WG2\WP-215
WG3\WP-5-20

ICAO ATN PANEL (ATNP)

WORKING GROUP 2
WORKING GROUP 3

South Brisbane Australia
5-9 February 1996

Proposed ATN Systems RFP PICS

Presented By Paul Hennig/United Airlines
Prepared by IATA, France, USA

Summary

Material in this working paper has been taken directly out of the ATN Systems, Inc. Request for Proposal for an ATN Router Reference Implementation (RRI). To promote interoperability, IATA, with the support of France and the US, suggest that Internet and Upper Layer SARPs be aligned with these PICS (where applicable), that validation activities concentrate on this ATN router and upper layer baseline, and that the non-PICS information be considered for adoption as guidance material.

BACKGROUND

On July 5, 1996 eleven US airlines formed a corporation called ATN Systems, Inc. (ATNSI) which immediately signed a cooperative agreement with the US government, Department of Transportation, Federal Aviation Agency (FAA) for the joint funding and acquisition of an ATN router reference implementation (RRI) and a conformance & interoperability test suite (C/ITS). The RRI is equally applicable and usable in both airborne and land based implementations. The US airlines are Alaska, American, American Trans Air, Continental, Delta, Federal Express, Hawaiian, Northwest, United, United Parcel Service and US Air.

The cooperative agreement also calls for individual member airlines to cause avionics customizations conformant with CNS/ATN-1 SARPs using the RRI, to conduct an operational evaluation among in-service CNS/ATN-1 airplanes and FAA operational controllers/ground automation, and an FAA commitment to oceanic benefits once an acceptable number of aircraft are suitably equipped.

The ATNSI Request for Proposal (RFP) was drafted, in great part, by a Requirements Definition Team (RDT) comprised of international vendors & manufacturers of similar avionics and land based products. The ATNSI RFP was issued on 2 January 1996. The ATNSI program plan calls for RFP responses by 15 February and for ATNSI to let contracts on/about 1 April 1996. The ATNSI program plan further expects to begin individual member avionics customizations in February 1997, to receive individual member Part 25 certifications in March 1998, and Part 125 certifications in August 1998.

RATIONALE FOR SARPS ALIGNMENT

The ATNSI RFP PICS are subsets of the CNS/ATM-1 Package SARPs and Guidance Material, Part V - Internet Communications Service, Version 3.0 dated 7 August 1995, and of the Draft SARPs and Guidance Material for ATN Upper Layers for the CNS/ATM-1 Package, Sub-volume IV, Version 1.1 dated 19 October 1996. Certain options have been selected. Writers of this paper are of the opinion that the options selected are necessary for global interoperability.

The material titled, “RRI Requirements Specification” and “Requirements for Managed Objects” is further felt to embody international consensus on interoperability among ICAO states and organizations of CNS/ATM-1 users, and are offered as guidance material for both internet and upper layer SARPs.

RECOMMENDATION

Given:

a) that independently validated ATN SARPs are agreed to be required by the ICAO community by the end of the first quarter of 1997 in order to support the goal of commercially-produced systems based on these SARPs being available in the mid-1998 time frame, and,

b) that an industrially-developed ATN router/end-system specification (such as is given in the attached RRI specification and its PICS) provides an accurate indication of the scope of the ATN SARPs that can reasonably allow the agreed validation and implementation schedule goals to be met.

It is recommended:

1. that a team of experts from Working Groups 2 and 3 urgently undertake the analysis of the areas in which the attached RRI specification and its PICS may differ from the requirements expressed in the current draft ATN SARPs.
2. that these experts prepare change proposals to these draft ATN SARPs, to allow the attached RRI specification and its PICS to achieve SARPs compliance, and,
3. that validation efforts be focused on these revised ATN SARPs.

ATN Router Reference Implementation (RRI)
Requirements Specification

18 January 1996

Table of Contents

VI. RRI Requirements Specification

Requirements are based on the ICAO CNS/ATM-1 draft SARPs for Internet Communication Services (Version 3.0, 7/08/95) and Upper Layers (Version 1.1, 19/10/95).

1. Product Scope

Avionics Products	**Description**
A1	Upper layer Network Management CMIP (Agent) and ROSE protocols.
A2	Upper layer ACSE and FASTBYTE protocols.
A3	Transport Layer protocols 8073, 8602.
A4	IDRP.
A5	CLNP and ES-IS protocols.
A6	Mobile SNDCF and 8208 packet level protocol.

Ground--based Products	**Description**
G1	Upper layer Network Management CMIP (agent and manager) and ROSE protocols.
G2	Upper layer ACSE and FASTBYTE protocols certified to MIL-STD-498.
G3	Transport Layer protocols 8073, 8602.
G4	IDRP.
G5	CLNP and ES-IS protocols.
G6	Ground and mobile SNDCF and 8208 packet level protocols.

General Notes

1. ATN RRI products for avionics and ground-based SW are essentially the same except certification level. Avionics products are certified to DO-178B and ground-based products are certified to MIL-STD-498.
2. The tables on the next two pages represent the ATN RRI products according to their respective applications and installations. Notice that on ground-based systems, all protocols are maintained for each of the network layers even though not all are used. This approach reduces part number count.

The “Info only” columns on pages two and three are included to depict existing systems. These are not part of the ATN product suite.

Avionics Protocol Matrix for ATN RRI (Heavy line boxes indicate ATN RRI software package #'s)

PROTOCOL LAYER	CMU (Three Possible) Configuration 1:	CMU Configuration 2: (AIS)	CMU Configuration 3: (AIS+AES)	FMS/GNLU/GNU (as ATN End System): (AES)	Integrated FMS/CMU Architecture: (AIS+AES)	ATSU Architecture: (AIS+AES)	ATNSI Software Package
ATS Applications	(ADS) Info only		(CPDLC, ADS, CMA, FIS)[1]	(CPDLC, ADS, CMA, FIS)[2]	(CPDLC, ADS, CMA, FIS)	(CPDLC, ADS, CMA, FIS)	
LAYER 7 Application		Net Mgmt/Agent, ROSE, CMIP	Net Mgmt/Agent, ROSE, CMIP	Net Mgmt/Agent, ROSE, CMIP	Net Mgmt/Agent, ROSE, CMIP	Net Mgmt/Agent, ROSE, CMIP	**<-A1**
		ACSE	ACSE	ACSE	ACSE	ACSE	
LAYER 6 Presentation		Fast Byte	Fast Byte	Fast Byte	Fast Byte	Fast Byte	**<-A2**
LAYER 5 Session		Fast Byte	Fast Byte	Fast Byte	Fast Byte	Fast Byte	
LAYER 4 Transport	8073, 8602	8073, 8602	8073, 8602	8073, 8602	8073, 8602	8073, 8602	**<-A3**
LAYER 3 Network (Router)		10747	10747	-	10747	10747	**<-A4**
	9542, 8473	9542, 8473	9542, 8473	9542, 8473	9542, 8473	9542, 8473	**<-A5**
	MOBILE SNDCF 8208	MOBILE SNDCF 8208	MOBILE SNDCF 8208	- -	MOBILE SNDCF 8208	MOBILE SNDCF 8208	**<-A6**
LAYER 2 Data Link layers	429W 429W - version 3 HDLC[3] 8802-2,-3	429W 429W - version 3 HDLC[3] 8802-2,-3	429W 429W - version 3 HDLC[3] 8802-2,-3	429W 429W - version 3[4] HDLC[3] 8802-2,-3	429W FDDI AVLAN 8802-2 LLC	429W 429W - version 3 FDDI, HDLC 8802-2,-3	
LAYER 1 Physical layers	429 10BaseT[3] MS 1553[3]	429 10BaseT[3] MS 1553[3]	429 10BaseT[3] MS 1553[3]	429 10BaseT[3]	429, 629 FDDI	429 10BaseT[3]	

1 If CMU is ATS end system, these applications reside in CMU.
2 If FMS is ATS end system, these applications reside in FMS. The ATN Stack also resides in FMS, or alternatively, in CMU.

Ground Protocol Matrix for ATN Systems Inc. (Heavy line boxes indicate ATN RRI software package #'s)

PROTOCOL LAYER	Info Only G/G Backbone	Ground/Ground Service (GGIS)	Air/Ground (AGIS)	End System (GES)	ATNSI Software Package
ATS Applications				CPDLC, ADS, CMA, FIS, MHS, AIDC	
LAYER 7 Application		Net Mgmt/Agent, ROSE, CMIP	Net Mgmt/Agent, ROSE, CMIP	Net Mgmt/Agent, ROSE, CMIP	<-G1
		ACSE	ACSE	ACSE	
LAYER 6 Presentation		Fast Byte 8823 opt	Fast Byte 8823 opt	Fast Byte 8823 opt	<-G2
LAYER 5 Session		Fast Byte 8327 opt	Fast Byte 8327 opt	Fast Byte 8327 opt	
LAYER 4 Transport		8073, 8602	8073, 8602	8073, 8602	<-G3
LAYER 3 Network (Router)	**10747/10589**	**10747 (10589 opt)**	**10747 (10589 opt)**	**-**	**<-G4**
	9542, 8473	**9542, 8473**	**9542, 8473**	**9542, 8473**	**<-G5**
	SNDCF 8208	SNDCF **8208 opt**	**MOBILE SNDCF SNDCF 8208 opt**	SNDCF **8208 opt**	**<-G6**
LAYER 2 Data Link layers	802.2, LLC TYPE 1 CLASS 1 (ISO 8802/2)	HDLC, LAPB (ISO 7776)	ISDN LAPB, CCITT Q 921	ATM FRAME RELAY	
LAYER 1 Physical layers	802.3 (ISO 8802/3) 802.4 (ISO 8802/4) 802.5 (ISO 8802/5)	FDDI (ISO 9314) RS-232, V.35	ISDN (CCITT I430, I431)	ATM FRAME RELAY	

[3] Future Data Link and Physical layers for Avionics. 4. Williamsburg Convergence Function (WCF) provided for 8473 and 9542.

2. Deliverables

2.1 Implementation Specification

Implementation specifications shall be developed for each product that will meet the requirements specified in Section 4, Requirements Matrix, and the requirement for interoperability with other systems.

Any subsequent changes in requirements shall be reflected in updates to the specification documentation.

2.2 Interface Control Documents

Interface control documents shall be developed for each product interface to meet the requirement for interoperability with other systems.

Any subsequent changes in requirements shall be reflected in updates to the ICD documentation.

2.3 Program Review Schedule

A schedule and process for program reviews shall be proposed.

2.4 Design Review Schedule

A schedule and process for preliminary and critical design reviews shall be proposed.

2.5 Factory Acceptance Test

Acceptance testing shall be conducted in accordance with an approved acceptance test plan that is designed to determine whether the system meets functional, performance, and operational requirements as described in Section 8.

2.6 Software Documentation

Documentation shall be provided to support any product compliant with DO-178B and /or MIL-STD-498, and shall be clearly described.

2.7 Training

Training shall be provided for each deliverable.

3. Architecture

3.1 Routing Policy Requirements

3.1.1 Minimal Routing Policies

This section outlines specific router policy requirements for ATN internetwork operation. Policies associated with mobile ATN routers are defined in section 3.1.2. Policies associated with ground based ATN routers are described in section 3.1.3.

Specific technical guidance concerning mobile and ground routing policies is provided in the ATN CNS/ATM-1 Package SARPS, Part V, Internet Communications Service, Version 3.0.

3.1.2 Mobile Routing Policies

A mobile ATN router shall be configurable via policy to advertise routes available within its own Routing Domain (RD) to each ground based ATN router to which it is currently connected. A RD is a set of end systems and intermediate systems which operate the same routing protocols and procedures and which are wholly contained within a single administrative domain. This policy ensures that the mobile router tells adjacent ground routers about itself.

A mobile ATN router shall support aircraft or ground based route initiation on a subnetwork basis. For aircraft based route initiation, the mobile ATN router shall initiate the establishment of subnetwork layer connection(s) between the mobile and ground routers. Similarly, for ground based route initiation, the ground ATN router shall initiate the establishment of subnetwork layer connection(s) between the mobile and ground routers.

The mobile ATN router shall be capable of terminating network layer connections with a peer ground ATN router when the aircraft leaves coverage of a mobile subnetwork. Depending on the air/ground subnetwork, the mobile router may receive an indication from the subnetwork that the aircraft has left coverage (via a “Leave Event”). If no indication is available from the subnetwork, then the mobile router may provide a “watchdog" timer for the subnetwork connection and clear the subnetwork connection once activity has ceased for a configurable period.

3.1.3 Ground Routing Policies

An ATN ground based router shall be configurable to support connectivity with mobile or ground based ATN routers, and shall have configurable policies to provide routing services for an ATN backbone Routing Domain Confederation (RDC), Transit Routing Domain (TRD) or End Routing Domain (ERD).
A RDC is a set of Routing Domains and/or RDCs which have agreed to join together and form a Routing Domain Confederation.

The formation of a RDC is done by private arrangement between its members without any need for global coordination. A Transit Routing Domain is a domain whose policies permit its Boundary Intermediate Systems (BISs) to provide relaying for Protocol Data Units (PDUs) whose source is located in either the local routing domain or in a different routing domain. An ERD is a RD that routes PDUs only from/to its own RD. An ATN backbone is an RDC comprising a subset of Transit Routing Domains within an ATN Island that provide general connectivity. An ATN Island is an RDC comprising Civil aviation administration (CAA) operated ATN RDs within a geographical region, and may include associated ATN service providers. It may also include an RDC comprising Aeronautical Industry members which are users of communications services of a single Aeronautical Industry Service Provider, or more than one such provider providing services in combination with each other.

3.1.4 Air/Ground Routing Policies

An ATN air/ground router shall support aircraft or ground initiated route initiation on an air/ground subnetwork basis. For aircraft based route initiation, the mobile ATN router shall initiate the establishment of subnetwork layer connection(s) between the mobile and ground routers. Similarly, for ground based route initiation, the ground ATN router shall initiate the establishment of subnetwork layer connection(s) between the mobile and ground routers.

An ATN air/ground router shall accept connectivity to an aircraft in emergency conditions. For subnetworks supporting mobile route initiation, the ATN air/ground router shall not refuse a Call Indication from the mobile ATN router when the indication is received less then five minutes after a previous Call Indication was rejected, or when a call was terminated by system management.

3.1.5 Ground Routing Policies

Backbone routing polices are defined in 3.1.5.1, TRD policies are defined in 3.1.5.2, ERD policies are defined in 3.1.5.3 and requirements associated with connectivity to a service provider are described in 3.1.5.4. ATN router support to forward Connectionless Network Protocol (CLNP) PDUs based on policy is described in 3.1.5.5.

3.1.5.1 Backbone Routing Policies

An ATN backbone router shall be configurable via policy to advertise mobile routes, routes available within the router's RD, routes within the ATN island, and routes associated with mobile "homes" to the other routers on the backbone. This policy ensures that the backbone router shall tell all its neighbors within the backbone about itself, shall inform all other backbone routers about all routes to all mobiles that it has available, and shall tell the other backbone routers about all fixed RDs that it knows. The "home" is typically identified by an NSAP Address Prefix that identifies all the RD's belonging to the organisation responsible for the Mobile RD (i.e. aircraft), or all the Mobile RDs belonging to the organisation. The former is only possible if all such Fixed RDs are part of the same ATN Island RDC

An ATN backbone router shall be configurable via policy to advertise routes within its local RD, routes within the ATN island, and a default route to all aircraft to other ATN non-backbone routers in the same island. This policy ensures that the backbone router shall tell all other non-backbone routers within the island about itself, tell all ATN routers within the island about all the fixed RDs it knows about, and tell the rest of the Island that each backbone router provides a default route to all aircraft.

An ATN backbone router shall be configurable via policy to advertise local routes within its RD to each connected airborne ATN router. This policy ensures that the backbone router tells all adjacent mobiles about itself.

An ATN backbone router shall be configurable via policy to advertise routes associated with the backbone's ATN island, routes to mobiles whose "home" is contained within its island, routes to mobiles whose "home" is contained within the backbone's ATN island, and routes to mobiles without "homes" to adjacent connected ATN backbones in a different ATN island. This policy ensures that the backbone router shall tell all adjacent backbone routers in a different island about the local ATN Island, about routes to mobiles whose "home" is in that island, about all routes to mobile RDs which have "home" routes advertised, and about all of the Mobile RDs that they know about.

3.1.5.2 Transit Routing Domain Policies

An ATN ground based router in a TRD shall be configurable via policy to advertise the routes within its local RD, routes to mobiles, and routes local to its ATN island to each backbone ATN router to which it is connected. This policy ensures that the ATN TRD router shall tell the backbone about itself, about all mobiles it knows, and about all fixed RDs it knows about in the same ATN Island.

An ATN ground based router in a TRD shall be configurable via policy to advertise the routes within its local RD, routes local to its ATN island and routes to mobiles to all other adjacent non-backbone ATN routers to which it is connected. This policy ensures that the ATN TRD router shall tell all adjacent non-backbone ATN routers within the island about itself, about all fixed ATN RDs in the same ATN Island that it knows, and to ensure the backbone is informed of the location of every mobile adjacent to the Island.

An ATN ground based router in a TRD shall be configurable via policy to advertise routes within its local RD to all mobile ATN routes to which it is connected. This policy ensures that the TRD router shall tell adjacent mobile RDs about itself.

3.1.5.3 End Routing Domain (ERD) Policies

An ATN router in an ERD shall be configurable via policy to advertise routes within its local RD to all other ATN routers to which its is connected. This policy ensures that the ERD router shall tell all other routers in the ERD about itself.

3.1.5.4 Routing Policies to communicate to a Service Provider

An ATN ground based router shall be configurable via policy to support the forwarding of traffic to an ATN Service Provider. A route shall only be advertised by an ATN Service Provider to an adjacent ATN RD when it can be ensured that data sent over that route by the RD to which the route is advertised, is acceptable to every RD and RDC in the route's path, and shall be relayed by them to the route's destination.

3.1.5.5 Forwarding Policies

The ATN router shall support forwarding of ATN Operational Communications traffic based on the security parameter in the network layer PDUs and based on the configurable policies supported by the ATN router. If the network layer PDU does not contain a security parameter, then the ATN router shall attempt to forward the traffic over a "General Communications" route or a default route based on configurable policies. In general, the forwarding processes for network layer PDUs shall operate by selecting the Forwarding

Information Base (FIB) identified by the security parameter found in the PDU, and selecting from that FIB, the entry, if any, identified by the longest matching NSAP Address Prefix. The next hop information found in this FIB entry is then used to forward the PDU.

3.2 Timing Requirements

The RRI shall be required to be linked to the master clock for functions such as time stamps, timer values, performance monitoring, etc. Any hardware computer clock shall be synchronised to the master clock.

4. Requirements Matrix

Protocol Implementation Conformance Statements for the protocols used in **ATN RRI** products are contained in Attachment 9.

5. Performance Requirements

5.1 Availability Requirements

The RRI software shall be developed to support an equipment availability of 99.9%.

5.2 Integrity Requirements

An end-to-end data integrity (the probability of an undetected error in a message) of 1 in 10**7 shall be provided between Transport Service Access Points. This is achievable through use of the TP4 checksum and underlying link layer CRCs.

5.3 Delay Requirements

A CLNP NPDU shall be processed such that all functional requirements are completed in 20 ms.

5.4 Capacity Requirements

The system shall be able to deliver 15 AOC messages and 15 ATC messages to a total of 700 aircraft over a 20 minute period (expected time in a domain). This equates to 1000 messages per minute. The average size of an AOC message is 32 octets uplink, 180 octets downlink.

Airborne systems shall be able to process 10 CLNP NPDUs per second.

6. Certification Requirements

6.1 Software Development Standards

Software development standards are listed below. If any software is proposed to be developed to less than these stated requirements, the proposal shall include a safety assessment which clearly indicates targeted functionality and corresponding failure condition categorization..

6.1.1 Ground System Software

The ground system software shall be developed to MIL-STD-498.

6.1.2 Avionics System Software

The avionics system software (except CMIP and Agent) shall be developed to RTCA DO-178B requirements for Level C software. The avionics system CMIP Agent software shall be developed to RTCA DO-178B requirements for Level E software.

6.2 Use of Non-Modifiable Software

Non-modifiable software only, not user-modifiable software, shall be developed..

6.3 Software Development, Testing, Documentation, and Maintenance

6.3.1 Software Development

Software development tools shall be used and developed as per RTCA DO-178B for avionics software and per MIL-STD-498 for ground system software. Commercial Off-the-shelf (COTS) software shall not be used in avionics development to DO-178B level C. COTS may be used in ground system development.

6.3.2 Software Testing

Software testing shall provide source code verification (verification that every line of code is tested by the test plan generated via the requirements). Modular level testing shall be performed in support of certification as per DO-178B.

6.3.3 Software Documentation

All necessary documentation, configuration control, and development and validation activities shall be performed.

6.3.4 Software Life Cycle Processes

All project files shall be maintained and controlled utilizing an on-line configuration management tool. All changes to baselined or existing documentation or code shall use a formal change control tool and be formally managed.

A software life cycle process shall be provided and utilized, to include software planning, development, verification. A proposal for long-term life cycle maintenance may be proposed.

A configuration management process shall be provided and utilized to ensure that released software and documentation satisfy stated requirements. A Control Library that serves as the primary archival point for all released software and documentation shall be provided. A database of all released software and documentation shall be maintained.

Software shall consist of groupings of configuration items for each product component in order to allow unique identification during development,verification, and implementation. There shall be a configuration control identification Managed Object (MO) internal to the RRI that identifies the version of the configuration items within the RRI (software part numbers).

A software planning process shall be provided and utilized that will:

- provide process activity definitions
- define transition criteria, inter-relationships, and sequencing among processes
- define the software life cycle
- define software development standards
- inlcude a software quality assurance process
- include a software verification process as per RTCA DO-178B and MIL-STD-498
- include a configuration control process for each product set
- provide a table that provides a cross reference from the set of data items that document qualification related topics for software as outlined in RTCA DO-178B and MIL-STD-498 to the set of standard software data items and documents generated in support of the project.

A Software Designated Engineering Representative (DER) shall be provided. Whether or not an independent DER will be used shall be indicated. DER responsibilities include:

- provide advice during project development
- evaluate certification documents
- coordinate certification activities with certification authority

It is desired that the DER be licensed.

6.4 Standards Equivalencies

Products developed to DoD-STD-2167A are considered equivalent to those developed to MIL-STD 498, with the addition of a documented quality assurance plan and configuration management plan.

Correspondance between products developed to DoD-STD-2176A/MIL-STD-498 and DO-178B is shown in the following table.

DO-178B PROCESS	DoD-STD-2176A PROCESS
4.3 Software Plans	4.1 Software Development Management
4.4 Software Life Cycle Environment Planning	4.1.3 Software Development Planning
4.5 Software Development Standards	4.1.3 Software Development Planning
4.6 Review & Assurance of Software Planning Process	
5.2 Software Design Process	5.3 Preliminary Design 5.4 Detailed Design
5.3 Software Coding Process	5.5 Coding and Unit Testing
5.4 Integration Process	5.6 Component Integration and Testing
5.5 Traceability	4.2.6 Traceability of Requirements to Design
6.3.1 Review and Analysis of the High-Level Requirements	5.1.4 System Requirements Analysis - Software Product Evaluation
6.3.2 Review and Analysis of the Low-Level Requirements	5.2.4 Software Requirements Analysis - Software Product Evaluation
6.3.3 Review and Analysis of the Software Architecture	5.3.4 Preliminary Design - Software Product Evaluations 5.4.4 Detailed Design - Software Product Evaluations
6.3.4 Review and Analysis of the Source Code	5.5.4 Coding & Unit Testing - Software Product Evaluations
6.3.5 Review and Analysis of the Integration Process	5.6.4 Component Integration and Testing - Software Product Evaluations
6.3.6 Review and Analysis of the Test Cases, Procedures, and Results	5.7.4 Configuration Item Testing - Software Product Evaluations
6.4 Software Testing Process	4.3 Formal Qualification Testing
6.4.2 Requirements-Based Test Case Selection	4.3.4 Traceability of Requirements to Test Cases
6.4.4 Test Coverage Analysis	
6.4.4.1 Requirements-Based Test Coverage Analysis	4.3.4 Traceability of Requirements to Test Cases
6.4.4.2 Structure Coverage Analysis	

DO-178B PROCESS	DoD-STD-2176A PROCESS
7.2.1 Configuration Identification	4.5.1 Configuration Identification
7.2.2 Baselines and Traceability	4.5.2 Configuration Control
7.2.3 Problem Reporting, Tracking and Corrective Action	4.1.9 Corrective Action Process, 4.1.10 Problem/Change Report
7.2.4 Change Control	4.5.2 Configuration Control
7.2.5 Change Review	4.5.5 Engineering Change Proposals
7.2.6 Configuration Status Accounting	4.5.3 Configuration Status Accounting
7.2.7 Archive, Retrieval and Release	4.5.4 Storage, Handling, and Delivery of Project Media
7.2.8 Software Load Control	
7.2.9 Software Life Cycle Environment Control	4.5.2 Configuration Control
8.3 Software Conformity Review	4.4 Software Product Evaluations
9.2 Compliance Substantiation	

DO-178B PRODUCTS	DoD-STD-2167A PRODUCTS
11.1 Plan for Software Aspects of Certification	
11.2 Software Development Plan	DI-MCCR-80030A Software Development Plan (SDP)
11.3 Software Verification Plan	DI-MCCR-80014A Software Test Plan (STP)
11.4 Software Configuration Management Plan	DI-MCCR-80030A (10.2.9) SDP - Software Configuration Management
11.5 Software Quality Assurance Plan	
11.6 Software Requirements Standards	
11.7 Software Design Standards	DI-MCCR-80030A (10.2.6.2.3) SDP - Software Design Standards
11.8 Software Coding Standards	DI-MCCR-80030A (10.2.6.2.4) SDP - Software Coding Standards DoD-STD-2167A (App. B) Requirements for Software Coding Standards
11.9 Software Requirements Data	DI-MCCR-80025A Software Requirements Specification (SRS)
11.10 Design Description	DI-MCCR-80012A Software Design Document (SDD)
11.11 Source Code	DI-MCCR-80029A Software Product Specification (SPS)
11.12 Executable Object Code	This would normally accompany the SPS above
11.13 Software Verification Cases and Procedures	DI-MCCR-80015A Software Test Description (STD)
11.14 Software Verification Results	DI-MCCR-80017A Software Test Report (STR)
11.15 Software Life Cycle Environment Configuration Index	DI-MCCR-80013A Version Description Document (VDD)
11.16 Software Configuration Index	DI-MCCR-80013A Version Description Document (VDD)
11.17 Problem Reports	DI-MCCR-80030A (10.2.5.11) SDP - Problem/Change Report
11.18 Software Configuration Management Records	DI-MCCR-80030A (10.2.9) SDP - Software Configuration Management
11.19 Software Quality Assurance Records	

11.20 Software Accomplishment Summary	

If software equivalency between DO-178B and DoD-STD-2167A/MIL-STD-498 is desired, then the following items shall be addressed:

- testing compliance substantiation
- structural coverage analysis (instruction, decision, decision condition)
- code walkthrough
- requirements traceability
- coding standards, dyamic memory allocation, dead code

A common approach for development of airborne and ground segments shall be considered and is recommended. An analysis for using this approach should cover:

- identification of common products or sub-products
- feasibility of a common development cycle (requirements, general design, detailed design, coding, integration, testing, etc.)
- feasibility of a common methodology (quality assurance, configuration management, requirements traceability, etc.)
- resulting economical benefits

6.5 Software Partitioning

Safety monitoring and protection mechanisms used for partioning and use of modifiable data shall be proven through analysis and demonstration. Software developed to different “levels” shall be partitioned.

DO-178B Section 2.3.1 provides the following guidance on software partitioning. “Partitioning is a technique for providing isolation between functionally independent software components to cotain and/or isolate faults and potentially reduce the effort of the software verification process. If protection by partitioning is provided, the software level for each partitioed component may be determined using the most severe failure condition associated with that component. If the partitioning involves software, then that software shall be assigned the software level corresponding to the highest level of the partitioned software components”.

Other design considerations of software functions residing within separate software partitions shall ensure:

- no function will contaminate another function's code, I/O, or data storage
- no function will consume computing resources to the exclusion of another function
- no function will consume I/O resources to the exclusion of another function
- failures of common hardware will not impact the capability for continued safe flight and landing
- failures of hardware unique to a partition will not cause adverse effects to be generated in any other software partition.

7. Portability Requirements

7.1 Ground Developed PSE

The ground PSE (Portable Streams Environment) shall be developed via MIL-STD-498, and shall support ,as a minimum, services listed below as defined in UNIX System V, Release 4 Streams Documentation Appendix C (ISBN-13-020660-1).

adjmsg, allocb,backq,bufcall,canput,copyb, copymsg, datamsg,dupb, dupmsg, enableok, flush, flushq, freeb, freemsg, getq, insq ,linkb, msgdsize, noenable, OTHERQ, pullupmsg, putbq, putctl, putctl1, putnext, putq, qenable, qreply, qsize, RD, rmvb, rmvq, testb, unbufcall, unlinkb, WR.

7.2 Airborne Developed PSE

The airborne PSE (Portable Streams Environment) shall be developed via DO-178B (level C) shall support ,as a mimium, the follow services listed below as defined in UNIX System V, Release 4 Streams Documentation Appendix C.

copyb,copymsg, allocb, freeb, freemsg, linkb, unlinkb, msgdsize, pullupmsg ,putq, putbq,putnext, getq, canput, flushq, qreply, qenable, putctl, putctl1, bufcall, unbufcall, RD, WR, OTHERQ.

7.3 User/application Interface to PSE (both ground & airborne)

Both the airborne & ground PSE shall provide the user level facilities listed below, as defined in UNIX System V, Release 4 Streams Documentation; the services shall be developed according to DO-178B and MIL-STD-498 respectively.

open, close, putmsg, getmsg, ioctl, poll

7.4 Minimum Software Environment Services

Expected minimum services provided by the software environment which will use the PSE are listed below:

- System time with minimum granularity of 100 milliseconds.
- Operating system with time slice or mechanicism to release the processor to another task.
- Shared memory or a IPC interface between tasks.
- The software environment must provide mutual exclusion..

Note 1: If the software being used uses additional services in SYSTEM V Release 4 , then the PSE can be developed to support these services.

Note 2: Target operating systems identified so far include HP-UX, DEC, TOPIX, AIX, SOLARIS.

8. Testing and Acceptance Requirements

8.1 Router Developmental Testing

The objectives of developmental testing are to demonstrate that each module has been tested, that every path in these modules is executed, and that the software satisfies its requirements.

The ground router developmental testing shall be conducted using the guidelines contained in MIL-STD-498. The developmental testing shall consist of unit testing, unit integration testing, CSCI qualification testing, CSCI/HWCI Integration testing and systems qualification testing.

The airborne router developmental testing shall be conducted using the guidelines contained in DO-178B. The developmental testing shall consist of low level testing, software integration testing, and hardware/software integration testing.

Note: If the target computer environment is the same as the development computer environment then the hardware/software integration testing is not required to be performed.

Acceptance testing shall be accomplished and will include the following: modular level testing in support of certification, traffic generation testing, and interference testing.

8.2 Conformance Testing

Conformance testing will be accomplished using the CTS, at a functional level in compliance with all functional RRI requirements and will be used in support of certification for installed equipment.

Availability and integrity of the communications network shall be proved through software development rather than through testing.

8.3 Interoperability Testing

Interoperability testing will be and may use acceptance testing tools and the CTS as a part of the interoperability testing effort.

8.4 Performance Testing

All "product specific" performance testing will be accomplished using the CTS at a product level in compliance with all RRI performance requirements, and will be used in support of certification for installed equipment.   Any "end-to-end" performance testing will also be accomplished.

9 Network Management Requirements

Network management using CMIP shall be used to collect and report data. Because of technical constraints in avionics, it is recommended that CMIP software development be to DO-178B level E. This could be achieved by using partitioned COTS software, building Managed Objects (MO)s in the stack, and using GETs to manipulate the data which would be acceptable for certification.

All storage (e.g. tables, databases) is defined as MOs in the the Management Information Bases (MIB). The MOs are defined in Attachment 8. All CSCIs in the RRI shall be capable of using the MIB (i.e. MOs).

There is a requirement for data that exceeds a certain threshhold to be transmitted in real time between an airborne system and a ground host computer. (e.g. this data may be used to influence which air/ground subnetwork is used for transmission). It is noted that this requirement may be met through use of a traffic type in the security option of IDRP, generated by the application. The solution to this problem will be ground-driven.

A solution for a network management architecture to meet these requirements shall be proposed.

10 Security Requirements

ATN RRI requirements are based on the draft ICAO CNS/ATM-1 package. Therefore, there are no current **ATN RRI** requirements for ATN security. This position has been coordinated with the FAA and participating airlines.

11 Subnetwork and Application Interface Requirements

11.1 Ground Subnetwork Interface Requirements

Specific Ground Subnetworks:
- NADIN II
- ARINC Packet Network
- SITA Mega Transport Network
- ADTN2000

Generic Ground Subnetworks:
- FDDI
- Ethernet (10 base T, 100 base T)
- X.25 (1984, 1988)
- Token Ring
- TCP/IP
- Asynchronous Transfer Mode (ATM)
- Frame Relay

Air/Ground Data Subnetworks
- Gatelink
- VDL (Mode 2)
- AMSS (Data 3)
- Mode S
- HF

Note 1: PICS for ISO 8208 to interface with AMSS and VDL are included in Attachment 9 and should be costed as part of the baseline product, PICS for ISO 8208 to interface with the Mode S subnetwork are not included and should be costed in the proposal response as an option.

Note 2: The V.42bis compression scheme is to be used in the baseline ATN RRI product (see 7.1.1. SNDCFPICS, Attachment 9). V.42bis is supported because it is data independent, and *a mature specification exists and is widely implemented. If another compression scheme is required, this must be negotiated between SNDCFs. (It is recognized that SATCOM and Mode S subnetwork efficiency will be improved by use of the ICAO Address Compression Algorithm (ACA), which is not part of the baseline ATN RRI product. The ACA may be included as an option by a participant in the customization phase of the ATN Router Project).*

Note 3: An upgrade to the PICS for the Mobile SNDCF to accommodate the interface with VDL will be proposed in the ICAO ATN Panel in January. This specification will be updated when agreement on the upgrade is reached in the ATNP.

11.2 Ground Application Support Requirements

ICAO CNS/ATM-1 Package Applications
- CPDLC
- ADS
- FIS (ATIS)
- CM

11.3 Airborne Subnetwork Interface Requirements

- ISO 8208 interface to avionics busses (429, FDDI, 646, 1553)

- Requirement for multiple (up to 4 simultaneous) DTE/DTE router connections on a specific subnetwork (e.g. AMSS)

Specific Avionics Busses
- AEEC 429
- FDDI
- AEEC 646 ELAN (10 base T)
- MIL Spec 1553

Air/ground data subnetworks:
- Gatelink
- Mode S
- VDL (Mode 2)
- AMSS (Data 3)
- HF

11.4 Airborne Application Support Requirements

ICAO CNS/ATM-1 Package Applications

- CPDLC
- ADS
- FIS (ATIS)
- CM

Note: Where interface to air/ground subnetworks is accomplished via ISO 8208, the ISO 8208 protocol is to be a part of the ATN RRI product set.

12 Congestion Management Requirements

Congestion control mechanisms must be implemented by all systems in a network. With only a partial implementation, those end systems that do implement congestion control mechanisms will see degraded performance compared to those that do not. It is recognized that a proposed methodology will need to be standardized for global implementation. The remaining part of section 12 discusses possible approaches.

The most common congestion recovery algorithm today is called "slow start", which is part of the transport layer protocol running in end systems. Slow Start reacts to the expiration of the transport layer's retransmission timer and requires no explicit feedback from routers. Slow Start is described in "Congestion Avoidance and Control" V. Jacobson, *Proceedings of ACM SIGCOMM '88,* Stanford, CA. (August): 314-329.

OSI networks may also use a congestion *avoidance* scheme in which a router that is congested sets a congestion experienced (CE) bit in the header of the internetwork packet. The destination of the packet monitors the congestion bits in received packets and when a certain percentage of received packets on a transport connection have the bit set, the receiving transport entity reduces the credit to the sender. The credit defines how many packets the sender may transmit before receiving an acknowledgment. This congestion avoidance scheme, often called "DECbit" is described in "A Binary Feedback Scheme for Congestion Avoidance in computer Networks with a Connectionless Network Layer", K.K. Ramakrishnan and Raj Jain, *Proceedings of ACM SIGCOMM '88,* Stanford, CA. (August): 303-313.

13 Monitoring Requirements

13.1 Performance Monitoring Requirements

Benchmarked transit delay into and out of the RRI.

14 Miscellaneous Requirements

14.1 Data Loader Function

Airline requirements are for a EIA Standard connector interface on the front panel of the hardware that houses the router software. The RRI requirement is for a linkage to this hardware data loader for both data and executable code.

14.2 PING

The RRI shall have the capability to launch and/or reply to multiple PINGs.

14.3 TRACEROUTE

The RRI shall have local and remote TRACEROUTE capability.

14.4 Benchmarking

RRI software shall be benchmarked on a target platform and benchmark values shall be distributed with the software version.

ATTACHMENT 8

REQUIREMENTS FOR MANAGED OBJECTS (MOs)

The following MOs have been identified to date. Additional MOs that may be felt to be necessary may be proposed. Customers may identify further MOs.

All MOs will be capable of threshholding (time/size)

SNDCF

Join/Leave events (or equivalent) by subnetwork
Aggregate on join/leave events
Queue counts by subnetwork
Aggregate queue counts

Network/IDRP

All router connections (origin/destination DTE)
Aggregate for all router connections
IDRP traffic (inbound and outbound, bit count and packets) on every router connection
Aggregate IDRP traffic
Forwarding information (FIB)
Policy information (PIB)
Routing information (RIB)

Transport

All Transport connections origin/destination TSAP/NSAP and associated priority
Bit counts (both overhead and data) by Transport connection
Aggregate for all bit counts for all connections
Queue counts by transport connection
Aggregate queue counts

ACSE

All ACSE connections (origin/destination Application Entity Titles)
Aggregate for all ACSE connections
Bit counts (both overhead and data) by ACSE connection
Message counts (data only)
Aggregate bit count
Aggregate message count
Queue counts by ACSE connection
Aggregate queue counts

Miscellaneous

Processing time through the RRI based on first bit in last bit out (benchmark/exceptions)
Error counts (errors tbd, definition requested from vendor)
Retransmit counts
ICAO 24-bit ID, hardware part number, software part number (one MO for each and one aggregate MO for all three)