus any File Entries marked as deleted (T).
3. Data Definitions (N)
   a. Byte Order (A).
   b. Character Set (D, A).
   c. Naming Restrictions (N).
   d. Characters: Specific prohibited characters will not be used (T, A).
      (1) Prohibited Characters (Table B-4) (T, A)
   e. Names (T)
      (1) Leading and trailing spaces will not be permitted.
      (2) Leading periods will not be permitted.
      (3) Names will fill their field starting with byte 0.
      (4) Names will terminate their field with 0x00.
      (5) When Names utilize full field length, then terminating 0x00 is omitted.

3.1.5 <u>RMM Connectors and Power Requirement</u>. The RMM connectors (D-sub 50 male pin or DTL 38999 male pin) and Data-Out Ports will comply with standards and protocols in accordance with Annex C to STANAG 4575, Physical and Power Interface Definitions.

3.1.5.1 Criteria.

1. RMM will use D-sub 50 male pin or DTL 38999 male pin equivalent connectors (I).
2. RMM will use the Pin-out detailed in Annex C to STANAG 4575 (I).
3. RMM will allow the NADSI Test Set or GS to detect a continuous short circuit across the RMM Safety Interlock Leads for a minimum of five seconds to verify the safety lock(T).
4. When removed from the acquisition platform, the RMM will operate to specification when the NADSI Test Set or a ground station provides power in accordance with STANAG 4575 (allotted power and within the tolerances) (D).
5. When removed from the acquisition platform, the RMM will boot up when power in accordance with STANAG 4575 is detected from the NADSI Test Set or a ground station (D).
6. When the RMM is installed in the acquisition platform, it will provide, at a minimum, access to the STANAG 4575 connector that houses the data and command interface (I).
7. Connectors will be tested for continuity and isolation.
8. The RMM will not use more power than allotted in table below (T):

Table D-2; Removable Memory Module Maximum Power Requirements (T)

Voltage	Current
3.3 VDC	15.0 A
5.0 VDC	10.0 A
12 VDC	13.5 A
28 VDC	5.0 A
Legend: A – Ampere VDC – Voltage Direct Current	

3.1.6 Environment Requirement. The RMM will operate in the environment provided by the GS that is compliant with Annex C, Ground Station Environment Requirements to STANAG 4575 (I).

3.1.6.1 Criteria. The RMM will operate during the following environmental conditions:

1. RMM will not require special cooling (I)
2. RMM will operating in an ambient air range of –20 to +50 degrees Celsius, non-condensing (I)
3. RMM will have any hot surfaces marked IAW proper safety guidelines (I)

3.2 Part Two: Ground Station

3.2.1 Test Objective. To determine if the NADSI GS can establish an interface to the NADSI RMM to request and receive required data as specified in STANAG 4575 and to determine that the NADSI GS can provide the required power and can accept all required cable/connector types.

3.2.2 Required Documentation and Software. The documents, software, and pretest procedures defined in 3.2.2.1 are required for performing the NADSI GS Compliance Test and Certification.

3.2.2.1 Documents.

1. STANAG 4575
2. AEDP-6 and AEDP-2, Volume II, Annex B
3. Owning Body Test Requirements Document (if applicable)
4. NADSI Test Requirements Document
5. NADSI Test Facility Test Plan and Procedures

3.2.2.2 Software. The owning Body or Vendor will provide the capability to control the RMM and interact with test data received during the test. The test data will be of sufficient size to require more than one Directory Block and will consist of test patterns and files of various file sizes and file types.

3.2.3 GS Electrical and Command Protocol Requirement. The GS interface will conform to the requirements of the Fibre Channel Private Loop SCSI Direct Attach (FC-PLDA, ANSI/NCITS TR19-1998) with the exception that it conforms to the minimum set of commands in Table B-1, Annex B of STANAG 4575, "Required" SCSI Commands, Features and Parameters.

3.2.3.1 Criteria.

1. The GS interface will use an electrical transmitter (D).
   a. Fibre Channel/SCSI 3 Diagnostic Test (D)
      (1) Pass/fail/anomalies
   b. Signaling Rate will be 1.0625 Gbaud (T)

2. GS will provide SCSI Initiator functionality.

3. GS will implement or will not implement in accordance with STANAG 4575, SCSI commands, features, and parameters that are:
   a. Required (T)
   b. Prohibited (T)
   c. Invokable (T)
   d. Recommended (if implemented) (T)
   e. Allowed (if implemented) (T)

4. The GS will not implement the Fibre Channel encryption services (D).

5. File (data) transfer from the RMM will be demonstrated (D).

3.2.4 GS File Structure Requirement. The GS interface will conform to the requirements of Paragraph 3. through 3.3.3.2 in Annex B of STANAG 4575.

3.2.4.1 Criteria.

1. GS will demonstrate the capability to read the RMM directory and file structure (D)
   a. Select, command, and receive discreet files (T).
   b. Select, command, and receive complete downloads (T).
   c. Files and complete downloads will be compared with test date to determine accuracy and completeness (T). *The method for extracting the data from the GS will depend upon the SUT and test procedures.*
   d. Block Size. Varying block sizes (not defined) will be determined via SCSI protocol (D).
   e. Vendor Unique (8 Bytes). For vendors to utilize (N).e. Names (T)
      (1) Leading and trailing spaces will not be permitted.
      (2) Leading periods will not be permitted.
      (3) Names will fill their field starting with byte 0.
      (4) Names will terminate their field with 0x00.
      (5) When Names utilize full field length, then terminating 0x00 is omitted.

3.2.5 Connectors, Cables, and Power Requirement. The GS connectors (50 contact female socket D-sub connector and DTL 38999 female socket) and Cables will comply with standards and protocols in accordance with Annex C, Physical and Power Interface Definitions to STANAG 4575(I).

3.2.5.1 Criteria. Cables will have the correct mating, pin out, and positive lock mechanism assemblage. Cables/Connectors will be tested for continuity and isolation(I, T).

1. Cables will utilize a twin-axial copper pair with differential impedance of 150 ohms (I, T)
2. Power Test to an RMM when RMM is removed (T).

Table D-2; Removable Memory Module Maximum Power Requirements (T)	
Voltage	**Current**
3.3 VDC	15.0 A
5.0 VDC	10.0 A
12 VDC	13.5 A
28 VDC	5.0 A
Legend: A – Ampere VDC – Voltage Direct Current	

Table D-3; D-sub 50 Pin Correct Power Test (T)							
Voltage	**Current**	**Watts**	**Regulation**	**Low**	**High**	**VDC Pass/Fail**	**Current Load Pass/Fail**
3.3 VDC	15.0 A	49.5	± 5%	3.135	3.465		
5.0 VDC	10.0 A	50.0	±5%	4.75	5.25		
12 VDC	13.5 A	162.0	± 5%	11.4	12.6		
28 VDC	5.0 A	140.0	± 10%	25.2	30.8		
Legend: A – Ampere VDC – Voltage Direct Current							

Table D-4; Circular Power Connector Correct Power Test (T)							
Voltage	**Current**	**Watts**	**Regulation**	**Low**	**High**	**VDC Pass/Fail**	**Current Load Pass/Fail**
3.3 VDC	15.0 A	49.5	±5%	3.135	3.465		
5.0 VDC	10.0 A	50.0	±5%	4.75	5.25		
12 VDC	13.5 A	162.0	±5%	11.4	12.6		
28 VDC	5.0 A	140.0	±10%	25.2	30.8		
Legend: A – Ampere VDC – Voltage Direct Current							

3. GS Power Supply Test

a. Turn On time (0V to regulated output voltage; no load): ≥0.5 mS (minimum) (T)
b. Turn On time (0V to regulated output voltage; full load): ≤ 5.0 mS (maximum) (T)
c. Turn On Voltage Overshoot (no load to full load): ≤ 50.0mV (maximum) for 3.3, 5.0, and 12 VDC, and ≤ 500.0mV for 28 VDC (T)

Table D-5; D-sub 50 Pin Turn On Time Test (T)				
Voltage	**Time On No Load ≥ 0.5 mS (min) Pass/Fail**	**Time On Full Load ≤ 5.0 mS (max) Pass/Fail**	**Time On Voltage Overshoot ≤ 50.0 mV (max) Pass/Fail**	**Time On Voltage Overshoot ≤ 500.0 mV (max) Pass/Fail**
3.3 VDC				N/A
5.0 VDC				N/A
12 VDC				N/A
28 VDC			N/A	
Legend: min – minimum max – maximum mS - milliseconds mV - milli Volts VDC – Voltage Direct Current				

Table D-6; Circular Power Connector Turn On Time Test (T)				
Voltage	**Time On No Load ≥ 0.5 mS (min) Pass/Fail**	**Time On Full Load ≤5.0 mS (max) Pass/Fail**	**Time On Voltage Overshoot ≤50.0 mV (max) Pass/Fail**	**Time On Voltage Overshoot ≤ 500.0 mV (max) Pass/Fail**
3.3 VDC				N/A
5.0 VDC				N/A
12 VDC				N/A
28 VDC			N/A	
Legend: min – minimum max – maximum mS - milliseconds mV - milli Volts VDC – Voltage Direct Current				

4. GS power supply will detect a continuous short circuit across the RMM Safety Interlock Leads for a minimum of five seconds before outputting power. (T)
    a. Pass/fail/time required.

3.2.6 Environment Requirement. The GS will provide an environment that is compliant with Annex C, Ground Station Environment Requirements to STANAG 4575 (I).

3.2.6.1 Criteria. The GS will provide for the RMM the following environmental conditions:
1. GS will provide a flat surface at least 18 inches wide, 18 inches deep, and 12 inches high (I)
2. GS will support a minimum of 43 pounds (19.5 kilograms) (I)
3. GS will provide a flat surface capable of withstanding +100 degrees Celsius on the contact surface (I)
4. GS will provide in an ambient air range of –20 to +50 degrees Celsius, non-condensing (I)

4. Quality Assurance Provisions. The Quality Assurance (QA) Provisions are an integral part of the program needed to assist the NADSI custodian in ensuring high standards are maintained throughout the system life cycle process, from documentation to system certification. QA consists of but is not limited to:

1. Editorial document reviews to ensure clear, concise communication.
2. Validating the STANAG.
3. Validating test set operation/calibration and test procedures prior to testing.
4. Independent test result assessments.

5. Reporting

5.1 Certification Letters and Test Summaries. The NADSI Test Facility will provide a Compliance Certification Letter with test summary to the NADSI Custodian and owning Body or Vendor if the NADSI system complies with STANAG 4575. The test summary will include the following:
1. System Title
2. Proponent
3. Program Manager
4. Testers
5. System Under Test Description
6. Test Network Description
7. System Configuration
8. Modes of Operation
9. Testing Limitations
10. Required Standards and Conformance
11. Summary providing:
    a. Number of trials passed
    b. Number of trials failed
    c. Total number of trials

5.2 Certification Recommendation to Custodian. The NADSI Test Facility will provide an Assessment Letter with test summary to the owning Body or Vendor and to the NADSI Custodian within 30 calendar days after completion of tests if the system does not comply with STANAG 4575 or when reporting demonstration results. The NADSI Test Facility will also out brief the owning Body or Vendor at the end of the test with known problems and provide an informal quick-look e-mail report to the owning Body or Vendor, NADSI Custodian and his AST within 15 calendar days. Compliance Certification Letters and Assessment Letters will be maintained with the NADSI Custodian, placed on the NADSI web site, and placed in the JITC registry.

5.3 Appeals to Custodian. The owning body or vendor may appeal to the NADSI Custodian for complaints involving test facility schedule conflicts, test procedures, or test results. Test result complaints need to be filed within 30 calendar days after issuance of the Assessment Letter by the NADSI Test Facility. The owning body or vendor will appeal to the NADSI Custodian in writing.

6. Test Facility(ies). The NADSI Test Facility encompasses the hardware and software (NADSI Test Set), and personnel needed to provide a NADSI Compliance Test capability. The NADSI Custodian will accredit NADSI Test Facilities. The NADSI Test Facilities should be accessible to any NATO body that wishes to make use of the compliance testing service. NADSI Test Facilities should have portable test equipment to provide maximum flexibility to the using test customer.

6.1 NADSI Test Set. The NADSI Test Set will be capable of testing the NADSI interfaces as specified in STANAG 4575 and will be tested and validated as part of the NADSI Test Facility accreditation.

6.2 Accreditation of NADSI Test Facilities.

6.2.1 Formal Request for NADSI Test Facility Accreditation. The NATO Body sponsoring the proposed NADSI Test Facility will submit a formal accreditation request to the NADSI Custodian. An approved checklist detailing the required system hardware, software, test equipment, and test procedures will be completed and attached. The request will state the preferred test location and at least three-accreditation test dates.

6.2.2 NADSI Test Facility/Set Accreditation. The NADSI Custodian will accredit all NADSI Test Facilities. A validated NADSI Test Set will be used to certify the NADSI Test Facility's compliance to STANAG 4575, the NADSI Test Requirements Document, and to test the interface as required in the approved procedure. Initially, the Joint Interoperability Test Command (JITC) NADSI Test Set will be used to accredit NADSI Test Facilities; once accredited, a NADSI Test Facility can be used under the direction of the Custodian to accredit other NADSI Test Facilities.

The JITC NADSI Test Set will be tested with several NADSI devices to ensure it accurately tests and evaluates NADSI systems for compliance to STANAG 4575 and the NADSI Test Requirements Document. The NADSI Custodian will certify the JITC NADSI Test Set based on successful test assessments and reports.

6.3.3 Accredited NADSI Test Facility Maintenance. The NADSI Test Facility will report all successful NADSI system compliance tests to the NADSI Custodian within 30 calendar days of test completion. The report will include as a minimum the items listed in paragraph 5 in this annex. The NADSI Test Facility will submit an annual report summarizing test activities and a statement that required test equipment had been calibrated. The NADSI Test Facility will implement hardware and software changes as directed by the NADSI Custodian to accommodate program and possible STANAG changes. Modifications and changes are addressed in paragraph 6.3.4.

6.3.4 Modifying an Accredited NADSI Test Facility. The Accredited NADSI Test Facility will notify the NADSI Custodian of planned or required modifications to the test facility. The notification will include the reason for modifying the test facility and what hardware and software is being modified or replaced. The NADSI Custodian will determine if the NADSI Test Facility needs to be reaccredited.

CONFIGURATION MANAGEMENT PLAN

1. Purpose. The purpose of this Annex is to provide the framework for the management of STANAG 4575 and all associated documents.

1.1 Related Documents.

1.1.1 Included Documents. Documents included in this configuration management structure are as follows:

1. STANAG 4575
2. AEDP-6 NADSI Implementation Guide
3. Other as designated by the STANAG 4575 Custodian

1.1.2 Other Referenced Documents.

AAP-3 *Procedures for the Development, Preparation, Production, and the Updating of NATO Standardization Agreements (STANAGs) and Allied Publications (APs)*

2. Scope. This document provides the framework for configuration management of STANAG 4575 and all associated documents. The participating NATO member nations define their respective levels of participation and all NATO member nations have equal opportunity to have their respective positions voiced in the STANAG 4575 community. Decision made within this framework are subject to final approval of NATO NAFAG Air Group IV (AG IV), in order to ensure the proper placement of STANAG 4575 within the overall NATO ISR Interoperability Architecture (NIIA). Overall, the configuration management structure is consistent with the NATO guidelines defined in AAP-3, *Procedures for the Development, Preparation, Production, and the Updating of NATO Standardization Agreements (STANAGs) and Allied Publications (APs)*. The key element of the configuration management process is the management of requests for change by individual nations.

3. STANAG Management Organization.

3.1 General.

3.1.1 NATO Nation Responsibility. Each NATO member nation is responsible for funding its own participation. Although each NATO member nation can assign representatives to the STANAG activities defined herein, any assigned representatives are expected to be active participants.

3.1.2 Participation Requirements. Should the STANAG 4575 Custodian be unable to properly execute business due to repeated lack of participation at the meetings, the Custodian will report the lack of participation to AG IV and AG IV will request the AG IV representative of the respective nation(s) to either withdraw from STANAG 4575 participation or appoint a new STANAG 4575 representative who will be able to fully participate.

3.2 Custodian/Chairman. The STANAG 4575 Custodian also serves as the chairman of all meetings of the configuration management functions. The Custodian is responsible for all STANAG 4575 activity. Specific duties include, but are not limited to the following tasks:

1. Tracks changes and provides "official" copy for promulgation
2. Reports to AG IV on status
3. Chairs STANAG 4575 Custodial Support Team (CST) meetings
4. Directs activity of STANAG 4575 Administrative Support Team (AST)

3.2.1 Tasking and Reporting Responsibility. The Custodian is the only individual to receive tasking from and report to AG IV on STANAG 4575. This authority can be delegated to other members of the STANAG 4575 community, but responsibility for the tasking and reporting resides with the Custodian.

3.3 STANAG 4575 Custodial Support Team (4575 CST). The Custodial Support Team decides on the changes to be made to STANAG 4575.

3.3.1 STANAG 4575 Representatives. The respective AG IV Representative appoints representatives to the 4575 CST. Each NATO member nation can appoint a representative to the 4575 CST by providing the name, organization, address, telephone and facsimile numbers, and electronic mail address of their 4575 CST member to the STANAG 4575 Custodian. (The STANAG 4575 Custodian will document the members of the 4575 CST and provide the information to the AG IV Secretary for recording in the AG IV decision sheet.) The national representative to the 4575 CST can be from government or industry as chosen by the AG IV representative. The national representative to the 4575 CST is the official spokesman for all participants from that nation.

3.3.2 National Representative's Responsibilities. Each national representative will define procedures for establishing the respective national position on proposed changes. These procedures can use whatever process is appropriate to that nation, but ultimately the national representative will voice the official national position to the 4575 CST.

3.3.3 National Representative's Delegation Authority. The authority of the national representative can be delegated to another individual from that nation in absence of the national representative. The delegation will be in writing to the Custodian/chairman prior to the start of the meeting at which the delegation of authority is effective. The substitute representative will have all authority and responsibility of the regular representative.

3.3.4 Other Participation. Other individuals from nations with representatives may participate at discretion of national representatives or the Custodian/chairman. The participants can be additional government personnel or contractor personnel. The intent of having additional personnel participate is to provide technical, operational, or procedural expertise that may not be resident with the representatives and to allow participation by those who are developing systems using STANAG 4575.

3.3.5 Other Interested Parties. Individuals from non-NATO nations may participate in 4575 CST meetings only at the request of the Custodian, and only to explain/defend changes proposed by the individual or a non-NATO nation.

3.4 STANAG 4575 Administrative Support Team (4575 AST). The STANAG 4575 Administrative Support Team provides the necessary planning and maintenance activities to manage STANAG 4575.

3.4.1 4575 AST Member Selection. The members of the 4575 AST are selected by the Custodian. Members are selected based on tasking, resources, and remain members of the 4575 AST at the discretion of the Custodian.

3.4.2 4575 AST Member Functions. The members of the 4575 AST will perform the following functions.

1. Prepare for meetings by identifying locations and dates for the meetings, preparing announcements, coordinating security clearances, providing guidance to meeting hosts, and preparing presentation materials and handouts.
2. Presentation of recommended changes during the meetings.
3. Track recommended changes submitted through 4575 CST channels.
4. Prepare minutes of all meetings.
5. Prepare revisions for distribution to AG IV secretary and members.
6. Perform the configuration management STANAG 4575, including maintaining the current version of document.
7. Disseminate all proposed changes to the 4575 CST as they are received and logged.

3.5 AG IV WEB Page. The AG IV Secretary is responsible for maintaining the configuration management of the AG IV web page on which STANAG 4575 is posted.
The Secretary will update the postings for past and upcoming meetings based on information provided by the Custodian. Once changes to STANAG 4575 are approved, the Secretary will post the revision to the AG IV web page within 45 days of the meeting, unless other arrangements are agreed during the AG IV meeting. The Secretary will maintain a list of the national representatives to the 4575 CST on

the web page, based on the nominations made during the AG IV meetings as documented in the AG IV meeting decision sheets.

3.6 Special Teams. The Custodian will have the authority to convene special teams to examine major technical issues that are beyond the scope of routine change proposal activity. Technical issues of this type can include major changes to the format or development of future strategies for advanced data storage, interface and data download. The Custodian can chair the special team or select another member of the NADS community to chair the special team and report on its progress. The members of the team will be appointed by the Custodian based on recommendations from the national representatives. The Custodian will identify any special teams, including the members, tasking, planned schedule, and expected products, to AG IV.

4.0 Change Identification.

4.1 Change Request Procedure. All representatives can submit change requests that change the content or structure of STANAG 4575. Other personnel requesting changes will submit their requests through the respective national representatives. For persons from NATO nations without formal representatives on the 4575 CST, the change requests will be submitted through their respective AG IV representative.

4.1.1 Submission of Changes from non-NATO Nations. Individuals from non-NATO nations may submit change proposals directly to the Custodian. In addition to the information contained in the Standardization Document Change Proposal (SDCP) form (Appendix 1), the submission will include a cover letter which clearly identifies the name, title, organization, and contact information of the submitter, as well as a statement as to whether the submission is in response to a national government requirement. If the change supports a national government requirement, the requirement should be identified, and an endorsement included which is signed by an appropriate government representative. In all cases, the submitter should be prepared to attend the 4575 CST meeting to explain and/or defend the proposed change.

4.2 Change Request Format. All change requests will use a standard format, either by completing the form in Appendix A or electronic mail containing the same information and order as the form. The paper form can be submitted either through the mail or by telefax. The change request is submitted to the appropriate national representative, who then endorses the change and forwards it to the Custodian. The Custodian provides the change request to the 4575 AST for logging and dissemination for discussion and review.

4.3 Class of Changes. All change requests will identify the proposed change as either Class I (amendments of substance) or Class II (editorial amendments). Class I changes modify the functionality of standard (requires s/w change to comply). This includes changes to the order of fields, changes to the allowed or required values for a field, or additions/deletions of fields or approved values. Class I changes are those identified as changes of substance in paragraph 214.2. of AAP-3(G). Class II changes are for administrative or editorial revisions or to clarify the usage of the STANAG. These changes are those identified as editorial amendments in paragraph 214.3 of AAP-3(G).

5. Configuration Management. Configuration Management, as defined in AAP-3(G), defines the top-level process. It specifies that once changes are produced, they should be forwarded to the NATO Standardization Agency (NSA). AAP-3(G) does not specify the process within the sponsoring agency or for the Custodian to use in recording proposed changes and managing the change approval process. The primary purpose of this plan is to specify the process to be used by the STANAG 4575 Custodian.

The STANAG 4575 Configuration Management will be conducted on a cyclic basis. The process is shown in Figure E-1. Changes can be submitted at any time, but will be reviewed by the 4575 CST on a quarterly basis as required. Presentations to AG IV will be performed on a semiannual basis to coincide with the AG IV meetings.

5.1 Routine Business Activities. These activities can be performed at any time by the appropriate personnel.

5.1.1 Change Requests. Change requests are submitted by any interested individual or organization to the respective national representative using the form included in Appendix 1. A list of national representatives will be maintained by the AG IV Secretary and included on the web page.

5.1.1.1 National Representative's Authority for Change Requests. The national representatives have disapproval authority over any proposed change from their respective nation prior to submission to the Custodian. If approved, the national representative endorses the change request and forwards the change request to the Custodian.

5.1.1.2 Direct Submission by non-NATO Nations. Change request submissions from individuals in non-NATO nations are submitted directly to the Custodian. The Custodian will review the submissions and approve for 4575 CST consideration those proposals that have potential benefit to the NATO community. Rejected proposals are returned to the submitter with the reasons for rejection.

5.1.2 Change Request Routing. The Custodian provides the change request to the 4575 AST for logging into the configuration management system. At the direction of the Custodian, proposed changes can be disseminated by the 4575 AST at any time for review.

5.2 Quarterly 4575 CST Meetings. The 4575 CST will meet quarterly unless there are no outstanding change proposals. The Custodian will formally call the meeting based on the arrangements established by the 4575 AST.

5.2.1 Procedure for Proposed Changes. Proposed changes are compiled and distributed to all national representatives no less than fourteen days prior to the meeting. The format of the change compilation is shown in Appendix 1. National representatives then distribute the proposed changes to other interested individuals from the respective nation. National representatives and others are directed to establish impact of the proposed changes. The respective national positions are determined by procedures established by each nation. If a nation is unable to attend a 4575 CST meeting, the nation may submit written comments to the Custodian prior to the 4575 CST meeting. The comments will be provided to all attendees for consideration during deliberations.

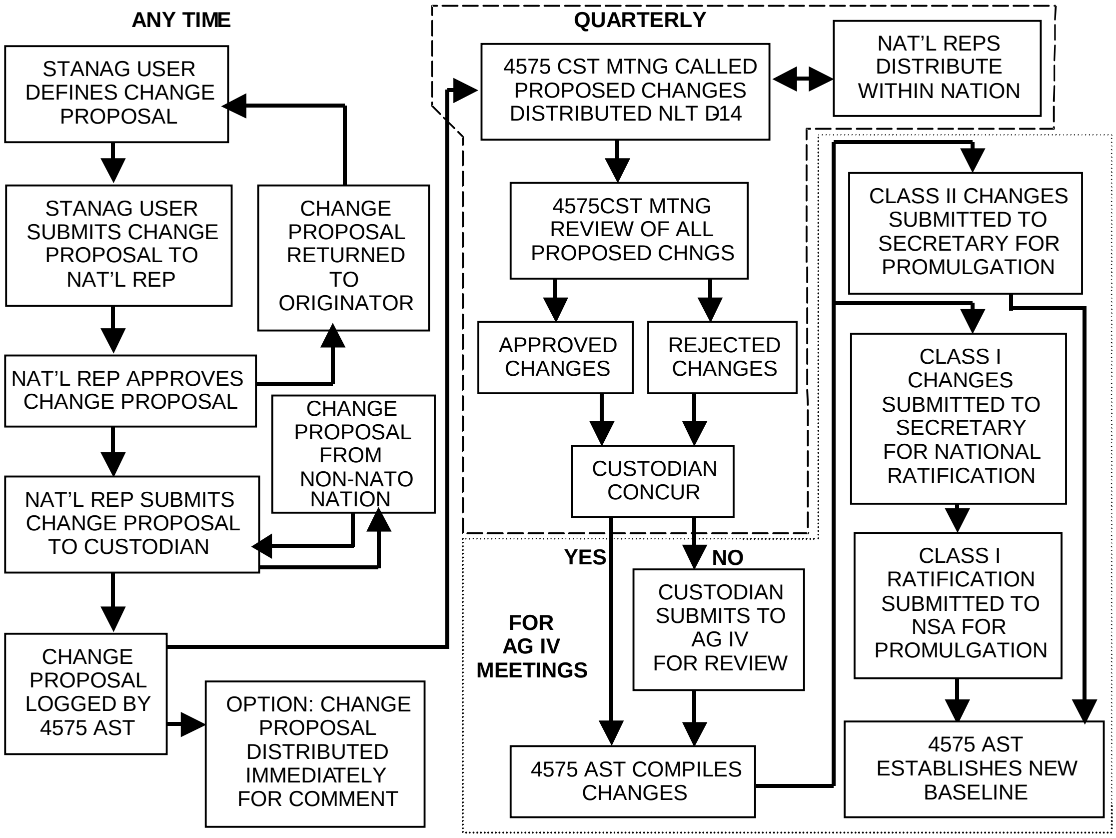


FIGURE E-1; CM PROCESS FLOW

5.2.2 Discussion of Change Proposals. During the 4575 CST meeting, each proposed change is discussed. Change proposals are discussed under direction of the Custodian. Change proposals can be deferred pending additional investigation/review, for which the Custodian assigns responsibility for addition study/review, or changes can be voted independently or in groups at discretion of Custodian.

5.2.2.1 Voting on Change Proposals. Only the national representatives vote on final configuration decisions. Class I changes require unanimous consent of national representatives (or designated alternates) in attendance and voting. Class II changes require a majority vote of national representatives in attendance and voting. Ties are decided by the Custodian.

5.2.2.2 Custodian's Options and Approval Authority. The Custodian can defer the decisions of the national representatives for AG IV review, request additional discussion and review by the national representatives, or approve them immediately. Approved decisions are incorporated into the STANAG by the 4575 AST. When deemed necessary by the Custodian, unapproved decisions are presented to AG IV for final decision. Those changes approved by the Custodian or ratified by AG IV are incorporated into the STANAG by the 4575 AST.

5.3 AG IV Meetings. At the AG IV meetings, two topics are presented along with the general status of the STANAG 4575 activities. The Custodian can present any change proposals approved or rejected by the 4575 CST for which the Custodian disagreed. Air Group IV makes the final decisions on those items presented for which the Custodian disagreed with the 4575 CST national representatives. The 4575 AST then incorporates the revisions as directed by Air Group IV.

In addition, the Custodian presents to AG IV completed amendments to the STANAG along with a summary of the changes for ratification. Revisions with Class I changes are then submitted to the AG

IV Secretary to formally present the modifications to the nations for ratification. Revisions with only Class II changes are considered ratified with AG IV approval. Regardless of the ratification process used, after ratification, the Secretary posts the revised STANAG to the AG IV web page and submits it to the Chairman of the MAS for promulgation.

6.0 Meeting Procedures.

6.1 Language. All meetings will be conducted in English. Those nations requiring the materials in different languages are responsible for translating the materials. Attendees to the meetings should be proficient enough in English to contribute to the meeting in English.

6.2 Meeting Advance Notice. All meetings will be announced with a minimum of 60 days notice.

6.3 Quorum. The quorum for approving changes for submission to AG IV is 2 nations formally represented by approved representatives or their alternates.

6.4 Meeting Minutes. Minutes of all formal meetings will be distributed within 14 days of the completion of the meeting. The minutes will include a record to document approved and disapproved changes, identify the status of all outstanding changes, and identify issues to be taken forward to AG IV.

6.5 Memorandum of Resolution. If, because of disagreement between the Custodian and the majority of national representatives, items are taken forward to AG IV for a final decision, the Custodian and 4575 AST will prepare a memorandum for record, distributed to all national representatives, which will identify results of AG IV discussions/decisions, and provide status of all changes. This memorandum will be disseminated to the national representatives within 14 days of AG IV meeting.

STANDARDIZATION DOCUMENT CHANGE PROPOSAL (SDCP) FORM

INSTRUCTIONS

1. Change proposals may be submitted on this form through either mail or telefax, or by electronic mail following the same order and content as this form.
2. Originator completes sections 1-16.
3. Originator forwards to the respective national representative. National representative is official representative to 4575 CST, or if none from the originator's nation, then the representative to Air Group IV. (See the NATO NAFAG AG IV Internet web page for names and addresses.)
4. National representative approves or rejects proposal from their nation by completing sections 17-25.
   - Approved proposals are forwarded to the STANAG 4575 Custodian.
   - Rejected proposals are annotated with the reason for disapproval and returned to the originator.

Note: This form may be used to submit changes to any document included in the STANAG 4575 data set. This form may not be used to request copies of these documents. The documents are available on the NATO NAFAG AG IV Internet home page (www.nato.int/structur/AC/224/home.htm), or through normal NATO document distribution channels.

RECOMMENDED CHANGE: (continue on additional sheets as necessary) page | | of | |

1. Document Number: AC/224-D/950	2. Document Version/Release Number: Edition 1/ Ratification Draft 1	3. Document Date: 17 July 2001

4. Document Title:
STANAG 4575, NATO Advanced Data Storage Interface (NADSI)

| 5. Proposed Change to: (Section, Paragraph, Line, Page) | 6. Change Class: I | | II | |

7. Current Wording:	8. Proposed Wording:

9. Reason/Rationale:

10. Originator's Name:	13. Originator's Telephone Number:
11. Originator's Organization:	14. Originator's Telefax Number:
12. Originator's Mailing Address:	15. Originator's E-Mail Address: 16. Date Submitted:
17. Nat'l Rep Name:	20. Nat'l Rep Telephone Number:
18. Nat'l Rep Organization:	21. Nat'l Rep Telefax Number:
19. Nat'l Rep Mailing Address:	22. Nat'l Rep E-Mail Address: 23. Date of Approval/Rejection:

24. Change Proposal: Approved |__| Rejected: |__|
25. Rejection Rationale:

Mail, Telefax, or E-Mail Change Proposals To: STANAG 4575 Custodian	26. Date Logged by 4575 AST/initials:

APPLICATION NOTES

1. Scope. This Annex provides application notes for the use of the NADS Interface based on practical experience and lessons learned from previous testing and demonstrations during the STANAG development. It will be updated with information as the certification phase defined in Annex D and the NATO-wide interoperability demonstrations progress.

2. Testing of NADS Interface with CIGSS Test Van at NAWC, China Lake, CA; 3 May 2001.

2.1. Background. The testing addressed in this section was required prior to the release of STANAG 4575 to NATO Air Group IV for ratification in order to verify that the STANAG is correct and complete. By having two or more independent organizations implement the interface and verify that the data stored can be recovered, a reasonable level of assurance is provided that there are no missing or unclear elements of the interface definition.

2.2 Objective. The objective of the testing was to confirm that image files previously recorded on a manufacturer's RMM (GDIS Disk Array) could be downloaded via the NADSI Fibre Channel port to the U.S. Common Imagery Ground/Surface Station (CIGSS), using the NADSI command structure and file system, and that those image files could be replicated from the downloaded data.

2.3 Results. The test identified a potential problem in that the operating system used (Sun Solaris 2.6) requires that an identifier be written to the device before any data could be read. This is not allowed by the STANAG. In subsequent teleconferences, it was determined that this seemed to be unique to the Sun library and other operating systems do not have this limitation. It was further determined that a different approach to the Sun driver would fix the problem for Solaris. As such, no change was required in the STANAG. It was agreed that this problem should be highlighted to the community in the AEDP. Because of the result of the test, it was agreed that the STANAG was complete and correct and could be submitted for ratification (which was subsequently completed).

2.4 Lessons Learned. It was clear from this first testing of the NADS Interface with the CIGSS Test Bed that the GS processor software may provide different levels of functionality when used with that RMM NADS interface.

2.4.1 Required Functionality. The drivers and software control of the RMM are required to provide for data download through the NADS Interface to the ground station processor. It is intended that this capability include identification of data files in the RMM and download of individual files as well as the option to download the complete memory of the RMM. The driver must be backward compatible whenever it is updated.

2.4.2 Optimal Functionality. There is no guarantee that any RMM will respond to recommended or optional commands from the ground station via the NADS Interface. The ground station must use discovery techniques to determine available commands and functions for a given RMM. It is expected that each ground station will develop their driver differently such that it best fits their system architecture. The driver provides the hardware interface between the RMM and the self-contained ground station processor application, including the API as shown in Figure E-1-1 below.

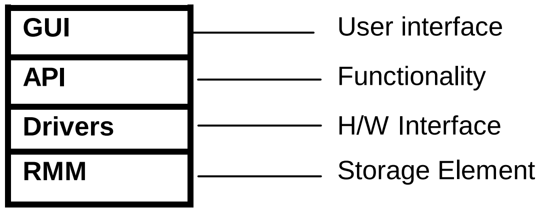


Figure-E-1-1 - RMM Interface to Ground Station (GS) Processor

3. NADS Interface Demo at UAV Topical Meeting, NATO HQ, Brussels Belgium; 23-24 Jan. 2003

3.1 Background. The demonstration included a QinetiQ supplied UK ground system (an SGI workstation with the UK software for the NADSI interface and an image processing capability), an L-3 Communications, Communivations Systems- East Solid State Recorder (SSR), which was a S/TAR recorder in the SHARP configuration and a General Dynamics Advanced Information Systems disk-based RMM. Both recorders had been loaded with the supplied test files and test imagery. The recorders were connected to the ground station through a Fibre Channel hub. The data was downloaded and processed individually from each RMM. Power supplies and converters were used to power the units. Both units underwent an initial integration at QinetiQ in the UK prior to being driven to Brussels.

3.2 Results. The ground station demonstrated the ability to command the download of files from both of the RMMs via the NADS Interface and accept, display and save the transferred files. The files included test sequences and imagery. The disk and the SSR were demonstrated individually using the identical data and commands. The directories were displayed and stored. The data was stored on the system storage unit and individual data files were evaluated and displayed. The test data was downloaded directly to the ground station and was compared visually to the transferred data.

3.3 Lessons Learned. Challenges with authorizations, equipment availability, integration and set up in Brussels caused the demonstration to be assembled at the last minute (within 2 weeks from initiation to demo). This schedule did not allow time for expected integration and test prior to the demo and forced the use of existing available hardware (engineering models). This resulted in a series of last minute problems related to cables, connectors, fibre channel hub, test data choice, and available power. Although the demonstration was successful, it came together at the very last moment and it would have been very difficult to explain the technical issues or a failure to operate, to the NATO audience. The lesson learned is that the systems must be integrated and tested prior to public use. Power availability and conversion must be addressed, knowing what quality and variances could be experienced. Alternate connection methods and converters should be verified prior to testing. Last minute demonstrations may not be appropriate unless the system can be verified operational with all components in place.

GLOSSARY

(ACRONYMS AND DEFINITIONS)

100Base-T	The Ethernet standard, 100BaseT, is defined by the IEEE 802.3 committee for two pairs of unshielded twisted pair (100BaseTX), for four pairs of unshielded twisted pair (100BaseT4), and for fiber optic cable (100BaseFX).
10Base-5	The implementation of the IEEE 802.3 Ethernet standard on thick coaxial cable. Thick, or standard Ethernet, as its commonly called, runs at 10Mbits/sec. It uses a bus topology and the maximum segment length is 500 meters.
Access Method	An access method is the set of rules by which the network arbitrates access among the nodes. Collision Sense Multiple Access with Collision Detection and token passing are two access methods commonly used in LANs.
Access Time	The time from the start of one access to the time when the next access can be initiated.
ADSS	Advanced Data Storage System
AEDP	Allied Engineering Documentation Publication
AF	Air Force
AF DCGS	Air Force Distributed Common Ground System
AGE	Aerospace Ground Equipment
AGE Cart	Aerospace Ground Equipment used to service, test or operate with aircraft installed or mounted equipment. It is often mounted on a handcart or vehicle.
AIP	ASARS Improvement Program
ANG	Air National Guard
ANSI/NCITS	American National Standards Institute / National Committee for Information Technology Standards
AP	Allied Publication
API	Application Program Interface
Applicable ICD	Company Applicable Interface Control Document (ICD)
ARC Net	Data point designed this 2.5Mbit/sec token-passing, star-wired network in the 1970s. Its low cost and high reliability has made it attractive to companies on a tight network budget.
ARITA	Airborne Reconnaissance Information Technical Architecture
ASARS	Advanced Synthetic Aperture Radar System
AST	Administrative Support Team
ATARS	Advanced Tactical Air Reconnaissance System
ATM	Asynchronous Transfer Mode - An international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed length (53 byte) cells. Fixed length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3.
ATR	Automatic Target Recognition
Attenuation	A reduction in magnitude (normally applied to a signal)usually stated as a ratio
ASN	Abstract Syntax Notation
Auditing	A method to monitor network traffic by tracking every users action in a network.
Bandwidth	Bandwidth is the difference between the highest and lowest frequency a channel can conduct, measured in MHz. Also used to describe the rated throughput capacity of a given network medium or protocol.
Baseband (Parallel)	Digital data transmission (bits 1 or 0). Signal flow is omni directional. Using repeater to fight attenuation.
Beaconing	Technique in Token ring topology to detect signal failure.
BER	1.Bit Error Rate, 2. Basic Encoding Rules
BCS	ISO Basic Character Set

BIOS	Basic Input/Output System
bps	Bits Per Second
Broadband **(**Serial**)**	Analog data transmission. Signal flow is unidirectional. Using amplifiers to regenerate signals
Buffer	An amount of memory that temporarily stores data to help compensate for differences in the transfer rate from one device to another.
Byte	Eight bits; historically, one word of data
C4ISR	Command, Control, Communications, Computers, Intelligence Surveillance and Reconnaissance
CAD	Computer Aided Design
CAS	CIGSS Acquisition Standards
CASH	CIGSS Acquisition Standards Handbook
CAWS	Commercial Analyst Work Station
CBER	Corrected Bit Error Rate is a measure of the reproduced quality of the user data after all decoding and correction has been accomplished.
CD-ROM	Compact Disk-Read Only Memory
CDL	Common Data Link
Certification	Comprehensive evaluation of the technical and non-technical features of an automated information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified requirements.
CHBDL	Common High Bandwidth Data Link
CIA	Central Intelligence Agency
CIGSS	Common Imagery Ground/Surface System
CINC	Commander in Chief
CIO	Central Imagery Office
CIP	Common Imagery Processor
CL	Compliance Level
Client	Client is the computer that requests resources-files, print, and application service from the server.
CM	Configuration Management
COE	Common Operating Environment
CONOPS	Concept Of Operations
CONUS	Continental United States
Compression	Compression is the reduction in size of data in order to save space or transmission time. For data transmission, compression can be performed on just the data content or on the entire transmission unit (including *header* data) depending on a number of factors.
Cooperative Multitasking **-**	The operating system is reliant to the application to give up the processor when needed.
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CRD	Capstone Requirements Document
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance. AppleTalk access method.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection - Contentation Method. Ethernet access method specified in IEEE 802.3
CST	Custodial Support Team
CSU/DSU	Channel Service Unit/Data Service Unit used in DDS lines. CSU/DSUs converts digital signal in media from customers' location, such as a router, to the telephone company's digital network.
DARP	Defense Airborne Reconnaissance Program
DARPA	Defense Advanced Research Projects Agency
DBMS	Database Management System
DCGS	Distributed Common Ground System

DCGS-I	Distributed Common Ground System-IMINT
DCRSi	Digital Cassette Recording System Improved
DDS	Digital Data Service, or DATAPHONE Data Service. DDS is a fixed-bandwidth point-to-point digital service.
Declassification	A decision process supported by procedures which allows unrestricted release of a data storage element
Device Driver	Software that forms the interface between specific computer hardware and the computer operating system.
Driver	A software interface between two or more entities.
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DoDIIS	Department of Defense Intelligence Information System
DT&E	Developmental Test and Evaluation
DVD	Digital Versatile Disk
EDAC	Error Detection And Correction is the encoding that is incorporated into the stored data, used for data correction during reproduction and is removed from the data during data recovery.
EEPROM:	Electronically Erasable Programmable Read Only Memory
EIA	Electronics Industry Association
ELT	Electronic Light Table
Encryption	Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.
ENET	Ethernet
EMC	Electro-Magnetic Compatibility
EMI	Electro-Magnetic Interference
EO	Electro-Optical
FDDI	Fiber-Optic Distributed Data Interface - A LAN standard, defined by ANSI X3T9.5, specifying a 100-Mbs token passing network using fibre-optic cable, with transmission distances of up to 2km. FDDI uses a dual-ring architecture to provide redundancy.
FC-PLDA	Fibre Channel Private Loop SCSI Direct Attach is an NCITS standard which is optimized for SCSI and Fiber Channel data transport.
Fibre Channel Interface	**–** An industry standard interface compatible with both wire and optical connection for the transfer of data and commands.
Flash Memory	"Flash Erase", non-volatile solid-state memory, Nonvolatile storage that can be electrically erased and reprogrammed so that software images/data can be stored, booted, and rewritten as necessary.
Flying Lead	For the NADSI application, a cable that is attached to the ground station at one end and has a NADSI connector on the other. For the NADSI application it connects the NADSI interface to a ground system
FO	Fiber Optic
FTP	File Transfer Protocol - An application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959
GB	Gigabytes
Gbps	Giga bits per second
GFI	Government Furnished Information
GFS	Government Furnished Software
GH	Global Hawk
GIAS	Geospatial and Imagery Access Service
GIF	Graphics Interchange Format
GIMS	Geospatial Imagery Management System

GIS	Geographical Information System
GOTS	Government off-the-shelf
GS	Ground Station
GSE	Ground Support Equipment
GUI	Graphical User Interface - A user environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored. Conventions such as buttons, icons, and windows are typical, and many actions are performed using a pointing decide (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms utilizing GUIs.
H/C	Hardcopy
HAE	High Altitude Endurance (UAV)
HCL	Hardware Compatibility List. Software that enables one to detect the hardware minimum requirement for an operating system.
HiPPI	High Performance Parallel Interface
HiPPI-FP	HiPPI Framing Protocol
HMMWV	High Mobility Multi-purpose Wheeled Vehicle
HiPPI-PH	HiPPI Physical Layer
HRU	Hardcopy Reconstruction Unit
HSI	Hyper-Spectral Imagery
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
H/W	Hardware
I&T	Integration and Test
IA	Imagery Analyst
IAB	Internet Architecture Board
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronic Engineers
IESS	Imagery Exploitation Support System
IG	Intelligence Group
IMINT	Imagery Intelligence
INFOSEC	Information Security
INT	Intelligence
Interoperability	Interoperability testing is the process of assessing the ability of a system to exchange usable electronic information with systems of other services or nations as specified in its requirements documents. Specialized test tools are used to monitor performance of products to determine if the proper actions and reactions are produced. A system is certified as interoperable at the completion of successful interoperability testing.
IOC	Initial Operational Capability
IP	Internet Protocol - A network-layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791. IPv4 (Internet Protocol version 4) is a connectionless, best-effort packet switching protocol.
IPA	Image Product Archive
IPL	Image Product Library
IPT	Integrated Product Team
IR	Infrared
IRLS	Infrared Line Scanner
IS	Information Systems
ISDN	Integrated Services Digital Network. A telephone service designed to carry both voice and data information.
ISO/IEC	International Organization for Standardization / International Electro-technical Commission

ISP	Internet Service Provider. A Company or organization that sells Internet accesses. ISPs may offer many levels of access from dial-up host-based services to direct network connections (WAN).
ISR	Intelligence, Surveillance, and Reconnaissance
ISU	Integrated Service Unit. See CSU/DSU.
I/O	Input and Output
IT	Information Technology
IU	Interface Unit
J-2	Intelligence Directorate of the Joint Staff
JAC	Joint Analysis Center
JAMA	Joint Airborne MASINT Architecture
JASA	Joint Airborne SIGINT Architecture
JCA	JSIPS Concentrator Architecture
JCS	Joint Chiefs of Staff
JFIF	JPEG File Interchange Format
JIC	Joint Intelligence Center
JICD	Joint Interface Control Document
JIEO	Joint Interoperability and Engineering Office
JION	Joint Interoperable Network
JITC	Joint Interoperability Test Command
JITF	Joint Integration Test Facility
JIVA	Joint Intelligence Virtual Architecture
JPEG	Joint Photographic Experts Group
JROC	Joint Requirements Oversight Council
JSIPS	Joint Service Imagery Processing System
JSIPS-N	JSIPS Navy
JSTARS	Joint Surveillance and Target Attack Reconnaissance System
JSTARS - CGS	JSTARS - Common Ground Station
JTA	Joint Technical Architecture
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System
KB	Kilobytes
Kbps	Kilobits per second
KCOIC	Korean Combat Operations Intelligence Center
LAEO	Low Altitude Electro-Optical
LAN	Local Area Network - A high-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LAN standards specify cabling and signaling at the physical and data link layers of the OSI reference model.
LOS	Line of Sight
LSB	Least Significant Byte
MAE	Medium Altitude Endurance (UAV)
Magic Number	An identifier for the directory block. This is a value chosen to support discovery of lost directory entries and directory reconstruction after a fault.
MAEO	Medium Altitude Electro-Optical
MAS	Military Agency for Standardization
MASINT	Measurement and Signature Intelligence
MB	Megabytes
Mbps	Megabits per second
MFLOPs	Million Floating Point Operations per Second
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MIPS	Millions of Instructions per Second
MIST	Modularized Interoperable Surface Terminal

Modem	Modulator-demodulator**,** A device that converts digital signal waves (computer signal) to analog waves (telephone line), and vice versa.
MPEG	Moving Picture Experts Group
MSB	Most Significant Byte
MSI	Multi-Spectral Imagery
MTI	Moving Target Indicator
Multitasking	(1) A mode of operation that allows concurrent performance or interleaved execution of more than one task or program. (2) A process that allows a computer or operating system to run multiple applications or tasks concurrently by dividing the processor's time among them rapidly. With computers that have only one processor, the programs/tasks are not actually running at the same time, the OS simply switches between tasks so quickly that the tasks appear to be running in parallel. The terms multitasking and multiprocessing are often used interchangeably, although multiprocessing implies more than one CPU is involved.
NAFAG	NATO Air Force Armaments Group
NADSI	NATO Advanced Data Storage Interface
NAFAG	NATO Air Force Armaments Group
NATO	North Atlantic Treaty Organization
NED	NATO Effective Date
NETBLT	Network Block Transfer (protocol)
NB	Narrow-Band
NCIS	NATO Common Interoperability Standards
NIC	Network Interface Card **-** used for connecting computer to the network.
NIIA	NATO ISR Interoperability Architecture
NIFTI	NATO Interoperability Framework Testing Infrastructure
NIL	National Image Library
NIMA	National Imagery and Mapping Agency
NIMP	NATO Interoperability Management Plan
NITF	National Imagery Transmission Format
NITFS	NITF Standard
NL	NIMA Library
NLT	No Later Than
Non-volatile	Memory Media that retains data when power is removed
NPIC	National Photographic Interpretation Center
NRO	National Reconnaissance Office
NRT	Near-Real Time
NSA	NATO Standardization Agency
NSIF	NATO Secondary Imagery Format
N-TIS	Navy Tactical Input Segment
NTISSP-9	National Telecommunications and Information Systems Security Policy
NTM	National Technical Means
NTSC	National Television Standards Committee
NVS	Non-Volatile Storage
OASD	Office of the Assistant Secretary of Defense
OCONUS	Outside Continental United States
OC-n	Optical Channel n (e.g., OC-3, OC-48)
ODT	Optical Digital Technology
ONI	Office of Naval Intelligence
ORD	Operational Requirements Document
OS	Operating System
OSD	Office of the Secretary of Defense
OSF	Open Systems Foundation
OSI	Open Systems Interconnection, . An international standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multi-vendor equipment interoperability.

OSI Reference Model-	A network architectural model developed by ISO and ITU-T. The model consists of seven layers, each of which specifies particular network functions such as addressing, flow control, error control, encapsulation, and reliable message transfer.
OT&E	Operational Test and Evaluation
Owning Body	The NATO Country/Command/Organization/Service that is responsible for Program/Product Management of a system or subsystem.
PPI	Preprogrammed Product Improvement
PACAF	Pacific Air Forces
Packet	A logical grouping of information that includes a header containing control information and (usually) user data. Packets are most often used to refer to network-layer units of data.
PAL	Phase Alternating Line
PASV	Passive
PBIT	Periodic Built In Test
PCE	Platform Communications Element
PED	Processing, Exploitation, and Dissemination
PIAE	Profile for Image Access Extensions
Plug and Play	Plug and Play technology offers automatic settings for hardware in computer. The term signifies plugging the device, for example Network Card and then automatically plays or run the computer without manual configuration by users.
PMO	Program Management Office
POC	Point of Contact
POSIX	Portable Operating System Interface
PPP	Point-to-Point Protocol. A replacement for SL/IP designed to provide IP services via modem.
Preemptive Multitasking	**-** The operating system is in control of the processor. It can take away the processor when other application needs it.
PRD	Pseudo Random Data -A generated sequence which repeats and is used as a test data sequence which incorporates various run lengths of 1s and 0s. The data sequence is defined in accordance with the repetition cycle, e.g. 2e23-1, 2e7-1, etc.
PVC	Permanent Virtual Circuits **-** PVC is similar to leased-line that is permanent and virtual, used in advanced packet switching technique. Customer pays only for the time the line is used.
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory - Volatile memory that can be read and written by a microprocessor.
Random Data	Any data sequence that is undefined and non-repeating. When used for over-write in declassification, random data refers to any non-repeating or arbitrary data pattern which is not predictive.
Recorder	The entity that includes the input and control interfaces, RMM, and functionality required to properly record data.
Redirector	Part of a network driver that intercepts I/O requests to be put on local service or redirect it to the ongoing network. Redirector resides in the presentation layer.
Repeater	Used in digital transmission to regenerate signals. Repeater works at the OSI physical layer, thus has no addressing, translation capability and cannot ease network congestion.
RFI	Radio Frequency Interference
RG-58U	A standardized type and impedance code designation for coaxial cable
RISC	Reduced Instruction Set Computers
RMM	Removable Memory Module. That element of the data recorder that contains the stored data and NADS Interface and is easily removed for download. This can range from a replaceable subassembly to the entire recorder, as appropriate.

RMS	Reconnaissance Management System
RPF	Raster Product Format
ROM	Read Only Memory **-** Nonvolatile memory that can be read, but not written, buy the microprocessor.
RULER	A software application for doing mensuration and related analysis functions
S-VHS	Super VHS
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SCI	Sensitive Compartmented Information
SCSI	Small Computer System Interface**,** (suffixed by version number e.g. SCSI-3 is version 3)
SCSI ULP	Small Computer System Interface Upper Level Protocol
SDE	Support Data Extension
SDH	Synchronous Digital Hierarchy
SEM	Softcopy Exploitation Management
SGML	Standard Generalized Markup Language
SHARP	Shared Reconnaissance Pod
SHF	Super High Frequency
SID	Secondary Imagery Dissemination
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network
SMPTE	Society of Motion Picture and Television Engineers
SMTP	Simple Mail Transport Protocol
SONET	Synchronous Optical Network
SP	Standardized Profiles
SPIA	Standards Profile for Imagery Archives
SQL	Structured Query Language
SSR	Solid State Recorder
STANAG	Standardization Agreement (NATO)
Stored Data	That data stored in the RMM that is required to be transferred to the ground system.
SUT	System Under Test
SYERS	Senior Year Electro-optical Reconnaissance System
T&E	Test and Evaluation
TACO-2	Tactical Communications (protocol) version 2
TACRECCE	Tactical Reconnaissance
TADIL	Tactical Data Information Link
TAMPS	Tactical Aircraft Mission Planning System
TARS	Theater Airborne Reconnaissance System
TBD	To Be Determined
TBR	To Be Resolved
TCDL	Tactical Common Data Link
TCP	Transmission Control Protocol,. One of the TCP/IP protocol suites designed to ensure reliable data transfer.
TCPED	adds Collection to TPED
TEG	Tactical Exploitation Group
TEMP	Test and Evaluation Master Plan
TENCAP	Tactical Exploitation of National Capabilities
TERABYTE	1,000 Gigabytes (10 raised to the 12th power)
TES	Tactical Exploitation System
TFRD	Tape Format Requirements Document
TGS	TENCAP Ground Station
TIA	Telecommunications Industry Association
TIDP	Technical Interface Design Plan
TIFF	Tagged Image File Format
TIS	Tactical Input Segment

TMAN	Trusted Manager
TPED	Tasking, Processing, Exploitation, and Dissemination
TRM	Technical Reference Model
TSID	Track Set Identification number
TSS	Tri-band SATCOM System
UAV	Uninhabited Aerial Vehicle
UBER	Uncorrected Bit Error Rate
UCS	Universal Multiple – Octet Coded Character Set
UIP	USIGS Interoperability Profile
ULP	Upper Level (Layer) Protocol
UNC	Universal Naming Convention is the standard to name network resources, in a form of \\servername\sharename.
USA	United States Army
USAF	United States Air Force
USAFE	United States Air Forces Europe
USIGS	United States Imagery and Geospatial Information Service
USIS	United States Imagery Systems
USMC	United States Marine Corps
USMTF	United States Message Text Format
USN	United States Navy
US NSA	US National Security Agency
USO	Universal Secure Overwrite
UTA	USIGS Technical Architecture
Validation	Validation testing is the process of ensuring: 1) proper requirements coverage by the proposed standards or specifications and 2) correct standards or specifications are available as the basis for developing products. In the context of validation, correct standards would be those demonstrated to be self-consistent, complete and feasible. Validation testing consists of two general phases: static analysis which satisfies item 1) above and dynamic analysis which satisfies item 2) above.
Vendor	The manufacturer/developer/retailer responsible for producing or marketing a System, subsystem, or product.
VHF	Very High Frequency
VHS	Video Helical Scan (1/2 inch recording format)
VMF	Variable Message Format
VPF	Vector Product Format
VQ	Vector Quantization
VTC	Video Teleconferencing
WAN	Wide Area Network - A data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANsWB Wide-Band
WGS	World Geodetic System
WIPT	Working Integrated Product Team
WORM	Write Once Read Many
WS	Work Station
WWW	World Wide Web. Multimedia hypertext-based system that uses HTML (Hypertext Markup Language) to provide access to services and information.
XML	Extensible Markup Language
0xXX	Hexadecimal representation where “XX” is the hexadecimal code; to distinguish hexadecimal field entries from decimal or BCS.