DCNS Alternative Media Description

RECORD OF CHANGES

Revision	Date	Action
0.1	4/1/2016	Version 0.1 Initial Draft
0.2	9/30/2016	Various editorial edits and addition of verification matrix/Appendix A.
1.0	10/2/2016	Initial baseline approved by DataComm Program Office

TABLE OF CONTENTS

Contents

LIST OF TABLES

LIST OF FIGURES

1   SCOPE

This is the DCNS Alternative Media Description Document. The purpose of this document is to define the qualification requirements for any media proposed to be used for domestic en route air traffic control operations.

1.1   Background

The Federal Aviation Administration (FAA) is planning on implementing Controller/Pilot Data Link Communications (CPDLC) service in domestic en route airspace in 2019. For the provision of CPDLC service, the FAA has contracted with Harris Corporation to provide a VDL mode 2 network subject to a set of functional and performance requirements. Several airspace operators have expressed an interest in using media other than the FAA contracted VDL mode 2 media. In order to qualify non VDL Mode 2 media as acceptable for use in CPDLC service delivery, a set of performance requirements must be developed.

1.2   Purpose

This document provides a requirements basis for the air/ground communications message delivery function to support qualification of a particular Alternative Media Network /media combination against a set of requirements representing DCNS Alternative Media. This document provides a service description for the data communications infrastructure needed to support a set of services described in the RTCA SC-214 System Performance Requirements (SPR), and the system level requirements needed to support the qualification process.

1.3   Scope

This document recognizes the avionics element as integral to system operation. However, avionics are discussed only as they affect the ground system design. The scope of this document is focused on the ground system. The aircraft systems are based on other standards documents that are available elsewhere.

This document covers FANS network environments over any subnetwork service.

1.4   Document Organization

- Section 1 states the purpose and scope of this specification, its relationship to other program source requirements documents, and the driving influences that must be considered in satisfying those requirements. It also defines terminology that provides the basis for consistent references in developing system level requirements.

- Section 2 defines the applicable reference documents cited in this specification.

- Section 3 specifies the Network Service (NS) requirements.

- Appendix A defines the verification process for the NS.

- Appendix B discusses considerations for Mode 0: including a key performance parameter assessment; monitoring/reporting considerations; and assumptions.

- Appendix C defines additional abbreviations and acronyms

1.5   Definitions

Communications Service Provider: An existing provider of VDL Mode 2 air/ground communications to aircraft cockpits.

Jeopardy Condition: This exists when a function is still available, but redundancy needed to meet reliability, maintainability and availability requirements is not.

Maintenance User: A person responsible for the proper operation of infrastructure of the FAA system.

Monitoring Service: The provision of status information on Network Service elements to assist in determination of air traffic control operational impacts due to Network Service infrastructure issues.

Network Service: The provision of air/ground data communications messaging in support of air traffic control communications.

Operational User: A person who is responsible for managing and/or controlling aircraft in the airspace.

Scheduled Maintenance: A planned and FAA-approved interruption or degradation of service. It includes all FAA-approved Preventative Maintenance, Corrective Maintenance, Emergency Maintenance, and upgrade interruptions of service. It excludes any length of time that exceeds the duration of an approved interruption or degradation.

2   APPLICABLE DOCUMENTS

The following documents form a part of this Service Description (SD) to the extent specified herein. Secondary references, or those documents referenced by documents contained in this section, also form a part of this SD to the extent specified by applicable sections of the documents referenced directly in this section.

2.1   ANSP Documents

- *DCIS DTFAWA-12-D-00058 Attachment J-13: DCIS DCNS Compliance Matrix V1.4*
- *DCP-DCNSD-VER 2.3 Attachment J-1: Data Communications Program (DCP) Data Communications Network Service Description (DCNSD) Requirements applicable to Segment 1, and 2*

2.2   ICAO Standards

N/A

2.3   Industry Standards

N/A

2.4   Other Documents

- *FANS 1/A over non-VDL Mode 2 Media Report: Recommendations for Performance-Based CPDLC in U.S. National Airspace System (NAS), May 18 2016*

3   GENERAL REQUIREMENTS

When used in this document, the word "**must**" refers to an explicit requirement of a system component or the complete system.

3.1   System Description

Current data communications capabilities utilize the ACARS network for Aeronautical Operational Control (AOC)/Flight Operation Control (FOC) and some limited Air Traffic Service (ATS) communications.

Figure 3-1 illustrates the high-level functional architecture of the system. Covered in this SD are the ground portion of the Air-Ground Message Delivery (AGMD) and parts of the Ground Message Delivery elements that interconnect the ground elements of the AGMD. The Communication Service Provider (CSP) interfaces with the ground and the aircraft system by relaying data messages between flight crew and controllers to accommodate various data applications that are transmitted on this network. Depending on the configuration, this same network may also be used to support communications between the flight crew and their airline operations center.
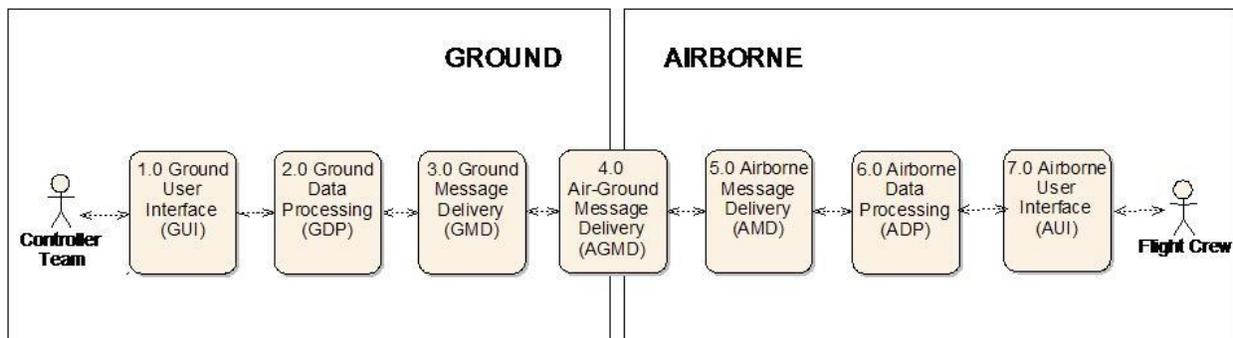
Figure 3-1. High Level Functional Architecture Diagram

3.2   System Functional Requirements

The Data Communications System for the Alternative Media Network functional requirements are described in the following subsections.

3.2.1   Messaging

3.2.1.1   General

 a.   The Alternative Media Network must support the exchange of data messages between ground and aircraft systems.

3.2.1.2   Service Delivery Point

 a.   The Alternative Media Network Service must provide redundant service delivery points, so that failure of one interface or associated telecommunication link(s) will not cause an

outage beyond the requirements of Section 4.4.3 for the most stringent RMA
performance level ordered.

3.2.2   Upgradeability

a. When upgrading service performance for a volume of airspace, the service must not be
   interrupted to the point where an outage would be declared for the lower performance
   level, unless the ANSP expressly agrees to a longer outage beforehand.

3.2.3   Incident Investigation

It is recognized that the Alternative Media Network will likely monitor additional information as
needed to manage their network. The FAA would like this information to be available to
investigators in case of communications-related incident.

a. The Alternative Media Network must maintain recorded data for 45 days.

3.2.4   Network Service and Monitoring Service Security

3.2.4.1 Access Control

    a. System account managers must manage accounts by creating, enabling, activating, modifying, and deactivating account privileges, identifiers, and authenticators in accordance with system procedures. Note: The deactivation of accounts (and not removal) is to support the concept of not reusing user account identifiers[1].

    b. System Account Managers must review system level user accounts (Operating System and Application) annually and privileged user accounts semi-annually, and must initiate required actions (e.g., deactivate, change access rights/privileges) based upon the review. System account procedures must include process and responsibilities for reviewing system accounts.[1.]

    c. Systems must automatically disable or remove temporary and emergency user accounts within 24 hours after the need for the account is no longer valid. [1.]

    d. Systems must automatically disable inactive user accounts (Operating System and Application) after 90 days of inactivity. [1.]

    e. System Owners must employ the concept of least privilege (assign and enforce the most restrictive set of rights/privileges, including system information input restrictions) when establishing system user accounts.

    f. System assets must enforce a limit of 5 consecutive invalid attempts within a 15 minute period. .[1.]

    g. System assets must be configured to either automatically: (1) Lock the account for 15 minutes, or (2) Lock the account until released by an administrator, when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection. [1.]

    h. Systems must prevent further access to the system by initiating a session lock (e.g., password protected screen saver), which conceals information, for local access sessions after 15 minutes of inactivity. [1.]

    i. Systems must retain the session lock until the user re-authenticates. [1.]

3.2.4.2 Awareness and Training

    a. System Owners must develop and implement system specific training for each security function. Training must be provided for each applicable security function (i) before authorizing access to the system or performing assigned security functions; (ii) when required by system changes; and (iii) annually thereafter. [1]

3.2.4.3 Audit and Accountability

---

[1] This Security Control was recently added as a result of the publication of NIST Rev 4 and is outside the current DCNSD requirements for VDLM2

a. Systems must generate audit logs for the following minimum events that occur for local, non-local, and remote sessions on all devices capable of generating event logs:
(1) Resource degradation alerts (e.g., 100% utilization, disk space full, volume full), (2) Login and logout, successful and unsuccessful, (3) Account creation/modification and permissions or configuration changes, (4) Administrator level activities, (5) Startup/Shutdown of System/Services/processes, (6) Access to privileged functions (e.g., setting auditable event and intrusion detection devices) including maintenance, (7) Results from malicious code protection (as capable), (8) Access control list denials (as capable), and (9) IDS signature based attacks (as capable).NAS OPIP network connected assets must send generated audit logs to the NAS Cyber Management System (NCMS) enterprise service. System Owners of assets that are not connected to any shared LAN/WAN environment may be given relief from this requirement, but must document rationale for deviating from these requirements in the SSP in order to obtain AO risk acceptance.

b. System assets must generate audit records that contain the type of event, date, time, system source or subsystem asset where the event occurred, user/subject identification, outcome of the event (success/failure), and session ID if applicable System Owners of NAS assets that are not connected to any shared LAN/WAN environment may be given relief from this requirement, but must document rationale for deviating from these requirements in the SSP in order to obtain AO risk acceptance.

c. System audit records must not contain sensitive information, such as passwords, actual system data, or privacy information. [1]

d. All system assets capable of generating audit logs, must allocate sufficient storage capacity to store 14 days of security-relevant audit records in online storage. Systems must configure the system auditing capacity to reduce the likelihood of audit record storage capacity being exceeded (e.g., provide 25% capacity above estimated need).

e. System Owners must review audit logs/records at least weekly or whenever there is an indication of inappropriate or unusual activity, unusual or suspicious activity/behavior; security incidents; policy violations; fraudulent activity; and operational problems.

f. System Owners of NAS OPIP network connected assets must send generated audit logs to the NCMS enterprise service to support audit reduction and report generation capabilities. System Owners of assets that are not connected to any shared LAN/WAN environment may be given relief from this requirement, but must document rationale for deviating from these requirements. [1]

g. System auditing procedures must include the process and responsibilities of audit reduction and report generation. System Owners of assets that do not generate audit logs must document rationale for deviating from this requirements. [1]

h. Systems that generate audit records and systems that provide enterprise audit services must not alter the original content or time ordering of audit records. [1]

i. Systems must provide accurate time stamps (including date, time, and UTC offset) in audit records

j. NAS OPIP network connected assets must send generated audit logs to the NCMS enterprise service for retention. The NCMS must retain audit records for a minimum of one year and for a minimum of three years, if associated with known security incidents. System Owners of assets that are not connected to the NAS OPIP network must retain any security audit records that are generated by the system for a minimum of one year and a minimum of three years, if associated with known security incidents.

3.2.4.4 Configuration Management

a. System Owners must develop, document, and maintain under configuration control, a current baseline configuration of the system, that includes all unique system configurations.[1]
b. System Owners must review, update, and submit the system baseline configuration (e.g., system boundary drawings, inventory table) to address any configuration changes made to the system. This includes new site installations of existing configurations. [1]
c. Systems Owners must generate a record of each approved configuration-controlled change to systems under their purview. [1]
d   System Owners must implement and maintain mandatory configuration settings for system components employed within the system in accordance with applicable industry (CIS, NIST, etc.) or vendor security checklists/benchmarks. [1]
e. System Owner Security Managers must review the system baseline configuration documentation annually and ensure that all configuration managed items are included. [1]

3.2.4.5 Contingency Planning

a. The System Owner must develop, document and test procedures for system recovery. [1]

3.2.4.6 Identification and Authentication

a. For NON-ICS system assets, user accounts must implement unique identifiers and authenticators for users (or processes acting on behalf of users) with the following exceptions:

(1) Identifiers and authenticators are not required for the specific user actions that can be performed on the system without identification or authentication, (e.g., access to public websites for viewing).

(2) Group authenticators may be used for administrator accounts, however, users must first log on to the system using their unique identifier and authenticator and then elevate privileges to the administrator level using a shared account identifier and authenticator.

b. System Owners must change default authenticator content prior to system installation. [1]

c. The System Owner must identify their default authenticator minimum and maximum lifetime restrictions and reuse conditions.

d. Systems must change/refresh authenticators in accordance with the applicable Secure Configuration Baseline Standards. [1]

e. Systems must protect authenticator content (passwords, PIN) from unauthorized disclosure and modification in storage and in transmission.   Authenticator content must use encryption for protection while in storage. Protection of authenticators in transmission may use either encryption or through isolation using a dedicated connection.

f. Systems must obscure feedback of authentication information (e.g., masking passwords, prohibit passwords from being displayed) during the authentication process to protect the information from possible unauthorized exploitation/use.

3.2.4.7   Incident Response

a. The System Owner must implement an incident handling capability for security incidents that includes: [1]

(1) Preparation,

(2) Detection and analysis

(3) Containment coordination,

(4) Eradication coordination, and

(5) Recovery coordination.

b. System Owner security personnel must report suspected or real security incidents.

3.2.4.8   Physical and Environmental Protection

a. With the exception of ground stations, System Owners/Managers of facilities containing Alternate Media Network system equipment must be audited against their ability to: [1]
(1) Develop, approve, and maintain lists of individuals with authorized access to the facility where any Alternate Media Network system resides,
(2) Issue authorization credentials for facility access,
(3) Review access lists for individuals with facility access annually
(4) Remove individuals from facility access lists when access is no longer required.

b. When system assets are in non-FAA-controlled facilities where ASH does not provide the security control, the System Owner/Facility Manager must:
(1) Enforce physical access authorizations for all physical access points by verifying individual access authorizations before granting access to the facility; and controlling ingress/egress to the facility using physical access devices and/or guards,
(2) Maintain physical access audit logs for all non-publicly accessible entry points,
(3) Provide controlled access to publicly accessible areas,
(4) Escorts visitors and monitors visitor activity in any area not open to the public,
(5) Secures keys, combinations, and other physical access devices,
(6) Inventories physical access devices used to access non-public areas annually, and
(7) Changes combinations annually when combinations are compromised or individuals are transferred or terminated. Change locks when keys are lost or stolen.

c. Facility Owners/Managers of facilities containing Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to monitor physical access to said systems to detect physical security incidents, excluding ground station locations. [1]

d. Facility Owners/Managers must be audited against their ability to monitor physical access to Alternate Media Network system equipment supporting en route CPDLC messaging and respond to physical security incidents, excluding DCNS ground station locations. [1]

e. Facility Owners/Managers of facilities containing Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to maintain visitor access records to the facility where said systems reside for at least one year, (With the exception of ground stations or areas within the facility officially designated as publicly accessible). [1]

3.2.4.9 Personal Security

a. System Account Managers for Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to deactivate individual accounts of terminated or transferred users within three business days. [1]

b. System Account Managers for Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to change the group account authenticators (i.e., shared passwords) for terminated or transferred users within three business days. [1]

c. System Account Managers for Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to disable accounts and information system access of terminated personnel within three business days. [1]

d. Facility Security Managers must be audited against their ability to ensure credentials (access cards, tokens, and badges) are terminated or revoked upon personnel terminations and transfers. [1]

3.2.4.10 System and Communications Protection

a. The Alternate Media Network system equipment supporting en route CPDLC messaging interface is considered a key boundary point.

3.2.4.11 System and Information Integrity

a. System Owners must implement security-relevant software updates within 90-days

b. System Owners must document how security-relevant software and firmware notifications and updates (i.e., web services, Operating Systems, IOSs, COTS applications (including MySQL), middleware, database, and development environments) are tracked.

c. Systems Owners must employ malicious code protection mechanisms (e.g., anti-virus software for workstations, IDS at the boundaries) for assets associated with the following:

(1) Boundaries defined by FAA Order 1370.116 (may be implemented via NESG or IAP),

(2) All Windows devices (e.g., workstations, servers, web servers, or mobile computing devices),

(3) All externally facing web servers for all operating systems (or via gateway virus protection),

(4) All mail servers (all operating systems), and

(5) All externally facing FTP servers for all operating systems (or via gateway virus protection).

SERVICE REQUIREMENTS

3.3   Network Service Functional Requirements

The Data Communications System for the Alternative Media Network functional requirements are described in the following subsections.

3.3.1   Coverage

The volumes of airspace coverage are defined within the confines below.

3.3.1.1   En Route

a. The Network Service must provide en route coverage between 16,000 feet MSL and 60,000 feet MSL across the ANSP airspace.

b. The Network Service must provide air/ground communications coverage for all published Part 121 and135 arrival and departure procedures within 5 NM around the Airport Reference Point (ARP), from airport surface areas to 2,500 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.

c. The Network Service must provide air/ground communications coverage for all published Part 121 and135 arrival and departure procedures within 20 NM around the Airport Reference Point (ARP), from 2,500 feet AGL to 10,000 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.

d. The Network Service must provide air/ground communications coverage for all published Part 121 and135 arrival and departure procedures within 40 NM around the Airport Reference Point (ARP), from 10,000 feet AGL to 12,000 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.

e. The Network Service must provide air/ground communications coverage for all published Part 121 and135 arrival and departure procedures within 60 NM around the Airport Reference Point (ARP), from 12,000 feet AGL to 16,000 feet AGL or 16,000 feet MSL, whichever is higher, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.

f. The Network Service must provide air/ground communications line-of-sight coverage to 115 NM off the coasts and land borders of the CONUS, or to the edge of the ARTCC boundaries, whichever is greater, at altitudes from 24,000 feet MSL and 60,000 feet MSL

g. The Network Service must provide air/ground communications line-of-sight coverage to 75 NM off the coasts and land borders of the CONUS, or to the edge of the ARTCC boundaries, whichever is greater, at altitudes from 16,000 feet MSL to 24,000 feet MSL.

3.3.2   Routing and Forwarding

The following subsections provide requirements for data communications networking.

3.3.2.1   Application Integrity Maintenance

a. The Network Service must deliver the application layer integrity information (e.g., checksum) without modification.

3.3.2.2   Future Air Navigation Systems (FANS) Protocol Support

a. The Alternative Media Network Service must support A/G communications using the ACARS over non-AVLC (non-AoA) protocol as defined in ICAO Doc 9776, RTCA DO-224, ARINC Specification 631, ARINC Specification 618 and ARINC Specification 620. The non-AoA protocol uses the ACARS ARINC 618/620 specifications for the network and transport layers while using any non-VDL Mode 2 system for the link and physical layers.

b. The Alternative Media Network Service must accept ARINC Specification 620 formatted messages and reformat to ARINC Specification 618 and uplink to the appropriate destination.

c. The Alternative Media Network Service must accept ARINC Specification 618 formatted downlink messages and reformat to ARINC Specification 620 and route to the appropriate ground end system.

d. The Alternative Media Network Service must support FANS-1/A+ data messaging consistent with the FANS ATS INTEROP standard, DO-258A and ARINC Specification 622.

e. The Alternative Media Network Service must report on the failure of uplink transmissions in accordance with ARINC Specification 620.

f. The Alternative Media Network Service must report on interception of downlink transmissions in accordance with ARINC Specification 620.

g. The Alternative Media Network Service must properly process the ACARS message assurance text element identifier defined in ARINC Specification 620.

3.4   Network Service Performance Requirements

The performance requirements for the Alternative Media Network are provided via a collection of Quality of Service (QoS) profiles, uniquely identified by a combination of Latency, and RMA performance levels. Each profile consists of a selection of the required latency, availability, and integrity level.

3.4.1   Latency

The following subsections provide the requirements for data latency through the Alternative Media Network.

Latency in this section is referred as the one-way transfer delay from when a message is received at the Alternative Media Network point of demarcation until its successful arrival at its destination. It includes delay such as propagation delay and retransmissions, as well as subnetwork delays resulting from   queueing/flow control, segmentation, processing, ground-network transmission, routing, etc. Delay is measured from last bit transmitted to last bit received on a data packet at the subnetwork level.

3.4.1.1   LAT1 Performance Level

The following define the Alternative Media Network allocated requirements.

a.   The Alternative Media Network uplink transfer delay must be less than or equal to 10 sec for 95% of all ATS data traffic measured in accordance with Appendix B.

b.   The Alternative Media Network downlink transfer delay must be less than or equal to 10 sec for 95% of all ATS data traffic measured in accordance with Appendix B.

c.   The Alternative Media Network uplink transfer delay must be less than or equal to 45 sec for 99% of all ATS data traffic measured in accordance with Appendix B.

d.   The Alternative Media Network Service downlink transfer delay must be less than or equal to 45 sec for 99% of all ATS data traffic measured in accordance with Appendix B.

3.4.2   Data Integrity

The Packet Error Rate at the Alternative Media Network Service Delivery Point must be less than $1x10^{-5}$. The packet error rate is the number of incorrectly received data packets divided by the number of received packets. A packet is declared incorrectly received if at least one bit is erroneous or if it is delivered to an incorrect recipient. This metric excludes packets that were lost in transmission due to connection failure or excessive latency, as those are accounted by other metrics.

3.4.3   Reliability, Maintainability and Availability

The Reliability, Maintainability and Availability performance requirements presented in this section apply to the specific Alternative Media Network subnetwork seeking qualification and should not take into account the availability of additional subnetworks in order to achieve the required performance levels.

3.4.3.1   Service Availability

A network service thread includes all equipment between the Alternative Media Network Service Delivery Point (SDP) and aircraft users, excluding any aircraft components. This would include the relevant emitting or receiving ground station antenna(s) as well as transmitting/receiving the necessary RF signal levels across the entire ordered service volume in question. Signal levels need to account for terrain impacts, as applicable to the service volume in question. For the

purposes of availability, utilization of diverse ground station sites and other means of redundancy are included to provide the required level of availability for the ordered service volume.

    a. The service availability for each alternative media network service thread must be at least 0.997 for the RMA1 performance level.

    b. The service availability for each alternative media network service thread must be at least 0.9999 for the RMA2 performance level.

c. The minimum calculated service availability must be measured over the latest 1-month period.

Availability is calculated as follows:

$$\frac{Available\_Time - Total\_Outage\_Time}{Available\_Time}$$

where:

Available_Time =Total time during the latest 12-month period that the service was under contract to the Government.

Total_Outage_Time = The total unapproved service interruption or degradation time during the *Available_Time*. It includes any unapproved degradation in which the service failed to meet all performance requirements of this specification. It includes any length of time that exceeds the duration of a FAA-approved interruption or degradation.

3.4.3.2 Scheduled Maintenance

Scheduled Maintenance: A planned and ANSP-approved interruption or degradation of service. It includes all ANSP-approved Preventative Maintenance, Corrective Maintenance, Emergent Maintenance, and upgrade interruptions of service. It excludes any length of time that exceeds the duration of an approved interruption or degradation.

The network service thread includes all equipment between the Alternative Media Network SDP and the emitting or receiving ground station antenna in question. Scheduled maintenance will take place as approved by the ANSP.

3.4.3.3 Mean Time Between Outages

Mean Time Between Outages (MTBO) is calculated over the latest 12-month period.

MTBO is calculated as follows:

$$\frac{Available\_Time \; - \; Total\_Outage\_Time}{Number\_of\_Unscheduled\_Service\_Outages}$$

where:

Available_Time =   *Total time during the latest 12-month period that the service was under contract to the Government.*

Total_Outage_Time =The total unapproved service interruption or degradation time during the Available_Time. It includes any unapproved degradation in which the service failed to meet all performance requirements of this specification. It includes any length of time that exceeds the duration of a FAA-approved interruption or degradation.

Number_of_Unscheduled_Service_Outages =   Total number of non-preventive maintenance outages of the service that occurred over the latest 12-month period. In addition, outages are to be included that are attributable to preventive maintenance that exceeded the total time allowed or that occurred in less than the minimum interval between service-interrupting preventive maintenance.

a. The Alternative Media Network Service must have a MTBO of at least 672 hours for the RMA1 performance level.

b. The Alternative Media Network Service must have a MTBO of at least 1344 hours for the RMA2 performance level.

3.4.3.4   Maximum Time to Restore Service

3.4.3.4.1 Service Restoral

An 'outage' is defined as the failure to meet requirements for a volume of airspace for any duration. Restoration time does not include customer time as defined below. Restoration time does not include the time to re-establish necessary connections, but is considered out of outage upon restoration of the capability that incurred the outage.

Customer Time is defined as time during which one or more of the following applies: a) ANSP or its representative is unable to provide site access (or chooses to delay site access), and site access is required to restore the service; b) ANSP doesn't respond to requests for additional information and such information is necessary in order to restore the service; c) or the ANSP authorizes it for other reasons.

a. The Alternative Media Network Service must restore service from an unplanned outage for the RMA2 performance level within 30 seconds except for catastrophic processor failures and force majeure events, in which case the maximum restoration time must be

within 3 minutes. See definition of "Loss of Critical Data Communications Service" under 4.2.3.5.

3.4.3.5   Single Point of Failure

a. A single failure within the Service must not cause loss of critical data communications service for services ordered as RMA2. Loss of Critical Data Communications Service: A Network Service interruption in any en route service volume which lasts more than 3 minutes.

3.4.3.6   Wide Area Impacts

a. Outages that affect more than 25% of the covered airspace ordered as RMA2 must be less than or equal to 30 seconds except for catastrophic processor failures and force majeure events in which case the restoration time must be within 3 minutes.

b. The Mean Time Between Outage for outages that affect more than 25% of the covered airspace ordered as RMA2 must be greater than or equal to 1344 hours.

c. The maximum preventive maintenance service interruption time for maintenance activities that affect more than the covered airspace ordered as RMA2 must total less than or equal to 2 hours per year.

d. Outages resulting from single-site catastrophic processor failures and single-site force majeure events must be restored within 3 minutes.

3.4.4   Capacity

The capacity of the Alternative Media Network Service is specified for each ground station in terms of Aircraft Traffic Loading. The capacity requirements presented in this section apply to alternative media subnetworks.

3.4.4.1   Aircraft Traffic Loading

The traffic loading below is for Air Traffic Service applications and does not represent any airline operational control/flight operational control communications that may also be on the Alternative Media Network.

3.4.4.1.1   En Route Domain

a. For an En Route ground station specified with En Route Loading Level 1 (ELL1), the Network Service must support an average hourly rate of 0.0010 bits per second per cubic kilometer within the ordered En Route service volume.

b. For an En Route ground station specified with ELL2, the Network Service must support an average hourly rate of 0.0030 bits per second per cubic kilometer within the ordered En Route service volume.

c. For an En Route ground station specified with ELL3, the Network Service must support an average hourly rate of 0.0050 bits per second per cubic kilometer within the ordered En Route service volume.

  d. For an En Route ground station specified with ELL4, the Network Service must support an average hourly rate of 0.0080 bits per second per cubic kilometer within the ordered En Route service volume.

  e. For an En Route ground station specified with ELL5, the Network Service must support an average hourly rate of 0.0100 bits per second per cubic kilometer within the ordered En Route service volume.

3.5 Monitoring Service Functional Requirements

3.5.1 System Event Reports

The Alternative Media Network Monitoring Service must differentiate between VDL Mode 2 networks and all other Alternate Media networks for any event reporting.

3.5.2 System Daily and Periodic Reports

  a. The Alternative Media Network Monitoring Service must differentiate between VDL Mode 2 networks and all other Alternate Media networks for any daily reports.

  b. The Alternative Media Network Monitoring Service must differentiate between VDL Mode 2 networks and all other Alternate Media networks for any periodic reports.

Appendix A   VERIFICATION

A.1.   Qualification Requirements

The evidence that will need to be provided to show that a particular Alternative Media Network satisfies the requirements contained in this document will need to be agreed upon between the ANSP and the applicant if the Alternative Media Network is to be used outside a regulatory or contractual framework. A.3 provides a verification matrix detailing example evidence by which alternate media can be qualified for initial and ongoing use of CPDLC messaging for En Route. Other reasonable, equivalent evidence could be considered, but that evidence would need to be agreed upon between the ANSP and the applicant.

A.2.   Waiver Process for Qualification

If any evidence or verification methodology shown in A.3 for initial and ongoing qualification of the network service cannot be reasonably provided, or the network service provider wishes to pursue a waiver for any requirement, they can apply with the ANSP to propose an alternative. The alternative media network service can therefore make a case for performance or function outside the bounds of the requirements provided below, but all requests will be considered on a case-by-case basis by the ANSP. The network provider for the alternative network must provide the requirement for which evidence will not be shown as in A.3, and provide a justification to do so otherwise.

Table A-1   Compliance/Verification Matrix

Table A.2.1 is a verification matrix detailing example evidence which could be provided to show compliance with the expectations presented in Section 4. Note: This matrix is specific for Mode 0 use (at the moment, the most likely alternative media candidate for use of CPDLC messaging in en route environments). Note verification is required to initially activate the requested services as well as for ongoing operational approval.

| Table A.2.1: Verification Matrix for Qualification: Initial Compliance for Mode 0 Use |

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
3.2	**System Functional Requirements** The Data Communications System for the Alternative Media Network functional requirements are described in the following subsections.	N/A	Not a requirement	N/A	Not a requirement
3.2.1	**Messaging**	N/A	Not a requirement	N/A	Not a requirement
3.2.1.1	**General**	N/A	Not a requirement	N/A	Not a requirement
3.2.1.1 (a)	The Alternative Media Network must support the exchange of data messages between ground and aircraft systems.	N/A	No extra verification needed for Mode 0. Mode 0 network has proven track record for supporting the exchange of data messages between ground and aircraft systems.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting the exchange of data messages between ground and aircraft systems
3.2.1.2	**Service Delivery Point**	N/A	Not a requirement	N/A	Not a requirement
3.2.1.2 (a)	The Alternative Media Network Service must provide redundant service delivery points, so that failure of one interface or associated telecommunication link(s) will not cause an outage beyond the requirements of Section 4.4.3 for the	Analysis	The Alternative Media Network must prove that the architecture for any network used for CPDLC traffic has redundant	N/A	Ongoing compliance will hinge on proving RMA performance – no need for proving continual compliance

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	most stringent RMA performance level ordered.		service delivery points to ensure required RMA levels		for this requirement
3.2.2	**Upgradeability**	N/A	Not a requirement	N/A	Not a requirement
3.2.2 (a)	When upgrading service performance for a volume of airspace, the service must not be interrupted to the point where an outage would be declared for the lower performance level, unless the ANSP expressly agrees to a longer outage beforehand.	Inspection	All planned maintenance activities must be scheduled and coordinated in advance with the ANSP. Provide a written requests to ANSP authorities a minimum of 10 days in advance of any planned Maintenance Events (ME) which impact the availability of CPDLC services. Emergency maintenance can be scheduled with less than 10 days' notice (with ANSP approval) to avoid a potential imminent unplanned outage. The network service must provide documentation that a maintenance plan exists to meet these requirements.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.3	**Incident Investigation** It is recognized that the Alternative Media Network will likely monitor additional information as needed to manage their network. The FAA would like this information to be available to	N/A	Not a requirement	N/A	Not a requirement

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	investigators in case of communications-related incident.				
3.2.3 (a)	The Alternative Media Network must maintain recorded data for 45 days.	Inspection	Show documentation or logs that prove recorded data is maintained for at least 45 days to help investigate incidents.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4	**Network Service and Monitoring Service Security**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.1	**Access Control**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.1 (a)	System account managers must manage accounts by creating, enabling, activating, modifying, and deactivating account privileges, identifiers, and authenticators in accordance with system procedures. Note: The deactivation of accounts (and not removal) is to support the concept of not reusing user account identifiers.	Inspection	Show documentation that proves that access control systems and processes are in place to manage user accounts. If the requirements from 4.2.4.1 can't be met exactly, the network service provider must prove that their system provides access controls that are equivalent to the intent of the requirements provided.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.1 (b)	System Account Managers must review system level user accounts (Operating System and Application) annually and privileged user accounts semi-annually, and must initiate required actions (e.g., deactivate, change access rights/privileges) based upon the review. System account procedures must include process and	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	responsibilities for reviewing system accounts.				
3.2.4.1 (c)	Systems must automatically disable or remove temporary and emergency user accounts within 24 hours after the need for the account is no longer valid.	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)
3.2.4.1 (d)	Systems must automatically disable inactive user accounts (Operating System and Application) after 90 days of inactivity.	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)
3.2.4.1 (e)	System Owners must employ the concept of least privilege (assign and enforce the most restrictive set of rights/privileges, including system information input restrictions) when establishing system user accounts.	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)
3.2.4.1 (f)	System assets must enforce a limit of 5 consecutive invalid attempts within a 15 minute period.	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)
3.2.4.1 (g)	System assets must be configured to either automatically: (1) Lock the account for 15 minutes, or (2) Lock the account until released by an administrator, when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)
3.2.4.1 (h)	Systems must prevent further access to the system by initiating a session lock (e.g., password protected screen saver), which conceals information, for local access sessions after 15 minutes of inactivity.	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)
3.2.4.1 (i)	Systems must retain the session lock until the user re-authenticates.	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)	See 4.2.4.1 (a)
3.2.4.2	**Awareness and Training**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.2 (a)	System Owners must develop and implement system specific training for each security function. Training must be provided for each applicable security function (i) before authorizing access to	Inspection	Show that training documentation exists for security functions.	N/A	As long as proof outlined in "Initial Verification Comments" is

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	the system or performing assigned security functions; (ii) when required by system changes; and (iii) annually thereafter.				followed, no additional verification is needed for ongoing compliance.
3.2.4.3	**Audit and Accountability**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.3 (a)	Systems must generate audit logs for the following minimum events that occur for local, non-local, and remote sessions on all devices capable of generating event logs: (1) Resource degradation alerts (e.g., 100% utilization, disk space full, volume full), (2) Login and logout, successful and unsuccessful, (3) Account creation/modification and permissions or configuration changes, (4) Administrator level activities, (5) Startup/Shutdown of System/Services/processes, (6) Access to privileged functions (e.g., setting auditable event and intrusion detection devices) including maintenance, (7) Results from malicious code protection (as capable), (8) Access control list denials (as capable), and (9) IDS signature based attacks (as capable).NAS OPIP network connected assets must send generated audit logs to the NAS Cyber Management System (NCMS) enterprise service. System Owners of assets that are not connected to any shared LAN/WAN environment may be given relief from this requirement, but must document rationale for deviating from these requirements in the SSP in order to obtain AO risk acceptance.	Inspection or Demonstration	Prove that the network service's audit and record keeping system generates logs for the events specified in the requirement.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (b)	System assets must generate audit records that contain the type of event, date, time, system source or subsystem asset where the event occurred, user/subject identification, outcome of the event	Inspection	Show that the network service's audit and record keeping system generates logs containing the	N/A	As long as proof outlined in "Initial Verification Comments" is

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	(success/failure), and session ID if applicable System Owners of NAS assets that are not connected to any shared LAN/WAN environment may be given relief from this requirement, but must document rationale for deviating from these requirements in the SSP in order to obtain AO risk acceptance.		information specified in the requirement.		followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (c)	System audit records must not contain sensitive information, such as passwords, actual system data, or privacy information.	Inspection	Show that the network service's audit and record keeping system generates logs that do not contain the information specified in the requirement.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (d)	All system assets capable of generating audit logs, must allocate sufficient storage capacity to store 14 days of security-relevant audit records in online storage. Systems must configure the system auditing capacity to reduce the likelihood of audit record storage capacity being exceeded (e.g., provide 25% capacity above estimated need).	Inspection or Analysis	Show or prove that enough capacity exists to store 14 days of audit records and that some kind of system exists to ensure that storage capacity isn't exceeded.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (e)	System Owners must review audit logs/records at least weekly or whenever there is an indication of inappropriate or unusual activity, unusual or suspicious activity/behavior; security incidents; policy violations; fraudulent activity; and operational problems.	Inspection	Prove that a periodic auditing review system is in place.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (f)	System Owners of NAS OPIP network connected assets must send generated audit logs to the NCMS enterprise service to support audit reduction and	Inspection, Demonstration, or N/A	Prove that audio logs are sent to the NCMS if NAS OPIP connected assets	N/A	As long as proof outlined in "Initial Verification

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	report generation capabilities. System Owners of assets that are not connected to any shared LAN/WAN environment may be given relief from this requirement, but must document rationale for deviating from these requirements.		are in place. If they are not in place, then no additional verification is needed.		Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (g)	System auditing procedures must include the process and responsibilities of audit reduction and report generation. System Owners of assets that do not generate audit logs must document rationale for deviating from this requirements.	Inspection	Show that these procedures exist or provide justification for deviation	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (h)	Systems that generate audit records and systems that provide enterprise audit services must not alter the original content or time ordering of audit records.	Analysis or Demonstration	Prove that the audit records or systems don't alter the original content or time of the records.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (i)	Systems must provide accurate time stamps (including date, time, and UTC offset) in audit records	Inspection	Show that accurate timestamps exist in audit records.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.3 (j)	NAS OPIP network connected assets must send generated audit logs to the NCMS enterprise service for retention. The NCMS must retain audit records for a minimum of one year and for a minimum of three years, if associated with known	See 4.2.4.3 (f)	See 4.2.4.3 (f)	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	security incidents. System Owners of assets that are not connected to the NAS OPIP network must retain any security audit records that are generated by the system for a minimum of one year and a minimum of three years, if associated with known security incidents.				verification is needed for ongoing compliance.
3.2.4.4	**Configuration Management**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.4 (a)	System Owners must develop, document, and maintain under configuration control, a current baseline configuration of the system, that includes all unique system configurations.	Inspection	Prove or provide documentation that shows that a configuration management system exists to control a baseline configuration for the system.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.4 (b)	System Owners must review, update, and submit the system baseline configuration (e.g., system boundary drawings, inventory table) to address any configuration changes made to the system. This includes new site installations of existing configurations.	Inspection	Show that a process exists or will exist to submit any changes to the baseline configuration to the ANSP.	Demonstration	Submit all proposed baseline configuration changes to the ANSP.
3.2.4.4 (c)	Systems Owners must generate a record of each approved configuration-controlled change to systems under their purview.	Inspection	Show that a process exists or will exist to generate records of any configuration-controlled change to systems under the network service's purview.	Demonstration	Generate and submit a record of any approved configuration-controlled change to systems under the network service's purview.
3.2.4.4 (d)	System Owners must implement and maintain mandatory configuration settings for system components employed within the system in accordance with applicable industry (CIS, NIST, etc.) or vendor security checklists/benchmarks.	Inspection	Show documentation proving that application industry or vendor security checklists/benchmarks are being follows.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
					for ongoing compliance.
3.2.4.4 (e)	System Owner Security Managers must review the system baseline configuration documentation annually and ensure that all configuration managed items are included.	Inspection	Show documentation proving that a process exists to review system baseline configuration documentation annually.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.5	**Contingency Planning**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.5 (a)	The System Owner must develop, document and test procedures for system recovery.	Inspection	Show documentation proving that tested procedures for system recovery exist.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.6	**Identification and Authentication**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.6 (a)	For NON-ICS system assets, user accounts must implement unique identifiers and authenticators for users (or processes acting on behalf of users) with the following exceptions: (1) Identifiers and authenticators are not required for the specific user actions that can be performed on the system without identification or authentication, (e.g., access to public websites for viewing). (2) Group authenticators may be used for administrator accounts, however, users must first log on to the system using their unique identifier and authenticator and then elevate privileges to the administrator level using a shared account	Inspection	Show documentation that proves that identification and authentication systems and processes are in place for user accounts. If the requirements from 4.2.4.6 can't be met exactly, the network service provider must prove that their system provides identification and authentication systems that are	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	identifier and authenticator.		equivalent to the intent of the requirements provided.		
3.2.4.6 (b)	System Owners must change default authenticator content prior to system installation.	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)
3.2.4.6 (c)	The System Owner must identify their default authenticator minimum and maximum lifetime restrictions and reuse conditions.	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)
3.2.4.6 (d)	Systems must change/refresh authenticators in accordance with the applicable Secure Configuration Baseline Standards.	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)
3.2.4.6 (e)	Systems must protect authenticator content (passwords, PIN) from unauthorized disclosure and modification in storage and in transmission. Authenticator content must use encryption for protection while in storage. Protection of authenticators in transmission may use either encryption or through isolation using a dedicated connection.	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)
3.2.4.6 (f)	Systems must obscure feedback of authentication information (e.g., masking passwords, prohibit passwords from being displayed) during the authentication process to protect the information from possible unauthorized exploitation/use.	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)	See 4.2.4.6 (a)
3.2.4.7	**Incident Response**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.7 (a)	The System Owner must implement an incident handling capability for security incidents that includes: (1) Preparation, (2) Detection and analysis (3) Containment coordination, (4) Eradication coordination, and (5) Recovery coordination.	Inspection	Show documentation that proves that an incident response process exists for the types of security incidents listed in this requirement.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.7 (b)	System Owner security personnel must report	Inspection	Show documentation that	Demonstratio	Generate and submit

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	suspected or real security incidents.		proves that a process exists for reporting any security incidents.	n	records of any security incidents that may occur on a monthly basis
3.2.4.8	**Physical and Environmental Protection**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.8 (a)	With the exception of ground stations, System Owners/Managers of facilities containing Alternate Media Network system equipment must be audited against their ability to: 1 (a) Develop, approve, and maintain lists of individuals with authorized access to the facility where any Alternate Media Network system resides, (b) Issue authorization credentials for facility access, (c) Review access lists for individuals with facility access annually (d) Remove individuals from facility access lists when access is no longer required.	Inspection or Demonstration	Show documentation that proves that the physical and environmental protection requirements laid out in this section are met. The audit in this section will be done against that documentation. The actual protections can be managed by the network service provider, but documentation should still be provided to show compliance to these requirements so that the service provider can be audited against being able to meet these requirements.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.8 (b)	When system assets are in non-FAA-controlled facilities where ASH does not provide the security control, the System Owner/Facility Manager must: (a) Enforce physical access authorizations for all physical access points by verifying individual access authorizations before granting access to the facility; and controlling ingress/egress to the facility using physical access devices and/or guards,	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	(b) Maintain physical access audit logs for all non-publicly accessible entry points, (c) Provide controlled access to publicly accessible areas, (d) Escorts visitors and monitors visitor activity in any area not open to the public, (e) Secures keys, combinations, and other physical access devices, (f) Inventories physical access devices used to access non-public areas annually, and (g) Changes combinations annually when combinations are compromised or individuals are transferred or terminated. Change locks when keys are lost or stolen.				
3.2.4.8 (c)	Facility Owners/Managers of facilities containing Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to monitor physical access to said systems to detect physical security incidents, excluding ground station locations.	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)
3.2.4.8 (d)	Facility Owners/Managers must be audited against their ability to monitor physical access to Alternate Media Network system equipment supporting en route CPDLC messaging and respond to physical security incidents, excluding ground station locations.	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)
3.2.4.8 (e)	Facility Owners/Managers of facilities containing Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to maintain visitor access records to the facility where said systems reside for at least one year, (With the exception of ground stations or areas within the facility officially designated as publicly accessible).	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)	See 4.2.4.8 (a)

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
3.2.4.9	**Personal Security**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.9 (a)	System Account Managers for Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to deactivate individual accounts of terminated or transferred users within three business days.	Inspection or Demonstration	Show documentation that proves that the personal security requirements laid out in this section are met. The audit in this section will be done against that documentation. The actual protections can be managed by the network service provider, but documentation should still be provided to show compliance to these requirements so that the service provider can be audited against being able to meet these requirements.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.9 (b)	System Account Managers for Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to change the group account authenticators (i.e., shared passwords) for terminated or transferred users within three business days.	See 4.2.4.9 (a)	See 4.2.4.9 (a)	See 4.2.4.9 (a)	See 4.2.4.9 (a)
3.2.4.9 (c)	System Account Managers for Alternate Media Network system equipment supporting en route CPDLC messaging must be audited against their ability to disable accounts and information system access of terminated personnel within three business days.	See 4.2.4.9 (a)	See 4.2.4.9 (a)	See 4.2.4.9 (a)	See 4.2.4.9 (a)
3.2.4.9 (d)	Facility Security Managers must be audited against their ability to ensure credentials (access cards,	See 4.2.4.9 (a)	See 4.2.4.9 (a)	See 4.2.4.9 (a)	See 4.2.4.9 (a)

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	tokens, and badges) are terminated or revoked upon personnel terminations and transfers.				
3.2.4.10	**System and Communications Protection**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.10 (a)	The Alternate Media Network system equipment supporting en route CPDLC messaging interface is considered a key boundary point.	N/A	Not a requirement	N/A	Not a requirement
3.2.4.11	**System and Information Integrity**	N/A	Not a requirement	N/A	Not a requirement
3.2.4.11 (a)	System Owners must implement security-relevant software updates within 90-days	Inspection	Show documentation proving that a process exists to implement security-relevant software updates within 90 days.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.11 (b)	System Owners must document how security-relevant software and firmware notifications and updates (i.e., web services, Operating Systems, IOSs, COTS applications (including MySQL), middleware, database, and development environments) are tracked.	Inspection	Show documentation proving that a process exists to track essential security-relevant software and firmware updates.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.2.4.11 (c)	Systems Owners must employ malicious code protection mechanisms (e.g., anti-virus software for workstations, IDS at the boundaries) for assets associated with the following: (1) Boundaries defined by FAA Order 1370.116 (may be implemented via NESG or IAP), (2) All Windows devices (e.g., workstations, servers, web servers, or mobile computing devices), (3) All externally facing web servers for all operating systems (or via gateway virus	Inspection	Show documentation proving that malicious code protection mechanisms exists for assets as mentioned in the requirement.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	protection), (4) All mail servers (all operating systems), and (5) All externally facing FTP servers for all operating systems (or via gateway virus protection).				
3.3	**Network Service Functional Requirements** The Data Communications System for the Alternative Media Network functional requirements are described in the following subsections.	N/A	Not a requirement	N/A	Not a requirement
3.3.1	**Coverage** The volumes of airspace coverage are defined within the confines below.	N/A	Not a requirement	N/A	Not a requirement
3.3.1.1	**En Route**	N/A	Not a requirement	N/A	Not a requirement
3.3.1.1 (a)	The Network Service must provide en route coverage between 16,000 feet MSL and 60,000 feet MSL across the ANSP airspace.	Analysis or Test	Provide coverage analysis (using coverage analyses/models or coverage selloff methods with live flights, etc.) proving en route coverage between 16,000 and 60,000 feet MSL across the ANSP airspace or provide justification for coverage based on co-located alternate media radios at Mode 2 radio locations based on any already-vetted Mode 2 coverage. *Note: In certain airspace regions, the underlying terrain*	Analysis or Test	New coverage architectures or changes to any existing architectures will require providing coverage analysis and/or coverage sell-off requalification as per initial compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			prevents the Network Providers from providing full coverage at 16,000 MSL as required without provisioning a large number of additional ground stations. The FAA may decide on a case by case basis if additional ground stations are warranted to provide added coverage in mountainous regions of the country.		
3.3.1.1 (b)	The Network Service must provide air/ground communications coverage for all published Part 121 and135 arrival and departure procedures within 5 NM around the Airport Reference Point (ARP), from airport surface areas to 2,500 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.	Analysis or Test	Provide coverage analysis (using coverage analyses/models or coverage selloff methods with live flights, etc.) proving air/ground communications coverage for all published Part 121 and135 arrival and departure procedures within 5 NM around the Airport Reference Point (ARP), from airport surface areas to 2,500 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route	Analysis or Test	New coverage architectures or changes to any existing architectures will require providing coverage analysis and/or coverage sell-off requalification as per initial compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			airspace is ordered. Or provide justification for coverage based on co-located alternate media radios at Mode 2 radio locations based on any already-vetted Mode 2 coverage. *Note: A coverage analysis can be performed around each airport to assure the specified coverage is achieved. Exceptions may occur if there is significant obstructive terrain (e.g., mountains) in the vicinity. The FAA may decide on a case by case basis if additional ground stations are warranted to provide added coverage.*		
3.3.1.1 (c)	The Network Service must provide air/ground communications coverage for all published Part 121 and 135 arrival and departure procedures within 20 NM around the Airport Reference Point (ARP), from 2,500 feet AGL to 10,000 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.	Analysis or Test	Provide coverage analysis (using coverage analyses/models or coverage selloff methods with live flights, etc.) proving air/ground communications coverage for all published Part 121 and135 arrival and departure procedures within 20 NM around the	Analysis or Test	New coverage architectures or changes to any existing architectures will require providing coverage analysis and/or coverage sell-off requalification as per initial compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			Airport Reference Point (ARP), from 2,500 feet AGL to 10,000 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered. Or provide justification for coverage based on co-located alternate media radios at Mode 2 radio locations based on any already-vetted Mode 2 coverage. *Note: A coverage analysis can be performed around each airport to assure the specified coverage is achieved. Exceptions may occur if there is significant obstructive terrain (e.g., mountains) in the vicinity. The FAA may decide on a case by case basis if additional ground stations are warranted to provide added coverage.*		
3.3.1.1 (d)	The Network Service must provide air/ground communications coverage for all published Part 121 and 135 arrival and departure procedures within 40 NM around the Airport Reference Point (ARP), from 10,000 feet AGL to 12,000 feet AGL,	Analysis or Test	Provide coverage analysis (using coverage analyses/models or coverage selloff methods with live flights, etc.)	Analysis or Test	New coverage architectures or changes to any existing architectures will require providing

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.		proving air/ground communications coverage for all published Part 121 and 135 arrival and departure procedures within 40 NM around the Airport Reference Point (ARP), from 10,000 feet AGL to 12,000 feet AGL, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered. Or provide justification for coverage based on co-located alternate media radios at Mode 2 radio locations based on any already-vetted Mode 2 coverage. *Note: A coverage analysis can be performed around each airport to assure the specified coverage is achieved. Exceptions may occur if there is significant obstructive terrain (e.g., mountains) in the vicinity. The FAA may decide on a case by case basis if additional ground stations are*		coverage analysis and/or coverage sell-off requalification as per initial compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			warranted to provide added coverage.		
3.3.1.1 (e)	The Network Service must provide air/ground communications coverage for all published Part 121 and 135 arrival and departure procedures within 60 NM around the Airport Reference Point (ARP), from 12,000 feet AGL to 16,000 feet AGL or 16,000 feet MSL, whichever is higher, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered, except when TRACON service for the associated air traffic control tower is operational.	Analysis or Test	Provide coverage analysis (using coverage analyses/models or coverage selloff methods with live flights, etc.) proving air/ground communications coverage for all published Part 121 and 135 arrival and departure procedures within 60 NM around the Airport Reference Point (ARP), from 12,000 feet AGL to 16,000 feet AGL or 16,000 feet MSL, whichever is higher, over all airports with operational Data Comm Tower Service when the overlapping en route airspace is ordered. Or provide justification for coverage based on co-located alternate media radios at Mode 2 radio locations based on any already-vetted Mode 2 coverage. *Note: A coverage analysis can be performed around each airport to assure the*	Analysis or Test	New coverage architectures or changes to any existing architectures will require providing coverage analysis and/or coverage sell-off requalification as per initial compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			specified coverage is achieved. Exceptions may occur if there is significant obstructive terrain (e.g., mountains) in the vicinity. The FAA may decide on a case by case basis if additional ground stations are warranted to provide added coverage.		
3.3.1.1 (f)	The Network Service must provide air/ground communications line-of-sight coverage to 115 NM off the coasts and land borders of the CONUS, or to the edge of the ARTCC boundaries, whichever is greater, at altitudes from 24,000 feet MSL and 60,000 feet MSL	Analysis or Test	Provide coverage analysis (using coverage analyses/models or coverage selloff methods with live flights, etc.) proving air/ground communications coverage for line-of-sight coverage to 115 NM off the coasts and land borders of the CONUS, or to the edge of the ARTCC boundaries, whichever is greater, at altitudes from 24,000 feet MSL and 60,000 feet MSL. Or provide justification for coverage based on co-located alternate media radios at Mode 2 radio locations based on any already-vetted Mode 2 coverage.	Analysis or Test	New coverage architectures or changes to any existing architectures will require providing coverage analysis and/or coverage sell-off requalification as per initial compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			Note: Over water coverage will be provided by ground stations in coastal areas. For an aircraft at 24,000 ft the nominal radio horizon is 190 NM. Occasional outages will be expected do to variations in atmospheric refractivity and multipath from the water's surface. Nominal coverage radius is defined as the maximum line-of-sight distance under nominal refractive conditions (4/3 earth model). It does not include a link budget analysis; it is included simply to provide a point of reference. Over water, refractivity can vary considerably, which can result in a change in the radio horizon which may obscure the aircraft.		
3.3.1.1 (g)	The Network Service must provide air/ground communications line-of-sight coverage to 75 NM off the coasts and land borders of the CONUS, or to the edge of the ARTCC boundaries, whichever is greater, at altitudes from 16,000 feet MSL to 24,000 feet MSL.	Analysis or Test	Provide coverage analysis (using coverage analyses/models or coverage selloff methods with live flights, etc.) proving air/ground communications	Analysis or Test	New coverage architectures or changes to any existing architectures will require providing coverage analysis and/or coverage sell-

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			coverage for line-of-sight coverage to 75 NM off the coasts and land borders of the CONUS, or to the edge of the ARTCC boundaries, whichever is greater, at altitudes from 16,000 feet MSL to 24,000 feet MSL. Or provide justification for coverage based on co-located alternate media radios at Mode 2 radio locations based on any already-vetted Mode 2 coverage. *Note: Over water coverage will be provided by ground stations in coastal areas. For an aircraft at 16,000 ft the nominal radio horizon is 155 NM. Occasional outages will be expected to variations in atmospheric refractivity and multipath from the water's surface. Nominal coverage radius is defined as the maximum line-of-sight distance under nominal refractive conditions (4/3 earth model). It does not*		off requalification as per initial compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			include a link budget analysis; it is included simply to provide a point of reference. Over water, refractivity can vary considerably, which can result in a change in the radio horizon which may obscure the aircraft.		
3.3.2	**Routing and Forwarding** The following subsections provide requirements for data communications networking.	N/A	Not a requirement	N/A	Not a requirement
3.3.2.1	**Application Integrity Maintenance**	N/A	Not a requirement	N/A	Not a requirement
3.3.2.1 (a)	The Network Service must deliver the application layer integrity information (e.g., checksum) without modification.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.
3.3.2.2	**Future Air Navigation Systems (FANS) Protocol Support**	N/A	Not a requirement	N/A	Not a requirement
3.3.2.2 (a)	The Alternative Media Network Service must support A/G communications using the ACARS over non-AVLC (non-AoA) protocol as defined in ICAO Doc 9776, RTCA DO-224, ARINC Specification 631, ARINC Specification 618 and ARINC Specification 620. The non-AoA protocol uses the ACARS ARINC 618/620 specifications for the network and transport layers while using any non-VDL Mode 2 system for the link and physical layers.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.
3.3.2.2 (b)	The Alternative Media Network Service must accept ARINC Specification 620 formatted	N/A	No extra verification needed. Mode 0 network	N/A	No extra verification needed. Mode 0

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	messages and reformat to ARINC Specification 618 and uplink to the appropriate destination.		has proven track record for supporting this requirement.		network has proven track record for supporting this requirement.
3.3.2.2 (c)	The Alternative Media Network Service must accept ARINC Specification 618 formatted downlink messages and reformat to ARINC Specification 620 and route to the appropriate ground end system.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.
3.3.2.2 (d)	The Alternative Media Network Service must support FANS-1/A+ data messaging consistent with the FANS ATS INTEROP standard, DO-258A and ARINC Specification 622.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.
3.3.2.2 (e)	The Alternative Media Network Service must report on the failure of uplink transmissions in accordance with ARINC Specification 620.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.
3.3.2.2 (f)	The Alternative Media Network Service must report on interception of downlink transmissions in accordance with ARINC Specification 620.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.
3.3.2.2 (g)	The Alternative Media Network Service must properly process the ACARS message assurance text element identifier defined in ARINC Specification 620.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.	N/A	No extra verification needed. Mode 0 network has proven track record for supporting this requirement.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
3.4	**Network Service Performance Requirements** The performance requirements for the Alternative Media Network are provided via a collection of Quality of Service (QoS) profiles, uniquely identified by a combination of Latency, and RMA performance levels. Each profile consists of a selection of the required latency, availability, and integrity level.	N/A	Not a requirement	N/A	Not a requirement
3.4.1	**Latency** The following subsections provide the requirements for data latency through the Alternative Media Network. Latency in this section is referred as the one-way transfer delay from when a message is received at the Alternative Media Network point of demarcation until its successful arrival at its destination. It includes delay such as propagation delay and retransmissions, as well as subnetwork delays resulting from queueing/flow control, segmentation, processing, ground-network transmission, routing, etc. Delay is measured from last bit transmitted to last bit received on a data packet at the subnetwork level.	N/A	Not a requirement	N/A	Not a requirement
3.4.1.1	**LAT1 Performance Level** The following define the Alternative Media Network allocated requirements.	N/A	Not a requirement	N/A	Not a requirement
3.4.1.1 (a)	The Alternative Media Network uplink transfer delay must be less than or equal to 10 sec for 95% of all ATS data traffic measured in accordance with Appendix B.	Inspection or Test	Provide 1 years' worth of uplink latency data for ATS data over any existing alternate media network or, if a new	Analysis	Provide monthly uplink latency data for ATS traffic over the alternate media network to prove

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			network or existing network with upgraded architecture is used, the network service can show a sufficient sample of test data (amount of test data and parameters of test data are agreed upon between the ANSP and the network service provider) demonstrating compliance to uplink latency requirements.		ongoing compliance for uplink latency requirements.
3.4.1.1 (b)	The Alternative Media Network downlink transfer delay must be less than or equal to 10 sec for 95% of all ATS data traffic measured in accordance with Appendix B.	Inspection or Test	Provide 1 years' worth of downlink latency data for ATS data over any existing alternate media network or, if a new network or existing network with upgraded architecture is used, the network service can show a sufficient sample of test data (amount of test data and parameters of test data are agreed upon between the ANSP and the network service provider) demonstrating compliance to downlink latency requirements.	Analysis	Provide monthly downlink latency data for ATS traffic over the alternate media network to prove ongoing compliance for downlink latency requirements.
3.4.1.1 (c)	The Alternative Media Network uplink transfer delay must be less than or equal to 45 sec for 99% of all ATS data traffic measured in accordance	Inspection or Test	Provide 1 years' worth of uplink latency data for ATS data over any	Analysis	Provide monthly uplink latency data for ATS traffic over the

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	with Appendix B.		existing alternate media network or, if a new network or existing network with upgraded architecture is used, the network service can show a sufficient sample of test data (amount of test data and parameters of test data are agreed upon between the ANSP and the network service provider) demonstrating compliance to uplink latency requirements.		alternate media network to prove ongoing compliance for uplink latency requirements.
3.4.1.1 (d)	The Alternative Media Network Service downlink transfer delay must be less than or equal to 45 sec for 99% of all ATS data traffic measured in accordance with Appendix B.	Inspection or Test	Provide 1 years' worth of downlink latency data for ATS data over any existing alternate media network or, if a new network or existing network with upgraded architecture is used, the network service can show a sufficient sample of test data (amount of test data and parameters of test data are agreed upon between the ANSP and the network service provider) demonstrating compliance to downlink latency requirements.	Analysis	Provide monthly downlink latency data for ATS traffic over the alternate media network to prove ongoing compliance for downlink latency requirements.
3.4.2	**Data Integrity**	Analysis or	Provide an analysis	N/A	As long as proof

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	The Packet Error Rate at the Alternative Media Network Service Delivery Point must be less than 1x10-5. The packet error rate is the number of incorrectly received data packets divided by the number of received packets. A packet is declared incorrectly received if at least one bit is erroneous or if it is delivered to an incorrect recipient. This metric excludes packets that were lost in transmission due to connection failure or excessive latency, as those are accounted by other metrics.	Test	showing that the current alternate media network meets data integrity requirements here, or, if a new network or existing network with upgraded architecture is used, the network service can show a sufficient sample of test data (amount of test data and parameters of test data are agreed upon between the ANSP and the network service provider) demonstrating compliance to data integrity requirements.		outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.4.3	**Reliability, Maintainability and Availability** The Reliability, Maintainability and Availability performance requirements presented in this section apply to the specific Alternative Media Network subnetwork seeking qualification and should not take into account the availability of additional subnetworks in order to achieve the required performance levels.	N/A	Not a requirement	N/A	Not a requirement
3.4.3.1	**Service Availability** A network service thread includes all equipment between the Alternative Media Network Service Delivery Point (SDP) and aircraft users, excluding any aircraft components. This would include the relevant emitting or receiving ground station antenna(s) as well as transmitting/receiving the	N/A	Not a requirement	N/A	Not a requirement

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	necessary RF signal levels across the entire ordered service volume in question. Signal levels need to account for terrain impacts, as applicable to the service volume in question. For the purposes of availability, utilization of diverse ground station sites and other means of redundancy are included to provide the required level of availability for the ordered service volume.				
3.4.3.1 (a)	The service availability for each alternative media network service thread must be at least 0.997 for the RMA1 performance level.	Inspection or Analysis	Provide 1 years' worth of RMA1 availability data for an existing alternate media network proposed for en route CPDLC use or show justification for enough shared resources and equipment between the alternate media network and the Mode 2 network (if applicable and if the Mode 2 network has already been proven to meet the availability requirement listed here) to show an analysis proving ability to meet availability requirements for the RMA1 performance level. If a new network or existing network with upgraded architecture is used, the network service can show a sufficient analysis (parameters of	Analysis	Provide monthly service availability data and analysis showing compliance for the availability for the alternate media network service for the RMA1 performance level.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			analysis are agreed upon between the ANSP and the network service provider) demonstrating compliance to RMA1 service availability. *Note: RMA2 level of service will be provided where practicable based on underlying terrain. Coverage maps will identify areas with full RMA2 level of service and areas with RMA1 level of service.*		
3.4.3.1 (b)	The service availability for each alternative media network service thread must be at least 0.9999 for the RMA2 performance level.	Inspection or Analysis	Provide 1 years' worth of RMA2 availability data for an existing alternate media network proposed for en route CPDLC use or show justification for enough shared resources and equipment between the alternate media network and the Mode 2 network (if applicable and if the Mode 2 network has already been proven to meet the availability requirement listed here) to show an analysis proving ability to meet availability requirements for the	Analysis	Provide monthly service availability data and analysis showing compliance for the availability for the alternate media network service for the RMA2 performance level.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			RMA2 performance level. If a new network or existing network with upgraded architecture is used, the network service can show a sufficient analysis (parameters of analysis are agreed upon between the ANSP and the network service provider) demonstrating compliance to RMA2 service availability. *Note: RMA2 level of service will be provided where practicable based on underlying terrain. Coverage maps will identify areas with full RMA2 level of service and areas with RMA1 level of service.*		
3.4.3.1 (c)	The minimum calculated service availability must be measured over the latest 1-month period. Availability is calculated as follows: $$\frac{Available\_Time - Total\_Outage\_Time}{Available\_Time}$$ where: Available_Time = Total time during the latest 12-month period that the service was under contract to the Government. Total_Outage_Time =The total unapproved service interruption or degradation time during the	N/A	Not a requirement. *Note: Total Outage Time (TOT) to exclude scheduled (planned), approved interruptions and degradations*	N/A	Not a requirement

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	Available_Time. It includes any unapproved degradation in which the service failed to meet all performance requirements of this specification. It includes any length of time that exceeds the duration of a FAA-approved interruption or degradation.				
3.4.3.2	**Scheduled Maintenance** A planned and ANSP-approved interruption or degradation of service. It includes all ANSP-approved Preventative Maintenance, Corrective Maintenance, Emergent Maintenance, and upgrade interruptions of service. It excludes any length of time that exceeds the duration of an approved interruption or degradation. The network service thread includes all equipment between the Alternative Media Network SDP and the emitting or receiving ground station antenna in question. Scheduled maintenance will take place as approved by the ANSP.	N/A	Not a requirement. *Note: The two categories of maintenance that result in planned interruptions and degradations are: 1) baseline configuration and/or modification, and 2) operational maintenance. Baseline modifications are planned upgrades. Operational maintenance is always corrective in nature. Corrective maintenance is the activity that will result in planned interruptions and degradations to services.*	N/A	Not a requirement
3.4.3.3	**Mean Time Between Outages** Mean Time Between Outages (MTBO) is calculated over the latest 12-month period. MTBO is calculated as follows: $$\frac{Available\_Time - Total\_Outage\_Time}{Number\_of\_Unscheduled\_Service\_Outages}$$ where:	N/A	Not a requirement. *Note: Total Outage Time (TOT) to exclude scheduled (planned), approved interruptions and degradations. Note: The two categories of maintenance that result in planned interruptions*	N/A	Not a requirement

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	Available_Time = Total time during the latest 12-month period that the service was under contract to the Government. Total_Outage_Time = The total unapproved service interruption or degradation time during the Available_Time. It includes any unapproved degradation in which the service failed to meet all performance requirements of this specification. It includes any length of time that exceeds the duration of a FAA-approved interruption or degradation. Number_of_Unscheduled_Service_Outages = Total number of non-preventive maintenance outages of the service that occurred over the latest 12-month period. In addition, outages are to be included that are attributable to preventive maintenance that exceeded the total time allowed or that occurred in less than the minimum interval between service-interrupting preventive maintenance.		*and degradations are: 1) baseline configuration and/or modification, and 2) operational maintenance. Baseline modifications are planned upgrades. Operational maintenance is always corrective in nature. Corrective maintenance is the activity that will result in planned interruptions and degradations to services.*		
3.4.3.3 (a)	The Alternative Media Network Service must have a MTBO of at least 672 hours for the RMA1 performance level.	Inspection or Analysis	Provide 1 years' worth of MTBO data for an existing alternate media network proposed for en route CPDLC use or show justification for enough shared resources and equipment between the alternate media network and the Mode 2 network (if applicable and if the Mode 2 network has already been proven to meet the	Analysis	Provide a monthly MTBO data update and analysis showing compliance for MTBO for the alternate media network service for the RMA1 performance level.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			MTBO requirement listed here) to show an analysis proving ability to meet MTBO requirements for the RMA1 performance level. If a new network or existing network with upgraded architecture is used, the network service can show a sufficient analysis (parameters of analysis are agreed upon between the ANSP and the network service provider) demonstrating compliance to RMA1 MTBO.		
3.4.3.3 (b)	The Alternative Media Network Service must have a MTBO of at least 1344 hours for the RMA2 performance level.	Inspection or Analysis	Provide 1 years' worth of MTBO data for an existing alternate media network proposed for en route CPDLC use or show justification for enough shared resources and equipment between the alternate media network and the Mode 2 network (if applicable and if the Mode 2 network has already been proven to meet the MTBO requirement listed here) to show an	Analysis	Provide a monthly MTBO data update and analysis showing compliance for MTBO for the alternate media network service for the RMA2 performance level.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			analysis proving ability to meet MTBO requirements for the RMA2 performance level. If a new network or existing network with upgraded architecture is used, the network service can show a sufficient analysis (parameters of analysis are agreed upon between the ANSP and the network service provider) demonstrating compliance to RMA2 MTBO.		
3.4.3.4	**Maximum Time to Restore Service**	N/A	Not a requirement	N/A	Not a requirement
3.4.3.4.1	**Service Restoral** An 'outage' is defined as the failure to meet requirements for a volume of airspace for any duration. Restoration time does not include customer time as defined below. Restoration time does not include the time to re-establish necessary connections, but is considered out of outage upon restoration of the capability that incurred the outage. Customer Time is defined as time during which one or more of the following applies: a) ANSP or its representative is unable to provide site access (or chooses to delay site access), and site access is required to restore the service; b) ANSP doesn't respond to requests for additional information and such information is necessary in order to restore	N/A	Not a requirement	N/A	Not a requirement

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
	the service; c) or the ANSP authorizes it for other reasons.				
3.4.3.4.1(a)	The Alternative Media Network Service must restore service from an unplanned outage for the RMA2 performance level within 30 seconds except for catastrophic processor failures and force majeure events, in which case the maximum restoration time must be within 3 minutes. See definition of "Loss of Critical Data Communications Service" under 4.2.3.5.	Inspection or Analysis	Provide 1 years' worth of service restoral data for an existing alternate media network proposed for en route CPDLC use. If a new network or existing network with upgraded architecture is used, the network service can show a sufficient analysis (parameters of analysis are agreed upon between the ANSP and the network service provider) demonstrating compliance to restoral time requirements.	Analysis	Provide annual service restoral data update and analysis showing compliance for service restoral for the alternate media network service.
3.4.3.5	**Single Point of Failure**	N/A	Not a requirement	N/A	Not a requirement
3.4.3.5 (a)	A single failure within the Service must not cause loss of critical data communications service for services ordered as RMA2. Loss of Critical Data Communications Service: A Network Service interruption in any en route service volume which lasts more than 3 minutes.	Inspection or Analysis	Provide 1 years' worth of data showing that no network service interruptions occurred for an existing alternate media network proposed for en route CPDLC use. If a new network or existing network with upgraded architecture is used, the network service can show a sufficient analysis (parameters of analysis are agreed upon	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			between the ANSP and the network service provider) demonstrating compliance to single point of failure requirements. *Note: Only in cases of a catastrophic failure of the central processor at the operational site, will restoral to a backup site require more than the specified time.*		
3.4.4	**Capacity** The capacity of the Alternative Media Network Service is specified for each ground station in terms of Aircraft Traffic Loading. The capacity requirements presented in this section apply to alternative media subnetworks.	N/A	Not a requirement	N/A	Not a requirement
3.4.4.1	**Aircraft Traffic Loading** The traffic loading below is for Air Traffic Service applications and does not represent any airline operational control/flight operational control communications that may also be on the Alternative Media Network.	N/A	Not a requirement	N/A	Not a requirement
3.4.4.1.1	**En Route Domain**	N/A	Not a requirement. *Note: En route service volume performance parameters are being finalized between the FAA, Harris, and the network service providers. So the the*	N/A	Not a requirement

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			requirements in this section are subject to change.		
3.4.4.1.1 (a)	For an En Route ground station specified with En Route Loading Level 1 (ELL1), the Network Service must support an average hourly rate of 0.0010 bits per second per cubic kilometer within the ordered En Route service volume.	Analysis or Test	Show proof that for an En Route ground station specified with En Route Loading Level 1 (ELL1), the Network Service must support an average hourly rate of 0.0010 bits per second per cubic kilometer within the ordered En Route service volume.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.4.4.1.1 (b)	For an En Route ground station specified with ELL2, the Network Service must support an average hourly rate of 0.0030 bits per second per cubic kilometer within the ordered En Route service volume.	Analysis	Show proof that for an En Route ground station specified with ELL2, the Network Service must support an average hourly rate of 0.0030 bits per second per cubic kilometer within the ordered En Route service volume.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.4.4.1.1 (c)	For an En Route ground station specified with ELL3, the Network Service must support an average hourly rate of 0.0050 bits per second per cubic kilometer within the ordered En Route service volume.	Analysis	Show proof that for an En Route ground station specified with ELL3, the Network Service must support an average hourly rate of 0.0050 bits per second per cubic kilometer within the ordered En Route service volume.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
3.4.4.1.1 (d)	For an En Route ground station specified with ELL4, the Network Service must support an average hourly rate of 0.0080 bits per second per cubic kilometer within the ordered En Route service volume.	Analysis	Show proof that for an En Route ground station specified with ELL4, the Network Service must support an average hourly rate of 0.0080 bits per second per cubic kilometer within the ordered En Route service volume.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.4.4.1.1 (e)	For an En Route ground station specified with ELL5, the Network Service must support an average hourly rate of 0.0100 bits per second per cubic kilometer within the ordered En Route service volume.	Analysis	Show proof that for an En Route ground station specified with ELL5, the Network Service must support an average hourly rate of 0.0100 bits per second per cubic kilometer within the ordered En Route service volume.	N/A	As long as proof outlined in "Initial Verification Comments" is followed, no additional verification is needed for ongoing compliance.
3.5	**Monitoring Service Functional Requirements**	N/A	Not a requirement	N/A	Not a requirement
3.5.1	**System Event Reports** The Alternative Media Network Monitoring Service must differentiate between VDL Mode 2 networks and all other Alternate Media networks for any event reporting.	N/A	Not a requirement	N/A	Not a requirement
3.5.2	**System Daily and Periodic Reports**	N/A	Not a requirement	N/A	Not a requirement
3.5.2 (a)	The Alternative Media Network Monitoring Service must differentiate between VDL Mode 2 networks and all other Alternate Media networks for any daily reports.	Analysis	Show proof that ATS traffic and any performance reports provided can and will be differentiated between the VDL Mode 2	Demonstration	Differentiate between VDL Mode 2 networks and all other Alternate Media networks for any daily reports.

Requirement Section (Ref)	Requirement	Initial Verification Methodology	Initial Verification Comments	Ongoing Verification Methodology	Ongoing Verification Comments
			network and all other Alternate Media Networks.		
3.5.2 (b)	The Alternative Media Network Monitoring Service must differentiate between VDL Mode 2 networks and all other Alternate Media networks for any periodic reports	Analysis	Same proof as 4.5.2(a)	Demonstration	Differentiate between VDL Mode 2 networks and all other Alternate Media networks for any periodic reports

Appendix B   MONITORING AND REPORTING: Considerations for Mode 0

B.1   KEY PERFORMANCE PARAMETER ASSESSMENT

In order to create a set of baseline expectations to qualify non VDL Mode 2 media as acceptable for use in CPDLC service delivery, a set of "key" performance parameters was analyzed and assessed for both initial and ongoing compliance. This analysis serves as a basis for including the functional expectations laid out in Section 4.3.

The leading candidate for Alternative Media is currently Mode 0. The following section is an assessment of Mode 0 performance parameters. If another alternative media becomes a candidate for use of CPDLC services for En Route, its associated parameters and their assessment would need to be provided.

The FAA has generated a list of performance parameters for utilization of Mode 0 in the En Route domain based on the VDLm2 requirements as originally defined in J-1 of the DCIS contract.   This section will examine each performance parameter and its suitability for Mode 0 usage.

B.1.1   Coverage

The *Alternative Media Description Document* specifies coverage requirements as described in Section 3.3.1 of this document. These requirements mirror the needed coverage set forth for VDLm2 in the DCNSD.

In order to provide consistent service for controllers and pilots alike, it is necessary that, to the extent possible, the Mode 0 and Mode 2 networks have the same coverage. This will ensure that the users will have uniform use of the Data Comm system, without regards to the underlying communications protocol of the aircraft avionics.

Creating a network which has concurrent Mode 0 and Mode 2 coverage is not expected to present a challenge to the program. In the case of both current CSPs, ground stations which contain Mode 2 radios also contain Mode 0 radios. As the frequency of the two protocols is similar, and the waveform of Mode 0 is more robust, it is expected that the coverage of Mode 0 will be sufficient to meet the program requirements.

Harris, at the FAA's request, can prove empirically that the coverage for Mode 0 meets the FAAs requirements.

B.1.2   RMA

The *Alternative Media Description Document* specifies several different RMA parameters which must be met by the DCNS system. This section will examine each of the parameters and their suitability to Mode 0 Operations.

B.1.3   Service Availability and Restoral

The availability of the Mode 0 subnetwork is a key factor to its usability. The *Alternative Media Description Document* has two different levels of service availability, RMA1 at 0.997 and RMA2 at 0.9999. In analyses for the Mode 2 subnetwork, Harris has shown that the availability of a given ground station is sufficient to provide RMA1 service, but not RMA2 service. In order to achieve RMA2 service, there must be overlapping coverage from multiple ground stations.

The architecture for Mode 2 has been designed with this in mind. Ground stations have been added to the architecture in such a way as to minimize, or eliminate, any en route areas with no redundant coverage. As mentioned in Section B.1.1, Mode 0 radios are collocated with Mode 2 radios, and as such, should meet the availability requirements to the same extent.

Mean Time Between Outage (MTBO) has two levels of requirements RMA1 at 672 hours and RMA2 at 1344 hours. The analysis which was conducted for availability can also be leveraged for MTBO. This analysis shows that by utilizing diverse telco strings and redundant ground stations, the RMA2 and RMA1 will be met.

 Mean Time to Restore (MTTR) metrics are technically achievable.

The architecture of VDLm0 minimizes the possibility of Wide Area Outages, but additional resources will not be allocated to harden the network to reduce the likelihood further.

B.1.4   Latency

The assigned latency for the Mode 0 network is the same as the Mode 2 network, which is 10 seconds to traverse from the entry to the FANS GW to the aircraft antenna, and vice versa.

There has not been a detailed analysis with the CSPs to determine if the latency value is achievable, but there are some differences which would suggest that Mode 0 will have worse latency. The most impactful difference is the burst rate of Mode 0 is 2.4 kbps vs Mode 2 at 31.5 kbps. This means that less messages can be sent over the medium without impacting latency, as well as each message will take longer to transmit.

Latency on the channel can be measured and monitored, but cannot significantly be improved upon. The main avenue for decreasing latency on the channel is the procurement of additional frequencies, and it is unlikely that additional Mode 0 frequencies will be allocated. As such, the system will not be designed for specific latency values, rather, latency will be a result of the implementation of the already existing system.

B.1.5   Data Demand

Detailed Data Demand analysis of the POA system has not been completed to best understand the expected demand, and based on that, appropriate requirements. It is unlikely that the POA system would be able to handle the same amount of traffic as the VDL system as the burst rate is approximately $1/10^{th}$.

In addition to the reduced burst rate of the channel, additional frequencies are unlikely to be allocated to Mode 0, in contrast with Mode 2.   As such, Data Demand requirements are unlikely to be designed to.

B.2   Monitoring of VDL Mode 0 using DCNS

Utilization of VDL Mode 0, or other approved alternate media for delivering en route CPDLC messages is contingent on the ability to ensure the availability of the underlying network infrastructure through active monitoring and timely event reporting. The Monitoring requirements presented in this section apply to the collective of all ATS messages being served by the Network Service provider, regardless of the subnetwork used to flow that traffic.

   a. To the extent possible, the interface for monitoring and control information with the FAA must be physically separate from the data interface for Network Service data traffic. When points of interface between monitoring and network are unavoidable, they will be identified to the FAA.

   b. Elements of the VDL Mode 0, or other approved alternate media network necessary for delivery of CPDLC messages will be adequately monitored allowing accurate assessment of that network's ability to delivery CPDLC messaging.

Monitoring of the following key performance parameters will be provided, as a minimum:

   c. Latency – measurement of latency performance for CPDLC messages transported using the CSP VDL Mode 0, or other approved alternate media network will be performed allowing evaluation against the requirements established in section 4.4.1

   d. Availability – outage and restoral times of CSP VDL Mode 0, or other approved alternate media network elements used for CPDLC messages will be performed allowing evaluation of system availability consistent with the criteria established in section 4.4.3

   e. Capacity – measurement of message throughput performance of CSP VDL Mode 0, or other approved alternate media network elements used for delivery of CPDLC messages will be performed allowing evaluation against the requirements established in section 4.4.4

The initial Concept of Operations for Monitoring of VDL Mode 0 services leverages existing interfaces and capabilities currently in use of Mode 2.

- Using existing FANS GW capabilities, CPDLC messages transported using the CSPs VDL Mode 0 networks are captured, parsed and analyzed for calculation of latency on uplink/downlink air-ground transactions.

- Using existing physical and messaging interfaces, CSPs will sent either uncorrelated (SITA) or correlated (ARINC) Mode 0 Network event information to the DCNS SOMS.

  - SOMS monitoring constructs will be extended to identify and uniquely present Mode 0 information

  - New Mode 0 RType messages will be created for publication to SWIM/NEMS.

B.3   Outage Notification Process

Notification and reporting of the CSP's VDL Mode 0, or other approved alternate media outages will be provided either at the point of occurrence for network state changes impacting operations, or reported monthly for aggregate outage evaluation and trending. Notification will be made primarily using the established Mode 2 SWIM/NEMS enterprise messaging model. The existing SWIM/NEMS message taxonomy will be extended to identify and uniquely present Mode 0 information.

a. The DCNS Monitoring Service for VDL Mode 0, or other approved alternate media must deliver an event report to NEMS via the DCNS Monitoring interface for all equipment status changes that impact Network Service function.

b. The DCNS Monitoring Service for VDL Mode 0, or other approved alternate media must deliver an event report to NEMS via the DCNS Monitoring interface for all equipment status changes that impact Network Service performance.

c. The DCNS Monitoring Service for VDL Mode 0, or other approved alternate media must deliver an event report to NEMS via the DCNS Monitoring interface when equipment fails in the operational string including those failures that may affect jeopardy conditions due to reduced redundancy.

d. The DCNS Monitoring Service for VDL Mode 0, or other approved alternate media must deliver an event report to NEMS via the DCNS Monitoring interface when equipment is returned to specified operational service.

e. Event reports must differentiate service loss, service interruptions, performance degradations, jeopardy conditions and service restoration events.

f. Event reports must include the date and time that the event was detected.

g. The DCNS Monitoring Service for VDL Mode 0, or other approved alternate media must report Security Incident reports to the DOT Cyber Security Management Center (CSMC) when security events occur as defined in AO Security Implementation Guidance\ATO-ISS-09-03 (AU), Section 7. Security incidents will be reported to the NCO.

The initial Concept of Operations for Outage Notification of VDL Mode 0 services leverages existing interfaces and capabilities currently in use of Mode 2.

- Using existing physical and messaging interfaces, DCNS SOMS will publish Mode 0 event messages to SWIM/NEMS.

    - New Mode 0 RType messages will be created for publication to SWIM/NEMS.

    - RMLS will subscribe to these new message types, providing users with differentiated reporting of Mode 0 Network performance.

- In addition to automated outage event messages, the DCNS NOC will continue to provide courtesy email and phone call notification to agreed-to distribution groups based on event type, severity and duration.

- In the event of a suspected Cyber Security event affecting the CSPs VDL Mode 0 networks, and following existing practices for Mode 2 events, the DCNS SOC will work directly with their CSP counterparts to collect pertinent event information for escalation to the NCO

B.4   Reporting

In addition to the outage reporting described in Section B.3, monthly reports of aggregate VDL Mode 0 performance will be generated and provided to the FAA.

a. Monthly Reports will include a summary of VDL Mode 0 trouble issues/outages for the month.

b. Monthly Reports will include a comparison of each operational service volume's actual VDL Mode 0 Network Service performance during the reported month against the service performance requirements of latency, availability and capacity.

c. Monthly reports must contain the VDL Mode 0 system monthly performance data for aggregated air/ground throughput. Throughput values will be correlated to latency performance and when performance compliance is in jeopardy, additional analysis will be provided.

d. Monthly reports will contain a summary description of any suspected Cyber Security event that was forwarded to the NCO and any available incident resolution.

e. The report must track all of the metrics trends for at least a six month running period.

The initial Concept of Operations for Reporting of VDL Mode 0 is to create a VDL Mode 0 appendix to the existing DCNS Monthly Operational Metrics Report (MOMR).

B.5   ASSUMPTIONS

1. Harris to provide VDL Mode 0 monitoring and reports only; no alternative media monitoring.

2. No SLAs are associated with VDL Mode 0 breaching existing performance requirements.

3. Operators, in conjunction with their elected CSPs are required to prove ability to meet requirements as per the Alternate Media Description Document.

4. CSPs will collect standard messaging fees directly from carriers using VDL Mode 0 for en route CPDLC messaging.

5. CSPs and carriers are responsible for providing SV status information in current ICD format. Harris will monitor latency. Harris will monitor VDL Mode 0 SV status as provided from CSPs.

6. Use of VDL Mode 0 for delivery of en route CPDLC messaging will be continue for five years or until activation of Segment 2 functionality, whichever comes last.

Table B-1: Abbreviations and Acronyms

Acronym	Description
4-D	4-dimensional
A/G	Air/Ground
ACARS	Aircraft Communications Addressing and Reporting System
AFN	ATS Facility Notification
Agl	Above Ground Level
AGMD	Air/Ground Message Delivery
ALL	Airport Loading Level
AMS	Acquisition Management System
ANC	Air Navigation Commission
AOA	ACARS over AVLC
AOC	Aeronautical Operational Control
APRL	ATN Profile Requirements List
ARINC	ARINC, Inc (formerly Aeronautical Radio, Inc)
ARTCC	Air Route Traffic Control Center
ATC	Air Traffic Control
ATN	Aeronautical Telecommunication Network
ATS	Air Traffic Services
ATSU	Air Traffic Services Unit
AVLC	Aviation Link Control
BEP	Back End Processor
BIS	Boundary Intermediate System
CFR	Code of Federal Regulations
CLNP	Connection-Less Network Protocol
CMU	Communications Management Unit
COCR	Communications Operating Concepts and Requirements
CONUS	Continental United States

Acronym	Description
D-ATIS	Digital Air Traffic Information Service
DCM	Data Communications Monitoring
DCNS	Data Communications Network Service
DCS	Data Communications System
DMZ	De-Militarized Zone
DTS	Dedicated Telecommunications Service
ELL	En Route Loading Level
ES	End System
FAA	Federal Aviation Administration
FANS	Future Air Navigation Service
FCS	Future Communications Study
FEP	Front End Processor
FIPS	Federal Information Processing Standards
FIS	Flight Information Service
FMS	Flight Management System
FOC	Flight Operations Control
FPR	Final Program Requirements
FTI	FAA Telecommunications Infrastructure
FTSD	FAA Telecommunications Services Description
G-BIS	Ground-Boundary Intermediate System
G/G	Ground to/from Ground
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
IDRP	Inter Domain Routing Protocol
IETF	Internet Engineering Task Force
IFCET	Interfacility Communications Engineering Team
IP	Internet Protocol
IRD	Interface Requirements Document
IS	Intermediate System
ISO	International Organization for Standardization
ITU	International Telecommunications Union
kbps	kilobits per second
kHz	Kilohertz
LACK	Logical Acknowledgement
LCD	Liquid Crystal Display
LOS	Line-of-sight
M&C	Monitoring and Control
MASPS	Minimum Aviation System Performance Standards
MCDU	Multifunction Common Display Unit

Acronym	Description
MHz	Megahertz
MTBO	Mean Time Between Outages
NAS	National Airspace System
NESG	NAS Enterprise Security Gateway
NextGen	Next-Generation Air Traffic Control for the 21st Century
NIST	National Institute of Standards and Technology
NM	Nautical miles
NTIA	National Telecommunications and Information Administration
OCC	Operations Control Center
PCB	Polychlorinated Biphenyls
PDU	Protocol Data Unit
PGW	Protocol Gateway
POA	Plain Old ACARS
QoS	Quality of Service
RF	Radio Frequency
RFC	Request for Comment
RMA	Reliability, Maintainability, and Availability
RMLS	Remote Monitoring and Logging System
RR	Receive Ready
RTCA	RTCA, Inc. (formerly Radio Technical Commission for Aeronautics)
SARPs	Standards and Recommended Practices
SD	Service Description
SDP	Service Delivery Point
SIR	Screening Information Request
SNAcF	Subnetwork Access Function
SNDCF	Subnetwork-Dependent Convergence Facility
SPR	Safety and Performance Requirements
SSD	Sub-System Description
T&E	Test & Evaluation
TDLS	Tower Data Link Service
TLL	TRACON Loading Level
TRACON	Terminal Radar Approach Control
VDL	VHF Digital Link
VDR	VHF Digital Radio
VHF	Very High Frequency
XID	Exchange Identifier (frame)

APPENDIX B - Performance Verification Methodology and Requirements

Latency compliance will be determined using the Method of Combining Samples from the MITRE whitepaper entitled "Communication Performance Requirement Verification Methodology" as described herein. Latency compliance will be determined using constant false alarm rate (0.001) and fixed level of confidence for both the 95% and 99% specifications. The measurements will use small sample sets for a "quick-look" reading of network performance. Compliance with the specification will be determined using a larger sample set comprised of 10 of the smaller sets.

The latency compliance percentage is estimated by dividing the number of messages in the sample set that meet the latency requirement by the total number of messages in the sample set. The parameters for the latency compliance tests are given in Table B-1

- The 95% latency measurement will be based on 10 sets of 600 messages each. For each small set (600), the estimated latency compliance percentage must be 92.3% or better. For the larger sample set (6,000), the estimated latency compliance percentage must be 94.1% or better.

- The 99% latency measurement will be based on 10 sets of 3000 messages each. For each small set (3,000), the estimated latency compliance percentage must be 98.4% or better. For the larger sample set (30,000), the estimated latency compliance percentage must be 98.8% or better.

Table B-2 Parameters for Latency Compliance Test

Test	Sample Size	Compliance Threshold
95%	600	$\geq$0.923
95%	6,000	$\geq$0.941
99%	3,000	$\geq$0.984
99%	30,000	$\geq$0.988