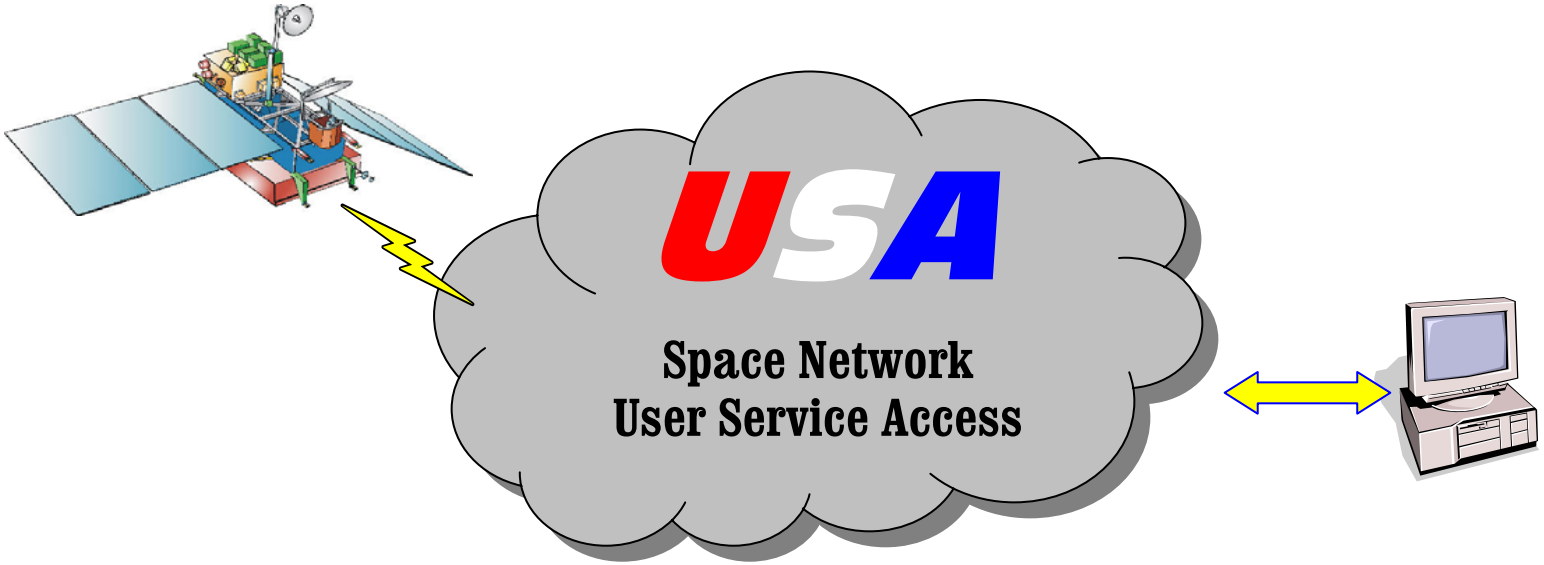
Space Network
User Service Access (USA)
System Requirements Review (SRR)



May 12, 2008 http://scp.gsfc.nasa.gov/snis/ Space Network Code 452

Agenda

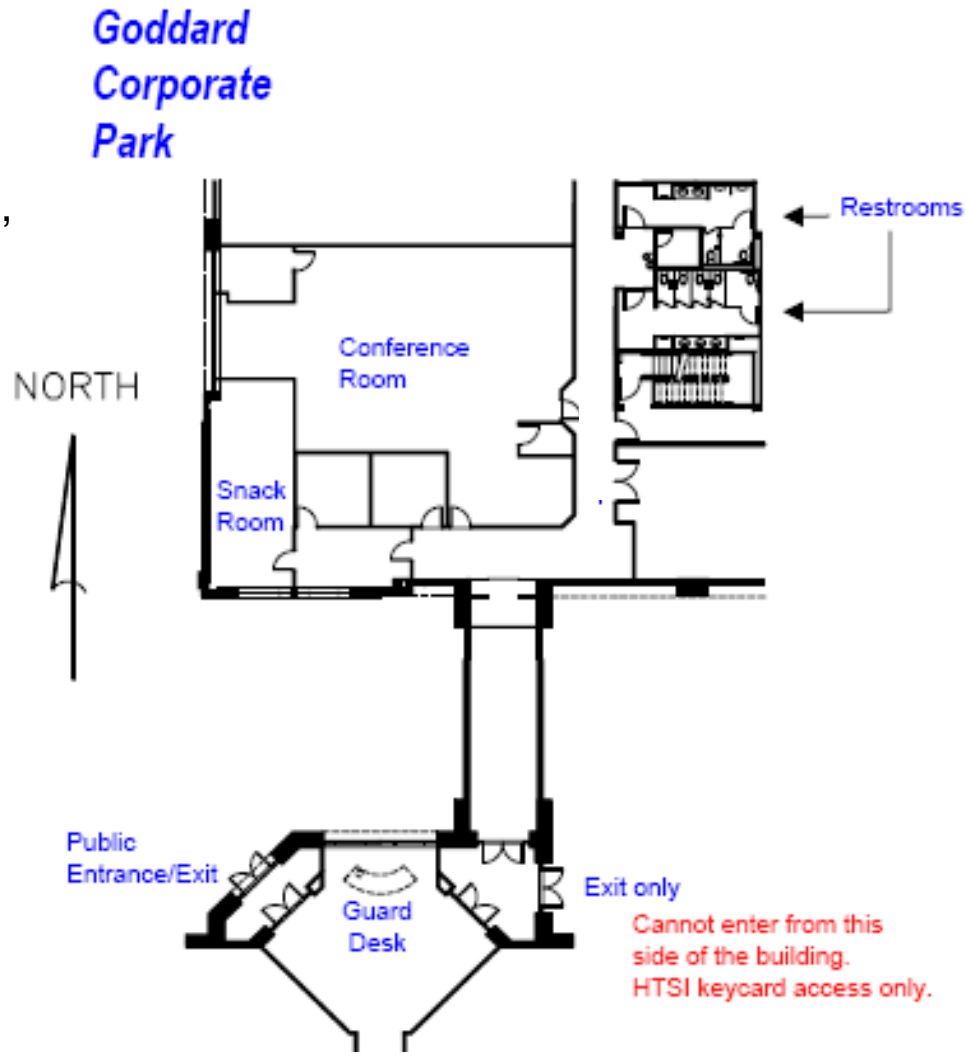
- Section 1. Introduction 9:00 am
- Section 2. Documentation
- Section 3. System Description
- Section 4. USA System Requirements
  - SRD Section 4. System Requirements
  - SRD Section 5. RMA Requirements
  - SRD Section 6. Security Requirements
  - SRD Section 7. Equipment Design, Construction, and Installation Requirements
  - SRD Section 8. Maintenance Requirements
- Section 5. Concept of Operations
- Section 6. Requirements Under Study
- Section 7. Requirements Management
- Section 8. Product Implementation
  - Schedule
  - Risk and Risk Mitigation
- Section 9. Closing Remarks 12:00 pm

Section 1
Introduction

Purpose and Scope
Review Board
Product Organization

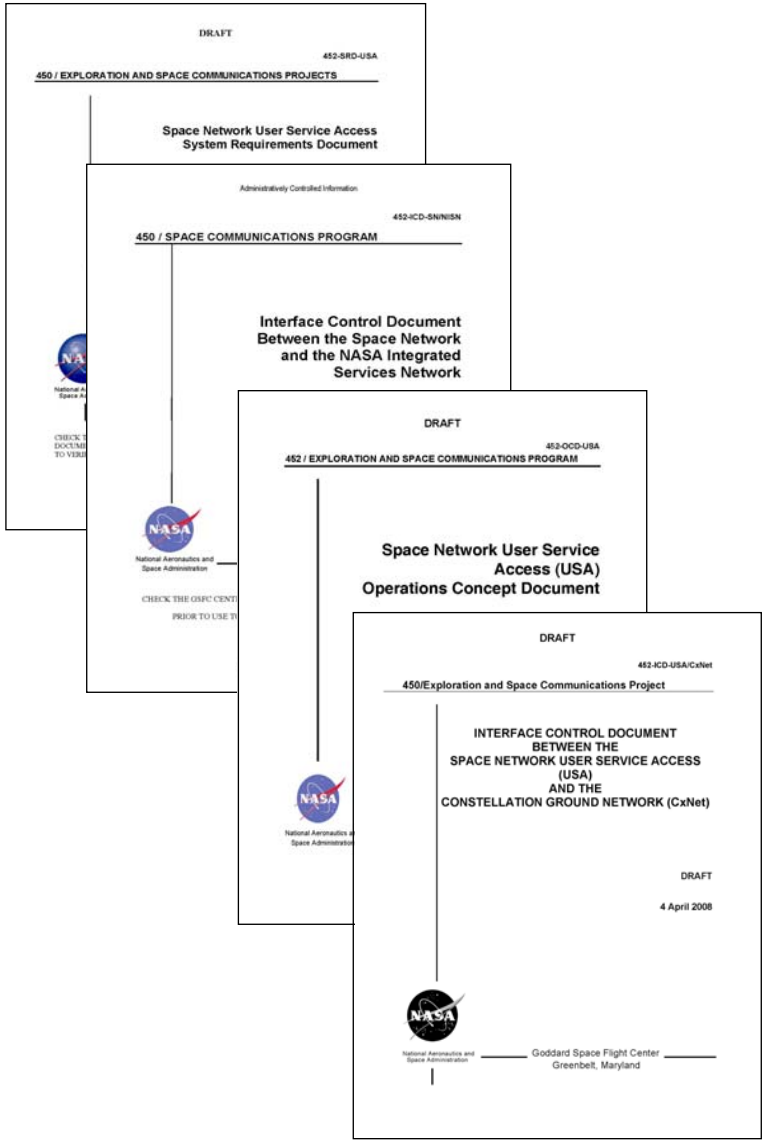
Goddard Corporate Park Details

- Location
  - Honeywell Goddard Corporate Park 7515 Mission Drive Lanham, Md.
- Entrance & Exiting the Building Attendee Sign-In List
- Restrooms
- Cell Phones
- No classified material



Welcome - Purpose of Review

- **The purpose of this review is to get feedback from SRR participants and the SRR Board to ensure the USA system requirements set is appropriate, complete and well defined**
- **This review is structured to provide a requirements-based overview of the USA system**
  - A comprehensive description of USA system capabilities is documented in:
    - 452-SRD-USA, System Requirements Document for the User Service Access System
    - DCN to 452-ICD-SN/NISN, Interface Control Document between the SN and NISN
    - 452-OCD-USA, User Service Access (USA) Operations Concept Document
    - 452-ICD-USA/Cx Network, Interface Control Document between the User Service Access System and the Constellation Network (CxNetwork)
  - Identification of known CxP issues with SNs planned implementation approach & rationale
  - Identification of additional requirements that require further study
- **USA design information will be presented at the System Definition Review scheduled for September 2008**



Welcome – Purpose of Review (continued)

- To perform a Code 450 Peer Review
- To provide an overview of the USA effort within the current system
- To describe the requirements and concepts that are driving the USA effort
- To describe the NASA USA system requirements and operations concepts
- To convey the USA architecture concept
- To provide recommendations for how to proceed
- To describe the risks associated with the implementation of the USA
- To ensure a thorough understanding of the risks associated with the current USA plans
- To demonstrate readiness and receive approval to proceed to the Design Phase of the USA System

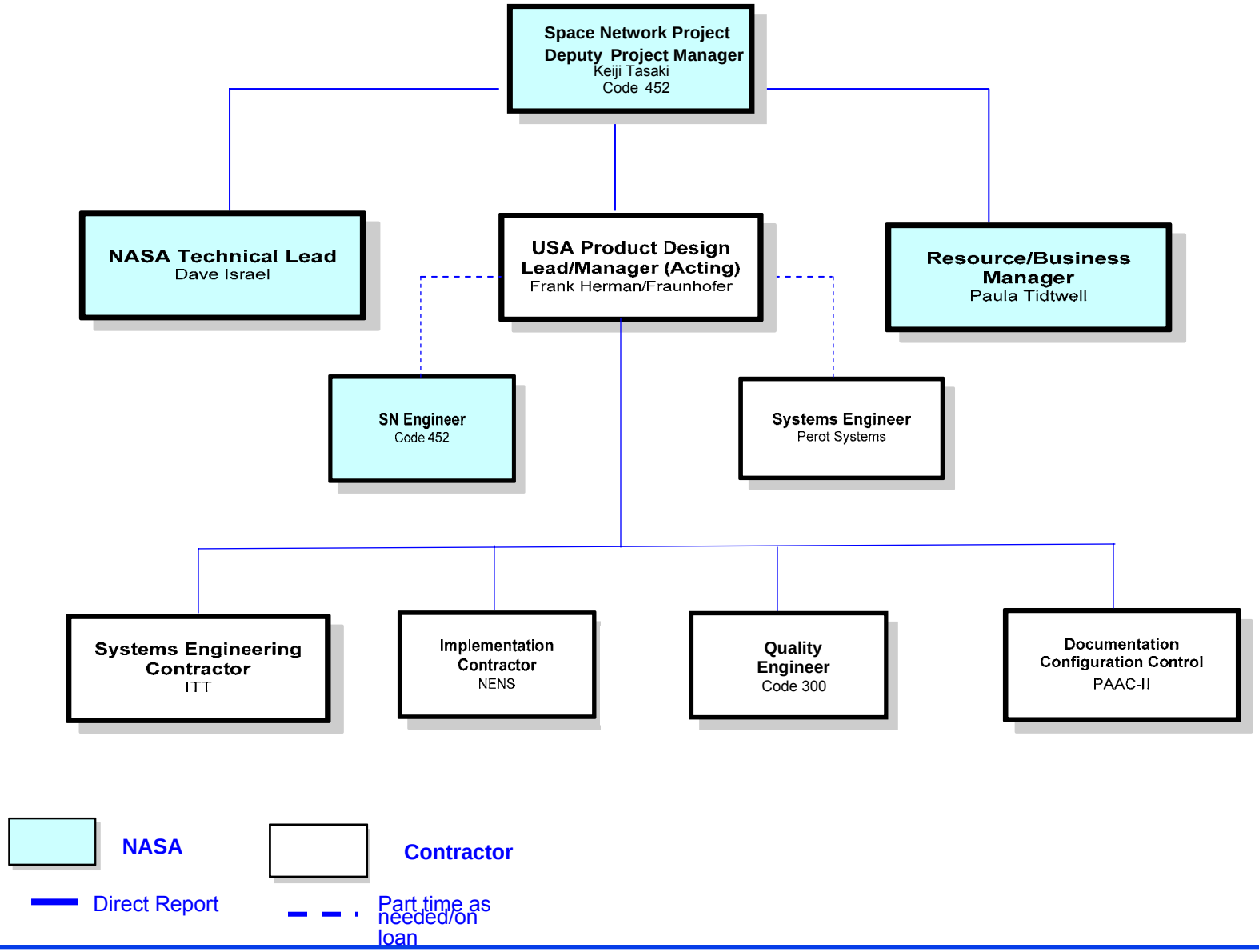
Section 1. Review Board

- Carolyn Dent – Chair, NASA Code 300
  Office of Systems Safety and Mission Assurance
- Harry Shaw – NASA Code 560 Electrical Engineering Division
- Polly Estabrook – JPL Code 3320
- Belkacem Manseur – NASA, Code 300
- Tom Gitlin – NASA, Code 456, SNE Project
- Kul Bhasin – NASA Glenn Research Center
- Dan Hein – White Sands Complex

Request For Action (RFA) Process

- An RFA is normally written as a result of the perception of unacceptable technical, cost or schedule risk
  - Each RFA must clearly state the action that the project is required to take. Provide a target due date.
  - The RFA rationale must clearly state the consequences of the project not taking the recommended action.
  - RFA's must be written or sponsored by a Review Team Member
- All RFA's will be tracked by the Code 450 CCB
  - RFA closure requires originator and Review Team Chair concurrence
  - The general project goal is to respond to all RFA's within ***1 week*** of SRR
  - Originators must accept or reject a proposed closure response within ***1 week*** of receipt
- Draft RFAs will be briefed to the project at the conclusion of this review
  - Blank RFA forms are available from Neil Dissinger (301-286-5832) or the review chair.
  - An electronic version of the RFA form can be obtained at **http://scp.gsfc.nasa.gov/snis/**
- RFA originators need to ensure contact information (e-mail address and telephone number) is provided

Section 1. USA Organization Chart



What is USA?

- USA's purpose is to implement new capabilities documented in the Cx-CTN IRDs & OCDs and the C^3I Specification into the Space Network in time to support the Orion 1 launch in March 2013.
  - USA is not a new concept
  - UAS originated as the Space Network IP Services (SNIS) project by Dave Israel some 5 years ago
- USA, in conjunction with User Service Subsystem Replacement (USSR) effort, additionally establishes a baseline for future SN Modernization.
- Both USA and USSR services will be made available to the SN Modernization Project.

SN Approach to Meeting CxP Requirements

Collection of SN Systems to be Modified for CxP Requirements

User Services Subsystem Replacement (USSR)

NEW

- AOS Frames
- LDCP Coding

User Services Access (USA)

NEW

- CCSDS IP Encapsulation
- IP header compression support
- IF & Line Outage Recording
- Tracking Data Msg delivery

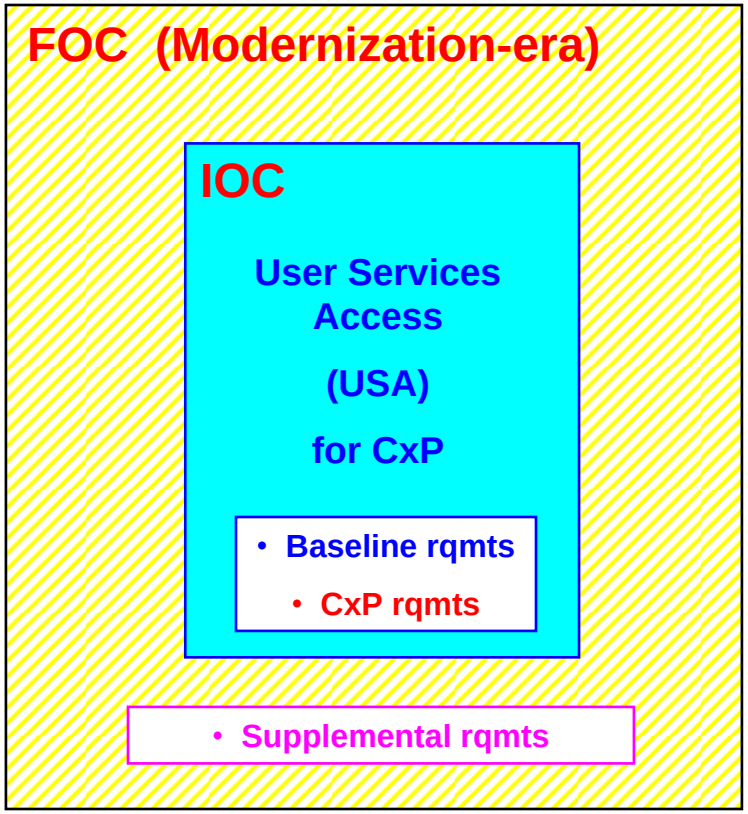
Changes to Existing Legacy Systems (e.g., NCCDS & ADPE)

Mods

- New interfaces with USA & USSR subsystems
- Accommodation of new capabilities provided by USSR & USA (e.g., LDPC and Encapsulation)

USA Implementation Plan Context (IOC/CxP vs. FOC/Modernization)

- USA is initially being implemented as an SN Upgrade to meet CxP requirements
  - Initial delivery referred to as the USA Interim Operations Capability (IOC)
  - Requirements for IOC delivery categorized as "Baseline" and "Constellation" in review package
- Subsequent USA deliveries lead to the Full Operations Capability (FOC)
  - Assumed to be part of and handled by the SN Modernization Project
  - USA IOC to be provided to SN Modernization for reuse, expansion, etc. as appropriate
- This USA SRR primarily focuses on the IOC-driving requirements and ops concept scenarios (i.e., by CxP)
  - Supplemental (FOC) requirements addressed where possible



IOC - Interim Operations Capability

FOC - Full Operations Capability (i.e., Modernization era)

Baseline*, *Constellation*, *Supplemental

Why is USA going to SRR now? (1 of 2)

- USA is faced with a very tight implementation schedule to support the Orion 1 manned launch in March 2013. Per John Rush/NASA HQ, Constellation is the SNs most important NASA customer.
  - General rule of thumb is for installation 1 year before in service use which indicates deployment NLT March 2012
  - Additionally, it is desirable to maintain a schedule reserve of 6 months to accommodate procurement delays, etc. which moves the schedule to September 2011 – approximately 3.5 years for design, implementation and test
- Within the 3.5 year timeframe, USA must:
  - Develop a system design and design and build the Development, Test & Training (DT&T) facility (1 year)
  - Implement the design, including issuing procurements for new hardware elements (2 years)
  - Conduct Integration and testing, ensuring Cx requirements are satisfied, USA integrates with USSR and there is no impact on the existing SN customer base (6 months)

Why is USA going to SRR now? (2 of 2)

- So that an unrealistic schedule compression does not occur and sufficient time will be maintained for testing and burn-in, USA must
  - Establish a requirements baseline that consists of:
    - Known, firm requirements {referred to as Baseline Requirements}
    - SN proposed solutions for CxP soft requirements as agreed to by SN and CxP via this SRR {referred to as Constellation Requirements}
    - Supplemental requirements such as the White Sands Complex TCP/IP Data Interface Services Capability (WDISC) Replacement, Space Link Extension (SLE), etc. that set a foundation for SN modernization in the future {referred to as Supplemental Requirements}
  - Proceed with an evolutionary design that is extensible and flexible to easily accommodate evolving CxP requirements and requirements that require additional study
- It is recognized that there is some risk in this approach. However, it is our belief that this risk is less than the risk associated with compressing the USA implementation, testing and burn-in schedule

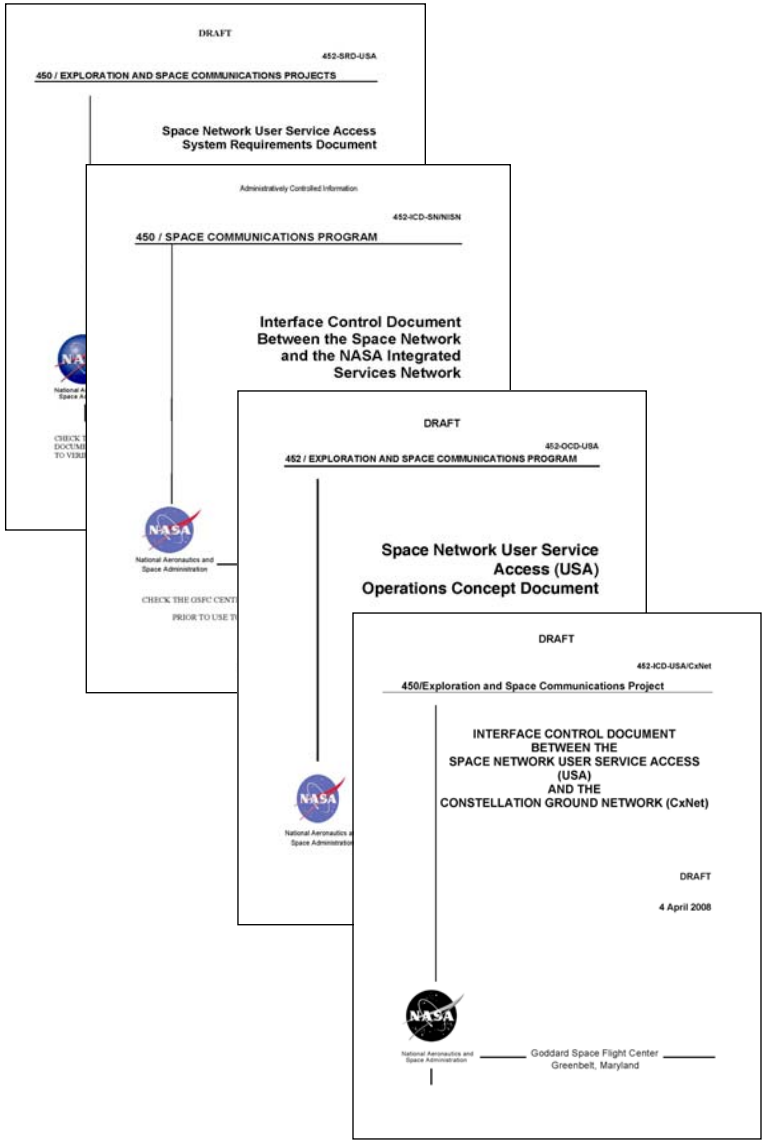
Section 1. Schedule

System Requirements Review	May 12, ’08
RFA Submission	SRR date + 1 day
RFA Proposed Resolution Provided	SRR date + 2 weeks
RFA Originator Acceptance or alternate solution	SRR date + 4 weeks
Documentation update & review	SRR date + 7 weeks
Documentation CCB’s	July 7, ‘08
Preliminary Design Phase	April ’08 to October ’08
System Definition Review (SDR)	September 4, ‘08
Preliminary Design Review (PDR)	April 1, ‘09
Critical Design Review (CDR)	September 1, ’09
Test Readiness Review (TRR)	September 1, ‘11
Operations Readiness Review (ORR)	October 31, ’12

Section 2
Documentation

Section 2. USA Product Documentation

- USA System Requirements Document (452-SRD-USA). available
- DCN to ICD Between SN and NASA Integrates Services Network (NISN) (452-ICD-SN/NISN). Draft. available
- USA Operations Concept Document (452-OCD-USA). available
- ICD Between USA and the Constellation Project (452-ICD-USA/CxP) draft available
- USA Product Management Plan (452-PMP-USA) available
- USA Security Plan (452-SP-USA)
  Under development-target date of 2 months after PDR



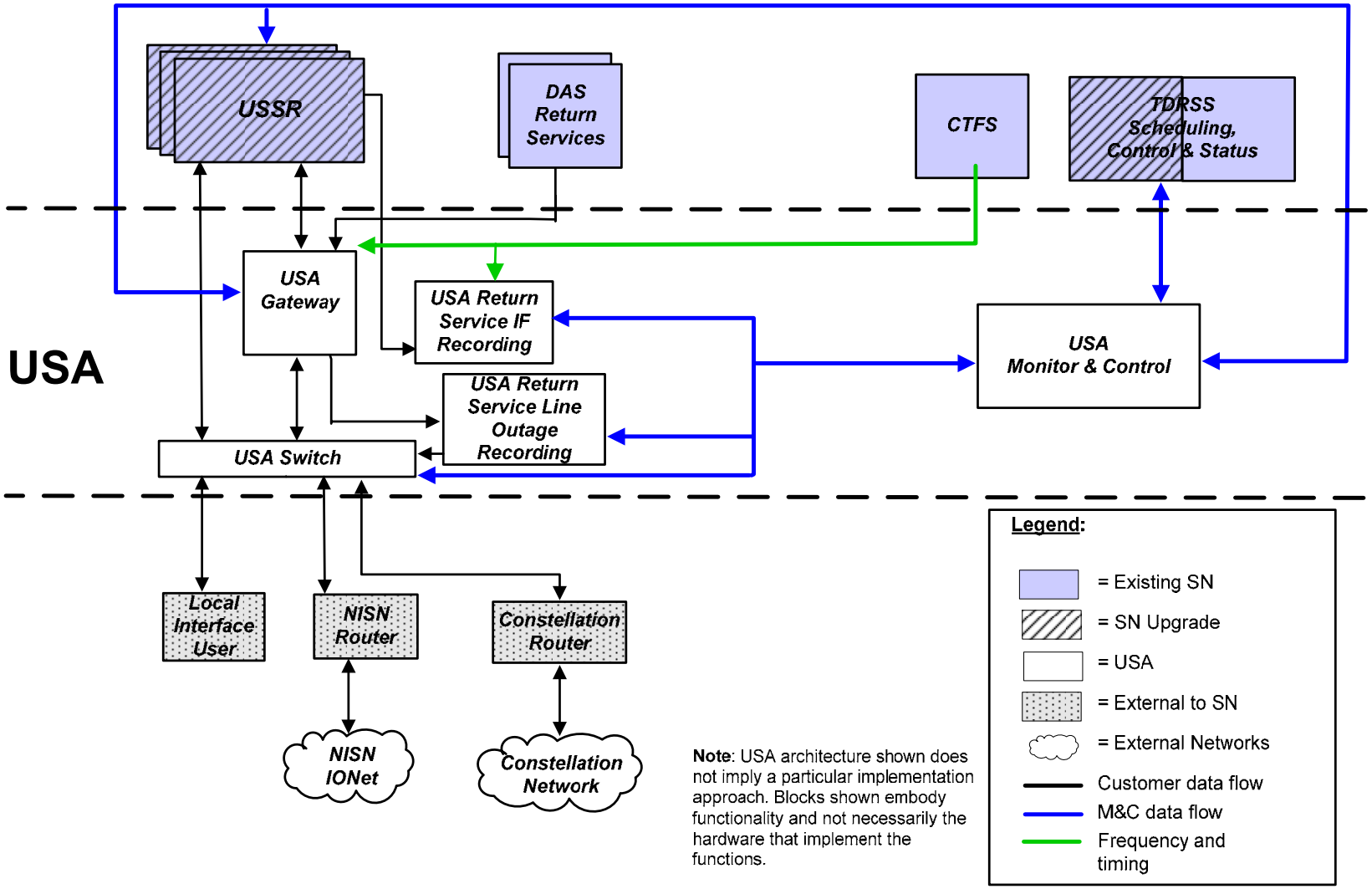
Section 3
System Description

USA “Ground Rules”
USA Reference Architecture
USA Interfaces
Driving Requirements
Architecture Description

Section 3. USA "Ground Rules"

1. USA system will meet the current set of SN requirements (post STS era)
    1. Delta to existing SN system
2. USA will not affect support to existing customers
3. USA will provide several new interfaces/capabilities alongside existing capabilities:
    1. We will be working with existing customers and will offer a migration path to the new interfaces/capabilities
    2. Ongoing operations (from a customer's point of view) will not be disrupted during USA implementation
4. SN will primarily continue as a bent-pipe network, with little knowledge of the actual customer data
5. USA will be fully consistent with the *SN Users' Guide*
6. USA will be designed to operate for 15 years and will be designed for flexibility and expandability

Section 3. USA Reference Architecture



Note: USA architecture shown does not imply a particular implementation approach. Blocks shown embody functionality and not necessarily the hardware that implement the functions.

Section 3. USA Interfaces

- USA-User Service Subsystem Replacement (USSR) (*internal interface within SN*)
  - Scheduling, Control, and Status interfaces
  - Forward and return link data interface
  - Captured in USA System Requirements Document (SRD) Appendix B at this time.
- USA-Data Interface System (DIS) Automatic Data Processing Equipment (ADPE) (*internal interface within SN*)
  - USA Monitor & Control (M&C) interface to the existing scheduling system via the DIS ADPE
  - Interface carries system commands, operational data messages etc.
  - Will be captured as a DCN to the existing document: 530-ICD-NCC-FDF/WSC , The ICD Between the WSC and the NCC/FDF
- USA-NASA Integrated Services Network (NISN)
  - Standard synchronous serial and Ethernet connections
  - Defined in DCN to the existing document 452-ICD-SN/NISN
- USA-CxP *(detailed discussion in section 6 of this presentation)*
  - Standard synchronous serial and Ethernet connections
  - Defined in recently developed Draft Interface Control Document between the SN and the Constellation Program, USA/CxP ICD

Section 3. USA Driving Requirements

- Primary drivers for the User Service Access system:
  - Technical and schedule requirements of Constellation Program
    - Technical Requirements:
      - » CCSDS Encapsulation for IP (IP over CCSDS space Links; CCSDS 702.1-R-2)
      - » Support for IP header compression
      - » Intermediate Frequency (IF) Recording
      - » Enhanced Line Outage Recording (LOR), recording of customer return service data
      - » Tracking Data Message (TDM) delivery
    - Schedule Requirement: March 2012
- Secondary drivers (Technical)
  - SLE Transfer service
  - WDISC replacement
  - Demand Access System (DAS) interface
- Other Considerations
  - SN/CxP demarcation point
  - CxP CR000130: Reduced Reliance On Ground Networks
  - Dissimilar voice and Emergency communications
  - Reentry and Recovery support for CxP
  - SN Modernization and TDRS K/L procurement

Section 3. Architecture Description

- Major USA functions: Gateway, Switch, Monitor and Control, and Recording
- USA functions performed on customer data are limited to the Open Systems Interconnection (OSI) layers 1 (Physical Layer) and 2 (Data Link Layer) only

USA Architecture Description
Gateway Functions (1 of 2)

The USA Gateway performs the following two functions:

- Link layer framing
- Customer data transport using TCP/IP

- The USA gateway will perform link layer framing/deframing, frame error detection, and CCSDS IP datagram encapsulation (ENCAP) per CxP requirements.

USA Architecture Description
Gateway Functions (2 of 2)

The Gateway provides TCP/IP data access service and CCSDS SLE services.

Enhances the WDISC functionality at WSC while maintaining backward compatibility.

The TCP/IP Interface service provides a bit-stream to TCP/IP conversion function that can:

- Receive IP encapsulated forward service data from a customer MOC via the NISN IONet, convert the data to serial form, and present it to the User Service System-Replacement (USSR) subsystem,
- Receive bit-stream return service data from the USSR, IP encapsulate it, and transmit to a customer Mission Operations Center (MOC) via the IONet.
- Perform data monitoring/reporting functions according to customer generated data channel processing specifications.

The SLE Service implements the CCSDS compliant SLE transfer services to transport forward and return data between a customer facility, such as the MOC, and the WSC. SLE transfer services are defined in terms of operations that are requested and performed in the context of a scheduled transfer service instance.

The SLE function encompasses the SLE System as defined in the document CCSDS 910.4-B-2. As a minimum, the SLE function will provide the following SLE transfer services:

- Return Service – Return All Frames (RAF) service to retrieve all frames received on a physical space link channel, including legacy bit stream data types
- Return Service – Return Channel Frames (RCF) service to retrieve all frames of a master channel or of a virtual channel;
- Forward Service – Forward Command Link Transmission Units (FCLTU) service to deliver command/forward link data to the spacecraft.

Architecture Description
Switch Function

The USA Switching function

- Provides schedulable data paths for the TDRSS forward and return services; (data paths are between the USSR and the NISN/Constellation routers or customer unique equipment).
- The USA switching function operates at OSI Layers 1 and 2
- Layer 1 switching allows synchronous bit stream transport to and from customer unique equipment requiring Local Interface (LI) services.
- Layer 1 switching allows the use of serial interfaces on the routers.
- Layer 2 switches allow direct IP and IP data access services.

Architecture Description
Monitor and Control (M&C) Function

The USA Monitor and Control (M&C) function provides the capability to control and monitor the full range of USA and USSR functionalities for all supported SN services.

- Capable of being controlled by the NCCDS (via Data Interface System (DIS) Automated Data Processing Equipment (ADPE))
  - Indicated by TDRS Scheduling, Control and Status in Reference Architecture
- Will complement the existing SN Exec ADPE.
- In future, USA M&C will be controlled by a ground Monitor and Control Subsystem under the proposed SN Modernization program.
- Customer access to performance parameters of USA/USSR functions through User Performance Data (UPD) messages delivered via the Space Network Access System (SNAS).
- Additionally, the M&C system will facilitate the delivery and recording of radiometric Tracking Data Messages (TDMs) directly to customers (CxP requirement).

Architecture Description
Return Service Recording

The USA Return Service Recording (RSR) function records customer return service in two ways as follows:

- **Recording at the Intermediate Frequency (IF) stage (CxP).**
  - Intended for anomaly investigations, and the data are retained for a specified period of time.
  - Customer access to the recorded data is made available on physical media.
- **Line outage recording (LOR)**
  - To ensure data integrity in the event of a failure in the terrestrial connection between the WSC and the customer facility.
  - Data retention period is user selectable, and a data retrieval capability based on Secure Copy Protocol (SCP) is provided for the retrieval of LOR data.
  - Considering renaming to Return Service Data Recording (RSDR)

Section 4

System Requirements

Introduction

SRD Section 4 - System Requirements (Richard Broomandan)

- General Requirements
- Logging Requirements
- Switching Requirements
- Gateway Requirements
- Monitor and Control Requirements
- Recording Requirements

SRD Section 5 - Reliability, Maintainability, and Availability Requirements

SRD Section 6 - Security Requirements

SRD Section 7 - Equipment Design, Construction, and Installation Requirements

SRD Section 8 - Maintenance Requirements

System Requirements - Introduction

- For traceability purposes, the USA requirements are grouped under three categories:
  - **Baseline requirements**
    - Requirements for the initial implementation of the USA.
  - **Constellation requirements**
    - Requirements that are specifically traced to the Constellation Program (CxP)
  - **Supplemental requirements**
    - Requirements allocated for future USA expansions. (Provision must be made in the initial implementation of the USA to facilitate system upgrades to accommodate these requirements.)
- Appendix A of the SRD provides a requirement traceability matrix that includes the above grouping. (See backup material for Appendix A)
- Ensuing presentation follows the structure appearing in Sections 4 through 8 of the Systems Requirement Document. The following color code is used to identify the requirement categories:
  - **Baseline**, **Constellation**, **Supplemental**

General System Requirements

Baseline*, *Constellation*, *Supplemental

- The USA shall support all existing SN data services as well as DAS services –
  - includes KaSAF, KaSAR, KuSAF, KuSAR, SSAF, SSAR, MAF, MAR, SMAF, SMAR, DAS.(108 existing SN services)
- The USA shall support a minimum of 12 (TBR) simultaneous additional TDRS forward services
  - 4 SSAF, 2 KaSAF, and 6 standby
- The USA shall support a minimum of 12 (TBR) simultaneous additional TDRS return services
  - 4 SSAR, 2 KaSAR, and 6 standby
- The USA shall support IPv4
- The USA shall support IPv6
- The USA shall be capable of remote operation of USA functions
- The USA shall deliver ALL Constellation data products to CxP router(s)
- The USA shall support all TDRSS forward data rates up to 6 Mbps
- The USA shall support all TDRSS return data rates up to 25 Mbps
- The USA shall be capable of automatically configured in 35 sec.
- The USA shall execute changes to reconfig. params. in response to customer requests within 35 seconds.

Logging System Requirements

- The USA shall log the following for all functional components:
  - Startup and shutdown, Authentication, Authorization/permission granting, Action by trusted users, Process invocation, Unsuccessful data access attempts (threshold = log on five unsuccessful attempts), Data deletion, Data transfer, Configuration change, Application of confidentiality or integrity labels to data, Override or modification of data labels or markings, Output to removable media, Output to a printer.
- USA log records shall contain: source, severity, timestamp, USA ID of person, text field with event description.
- USA log records shall be maintained on a central log server
- USA shall provide an audit trail in compliance with NPR 2810.1A
- USA log records shall be archived, protected, and access limited

Switching System Requirements

Baseline*, *Constellation*, *Supplemental

- USA shall provide schedulable synchronous serial data paths to USSR
- USA shall provide schedulable data paths between the USA Gateway and the NISN routers
- USA shall provide schedulable data paths between the USA Gateway and the Constellation routers
- USA shall provide DAS return data to NISN routers
- USA shall carry a single customers data on the same NISN router interface
- USA shall carry a single customers data on the same CxP router interface
- USA M&C function shall control the USA Switch function
- USA shall maintain complete separation/isolation between networks (NISN closed, NISN Restricted, CxP)
- USA Switch shall be configured in less than or equal to 35 seconds
- USA Switch status and health provided to M&C every 5 seconds

Gateway System Requirements (1 of 4)

Baseline*, *Constellation*, *Supplemental

- Gateway shall be configurable based on commands received from M&C
- Gateway shall provide Point to Point Protocol (PPP) and Frame Relay Protocol interfaces to the routers
- Gateway shall be backward compatible with WDISC
- Gateway shall implement SLE FCLTU, RAF, and RCF services
- Gateway shall have a client/server relationship with the customer MOCs (the client or server can be either the Gateway or the MOC)
- Gateway shall exercise access control based on identity of initiator and responder (e.g Gateway, remote MOC, or user)
- Gateway shall implement authentication for invocation of all data transfer services

Forward Gateway Requirements (2 of 4)

Baseline, Constellation, Supplemental

- A forward data channel processing spec. shall be activated prior to a scheduled service start time. The processing specification is as specified in the 452-OCD-USA document. The specification contains: processing requirements, link layer specifications and a valid MOC IP address
- The Gateway shall initiate a TCP/IP connection with a customer MOC, if selected by the customer
- The Gateway shall be able to accept forward data flow configuration control information from the MOC
- The Gateway shall accept forward packet data files from the USA Switch which may contain IP packets destined for customer platforms or customer data encapsulated in IP packets
- The Gateway shall transfer IP packets using CCSDS AOS VCP/ENCAP Service, if selected by the customer
- The Gateway shall perform link layer protocol translation between PPP/MPoFR and CCSDS ENCAP to support IP header compression, if selected by the customer
- The Gateway shall encapsulate forward service data inside CCSDS AOS frames, if selected by the customer
- The Gateway shall perform idle pattern generation, if selected by the customer
- The Gateway shall transfer data to the USSR via synchronous, serial, bitstream

Return Gateway Requirements (3 of 4)

Baseline*, *Constellation*, *Supplemental

- A return data channel processing spec. is activated prior to a scheduled service start time. The specification contains: processing, monitoring, recording requirements, as well as link layer specifications and a valid MOC IP address
- The Gateway shall establish a TCP/IP connection with the MOC, if selected by the customer
- The Gateway shall receive synchronous, serial bitstream return data from the USSR
- The Gateway shall extract data packets encapsulated in CCSDS AOS frames, if selected by the customer
- The Gateway shall extract IP data packets encapsulated inside CCSDS AOS VCP/ENCAP, if selected by the customer
- The Gateway shall perform link layer protocol translation between CCSDS ENCAP and PPP/Multi Protocol over Frame Relay in support of IP header compression, if selected by the customer
- The Gateway shall monitor link layer performance parameters and include performance info in protocol headers appended to return service data, if selected by the customer

Return Gateway Requirements (cont.)(4 of 4)

Baseline*, *Constellation*, *Supplemental

- The Gateway shall time tag data frames with an accuracy of 10 ms, if selected by the customer
- The Gateway shall send the return service data packets to the NISN routers using the specified link layer protocol
- The Gateway shall send the return service data packets to the CxP routers using the specified link layer protocol
- The Gateway shall provide return service data streams to LOR recorders
- The Gateway shall provide status and health to the M&C function every 5 seconds

Monitor and Control System Requirements (1 of 2) Baseline, Constellation, Supplemental

- M&C shall be scheduled, controlled and monitored through the DIS ADPE
- M&C shall use an open-standards based architecture built on IP technology
- M&C shall indicate via an operator alert when abnormalities are detected in USA or USSR operations and/or resources
- M&C shall accept customer sets of USA resource configuration parameters as well as shall accept reconfiguration parameters from customers
- M&C shall configure USSR and accept reconfiguration parameters for USSR
- M&C shall collect and log status on each scheduled event; on each customers allocated network interface; and on customer's allocated USSR resources
- M&C shall generate USA and USSR resource allocation status reports
- M&C shall receive Customer TDMs from USSR and format them into the TDRSS Universal Tracking Data Format (UTDF), and record TDMs
- M&C shall time tag logs, shall provide capability for Operators to: extract from logs; to archive logs onto removable media; view logged data; & to print

Monitor and Control System Requirements

(2 of 2) Baseline, Constellation, Supplemental

- M&C shall not exceed service response times specified in 530-RSD-WSC
- M&C shall reject Resource Allocation modifications within 1 min. prior to service termination
- M&C shall automatically log Resource Allocation and Configuration status at 1 minute intervals
- M&C shall log performance status of all components that constitute USA and those that constitute USSR once per second
- M&C shall provide the M&C parameters through existing planning, scheduling, and real-time messages as defined in 530-ICD-WSC/NCC-FDF
- M&C shall provide performance status data to NCCDS at 5 sec. intervals
- M&C shall send CxP Customer TDMs to the CxP router every 10 secs (TBR).
- M&C shall send recorded CxP Customer TDMs to the CxP router within 10 minutes (TBR) of a valid request
- M&C shall retain system status log data for 1 yr.

Return Service Recording (RSR) System Requirements (1 of 2)

Baseline, Constellation, Supplemental

- RSR function shall be automatically configured by the USA Monitor & Control System
- RSR shall receive the S-band SA and Ka-band SA return service for IF (TBD MHz) recording
- RSR shall record IF samples in terms of identifiable, time tagged data blocks with a not to exceed length of 3 hours
- RSR shall retain each recorded IF block for a minimum of 2 hours before discarding
- RSR shall make recorded media available for IF recording
- RSR shall receive return service data frames from the USA Gateway
- RSR shall record these frames into LOR data files
- RSR shall retain LOR data files for a minimum of 7 days and a maximum of 30 days
- RSR shall provide LOR data upon request per USA Ops Concept Document

Return Service Recording (RSR) System Requirements (2 of 2)

Baseline, Constellation, Supplemental

- Return Service Recording function shall support data rates less than or equal to 25 Mbps
- RSR shall provide current Status and Health to the M&C every 5 seconds in accordance with present WSC hardware specs.

SRD Section 5 Reliability, Maintainability, and Availability Requirements

- **Standard SN RMA definitions and computations apply.**

Key Points:

- **Mean Time To Repair (MTTR): Not to exceed 30 minutes during 15 yr. life**
- **Inherent Availability: 0.9998 (for any 10,000-hour period)**
- **All USA equipment shall meet the USA Operational Availability requirement of: 0.9999 (for any 10,000-hour period)**
- **USA will meet the same availability requirements as existing WSC systems**

Refer to Backup Material for detailed RMA requirements

USA Security

(Joe Clark)

The Security Life Cycle

- Establish the Security Categorization
- Select the Security Controls
- Assess the Risks and refine the Security Controls
- Document the Security Controls in the Security Plan
- Implement the Security Controls
- Assess the Security Controls Implementation
- Authorize the operation of the System
- Monitor the performance of the Security Controls
- Start all over again

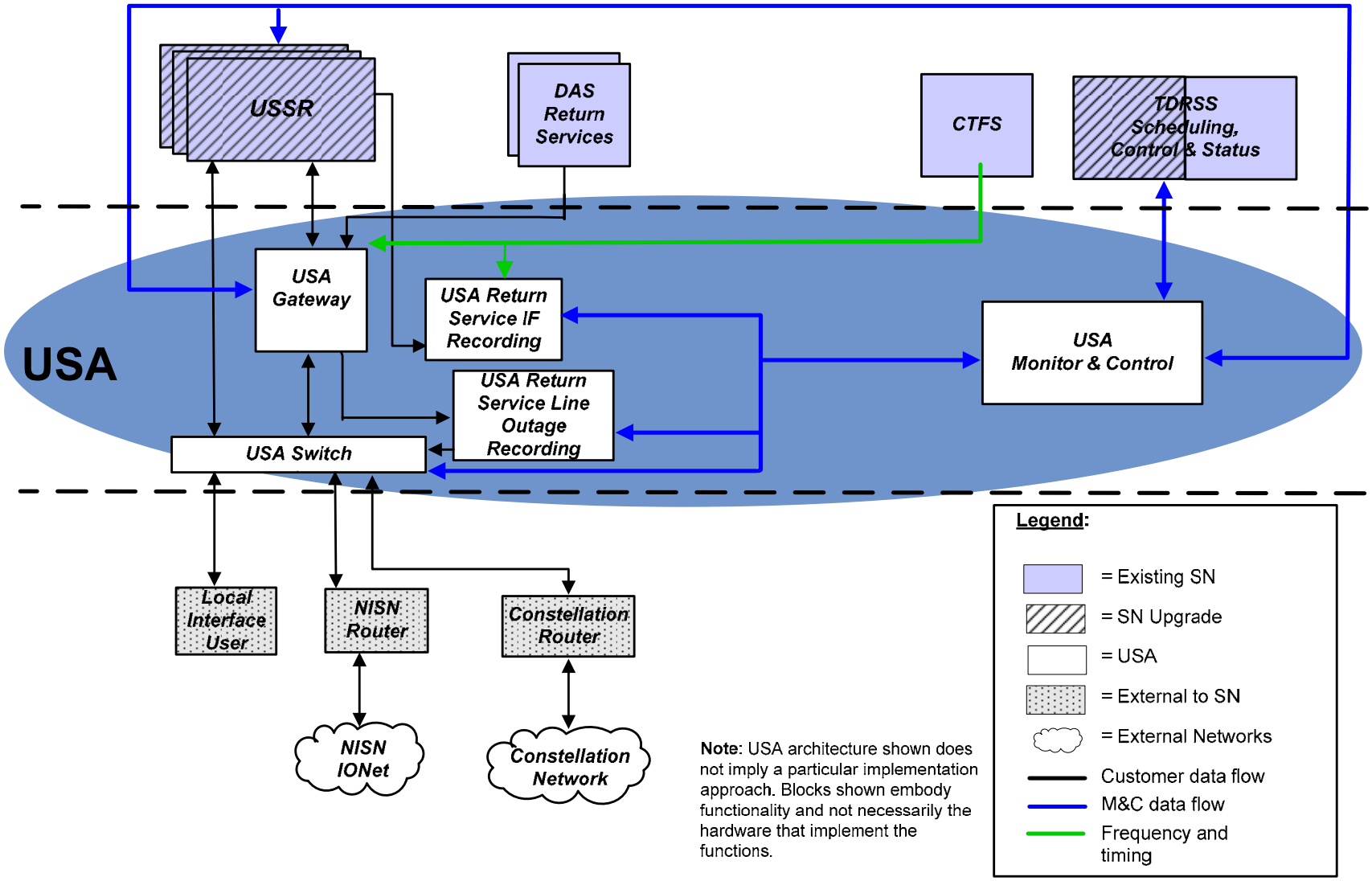
The USA Security Plan Status

- The Security Categorization has been established
- The Security Controls have been selected
- Details of the design and implementation are required before the process can be completed

FIPS 199 Security Category

- Federal Information Processing Standard (FIPS) 199/National Institute of Standards and Technology (NIST) SP 800-60 Information types that will be processed by USA
  - Security Categorization: High
    - Space Operations Information (D.11.4)
  - Security Categorization: Moderate
    - Space Exploration and innovation Information (D.19.2)
    - Research and Development Information (D.20.1))
  - Security Categorization: Low
    - Customer Service Information (C.2.6.1)
    - Facilities, Fleet, and Equipment Management (C.3.1.1)
    - Information and Technology Management (C.3.5.4)
    - Information Infrastructure Management Information (D.22.4)
- Security Categorization (High Water Mark): High

USA System Security Boundary



Note: USA architecture shown does not imply a particular implementation approach. Blocks shown embody functionality and not necessarily the hardware that implement the functions.

Security Document Preparation Status

- Required documents cannot be fully developed because implementation details are not available
- Security Plan is about 60% complete
  - All security controls listed in NIST SP 800-53 for High Systems are included
  - Implementation of many of these controls is either mandated by NASA or provided by WSC
    - Awareness and Training
    - Physical and Environmental protection
  - Implementation of the Technical Controls depends on the system design and implementation
    - Identification and Authentication
    - Access Control
    - Audit and Accountability
    - System and Communication Protection
- Risk Assessment Document is about 60% complete
- Place holders have been prepared for other documents including
  - The Self Assessment Plan
  - The Plan of Action and Milestones (POA&M)

Section 6 USA SRD Security Summary

Baseline*, *Constellation*, *Supplemental

- Requirements based on Security Documents
  - Specific sections of NPR 2810.1a identified.
  - Specific section of the NISN access requirements called out in 290-004, IP Operational Network (IONet) Access Protection Policy and Requirements.
  - The Constellation Command, Control, Communication and Information (C3I) Interoperability Handbook
    - Volume 1: Interoperability Specification Section
    - Volume 5: Data Exchange Protocol Specification
- Security Features
  - The USA will initiate communications with external systems
  - The USA will automate enforcement of password rules
  - The USA will limit Customers' access
    - To services for which they are authorized
    - To networks for which they are authorized
  - The USA will create and maintain audit files

SRD Section 7 Equipment Design & Construction

- **Standard SN STDN and MIL specs. Apply.**
- **Key Points:**
  Requirements cover:
  - **Electronic Equipment Racks**
  - **Cabling and Connectors**
  - **Electromagnetic Interference**
  - **Modularity and Expandability**
  - **Computer Processor Reserve Capacity**
  - **Waivers/approval of PDL accepted, as needed, due to "dated" STDN specs**

Consistent with standard WSC definitions

Refer to Backup Material for detailed requirements

SRD Sect. 8 : Maintenance Requirements

- **Standard SN Maintenance Requirements specs apply.**
  Key points:
  - **Hardware 1st and 2nd level Maintenance is performed at WSC and will follow standard SN maintenance processes**
  - **Software maintenance is done at WSC SMTF**
  - **Spare parts and quantities shall be based upon satisfying the availability and maintainability requirements**
  - **Spare parts shall be available for 15 years after Final Acceptance Testing**

Refer to Backup Material for detailed requirements

Section 5
Concept of Operations

USA Operations Scenarios

Operational Capabilities

- **CCSDS Encapsulation (CCSDS ENCAP)**
- **Intermediate Frequency (IF) Recording**
- **IP Header Compression Support**
- **Line Outage Recording (LOR)**
- TCP/ IP Data Access (WDISC)
- CCSDS Space Link Extension (SLE)
- **Monitor and Control**

Operational Scenarios and Stages

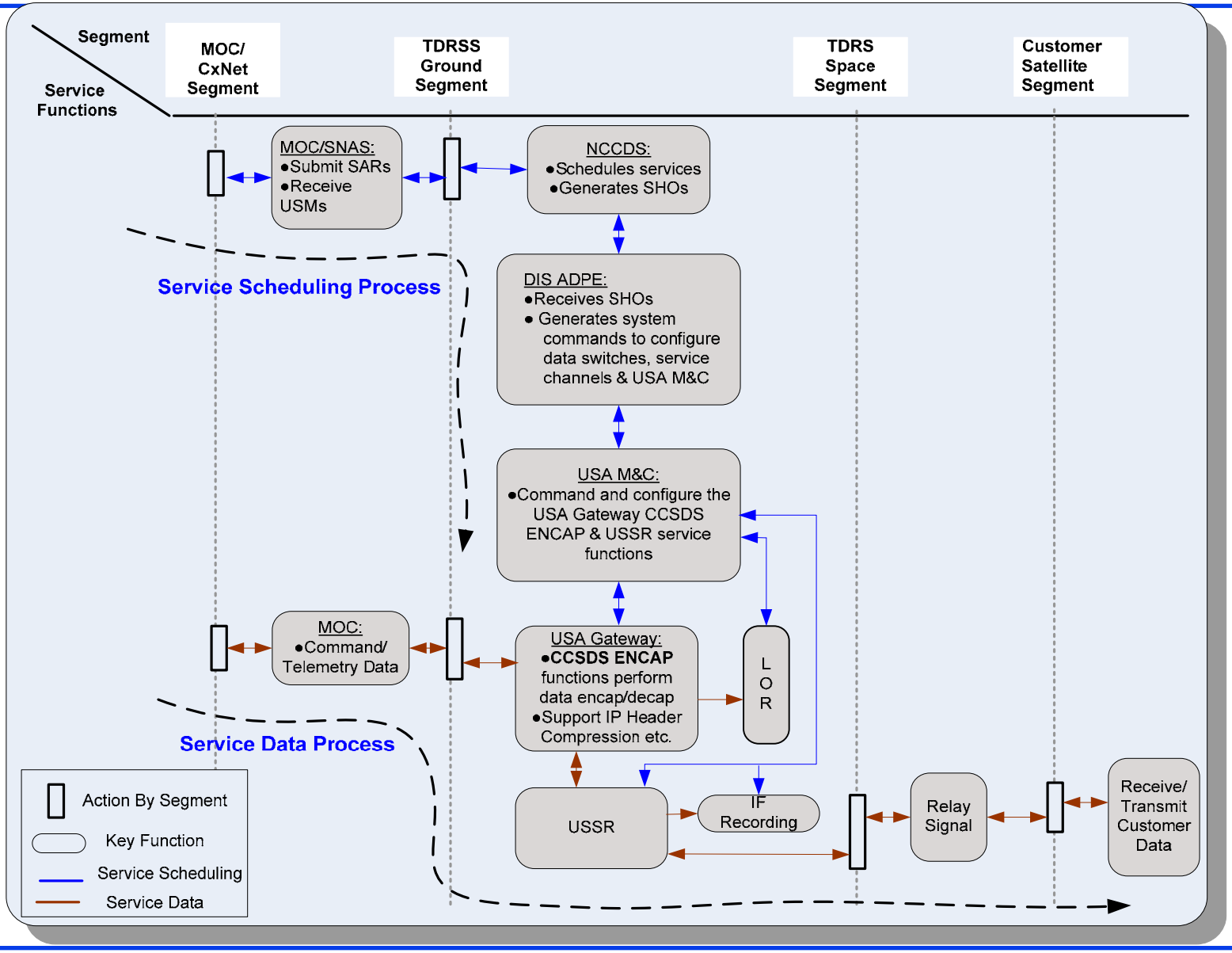
Operation Scenarios

- CCSDS Encapsulation Service (CCSDS ENCAP)
- Intermediate Frequency (IF) Recording Service
- Direct TCP/IP Access Service (WDISC)
- Space Link Extension (SLE) Service

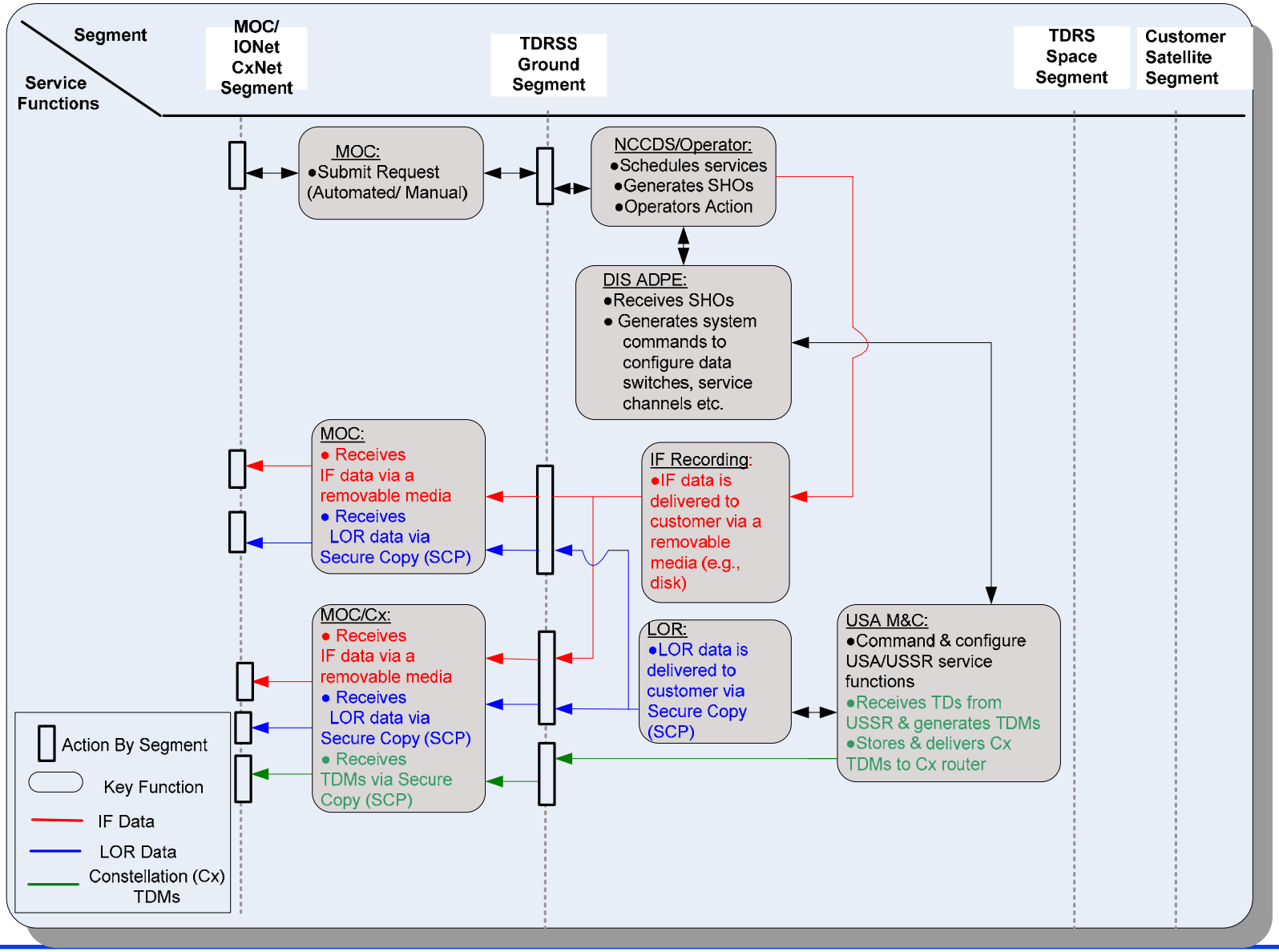
Operational Stages

- Service Request
- Service Planning
- Resource Allocation
- Service Implementation and Monitoring
- Real-Time Service Configuration
- Service Termination
- LOR Data Retrieval
- Performance Data

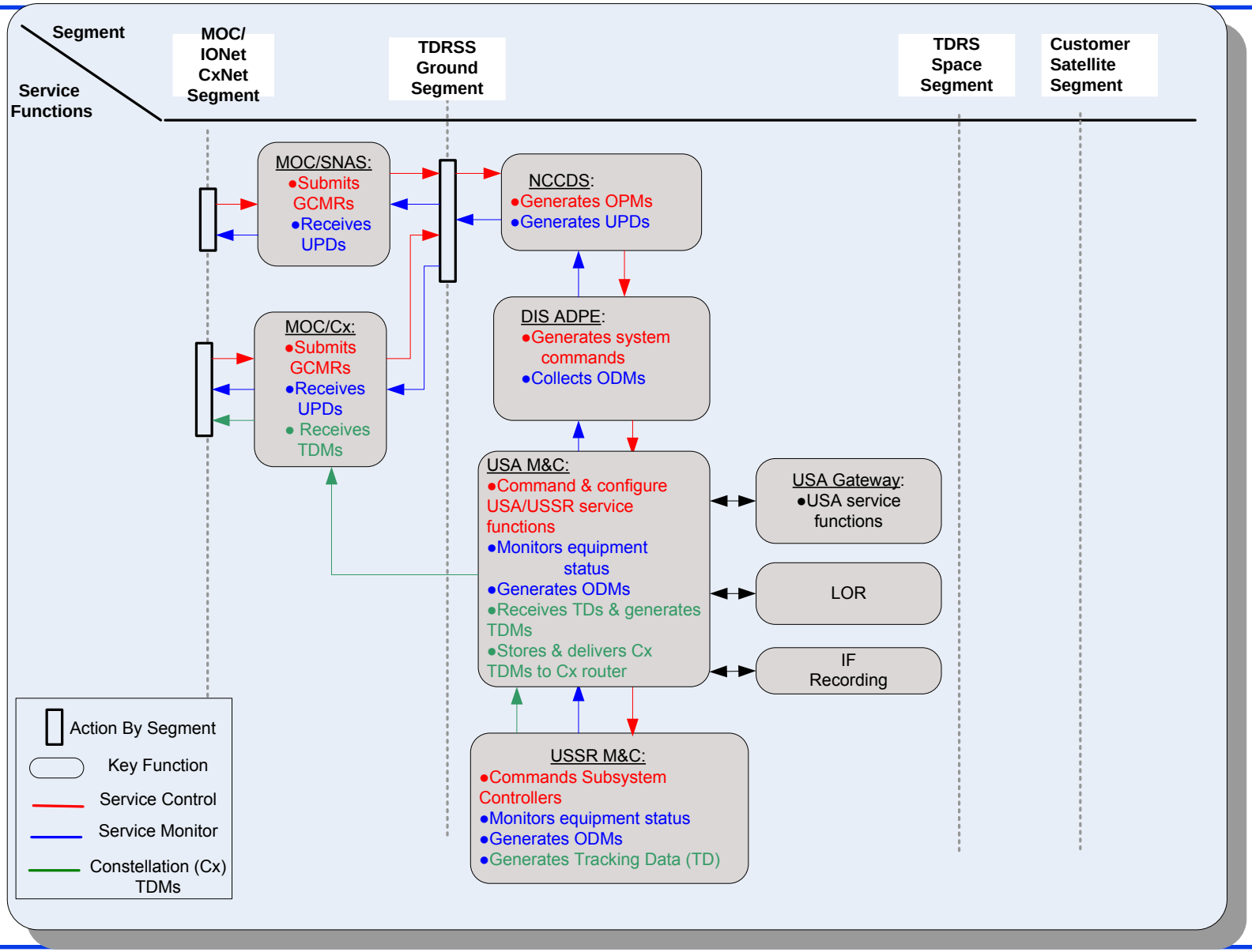
USA Service Scheduling & Data Operational Flows (CCSDS ENCAP)



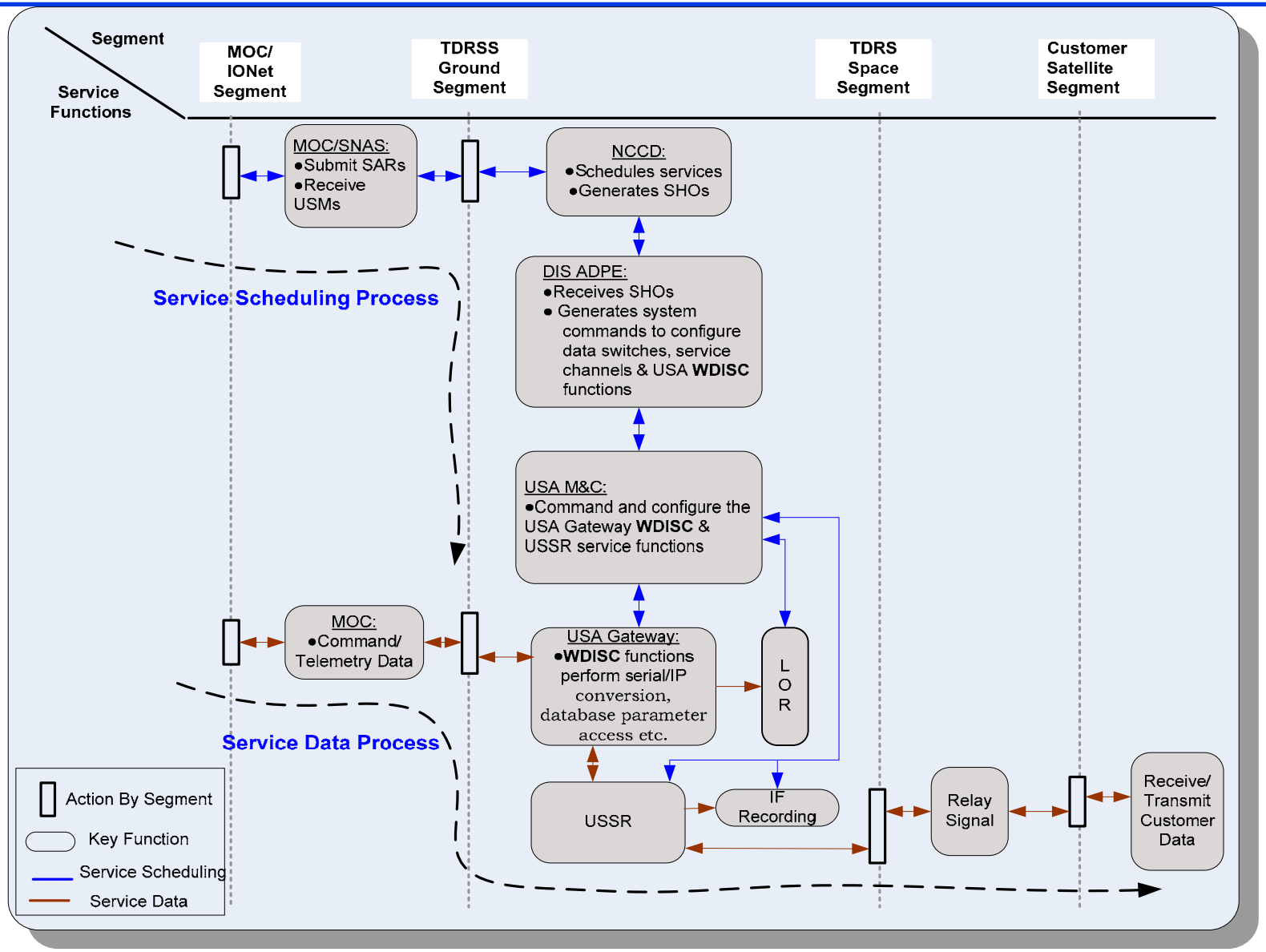
USA Service "Recorded Data/CxP TDMs" Retrieval Operational Flows



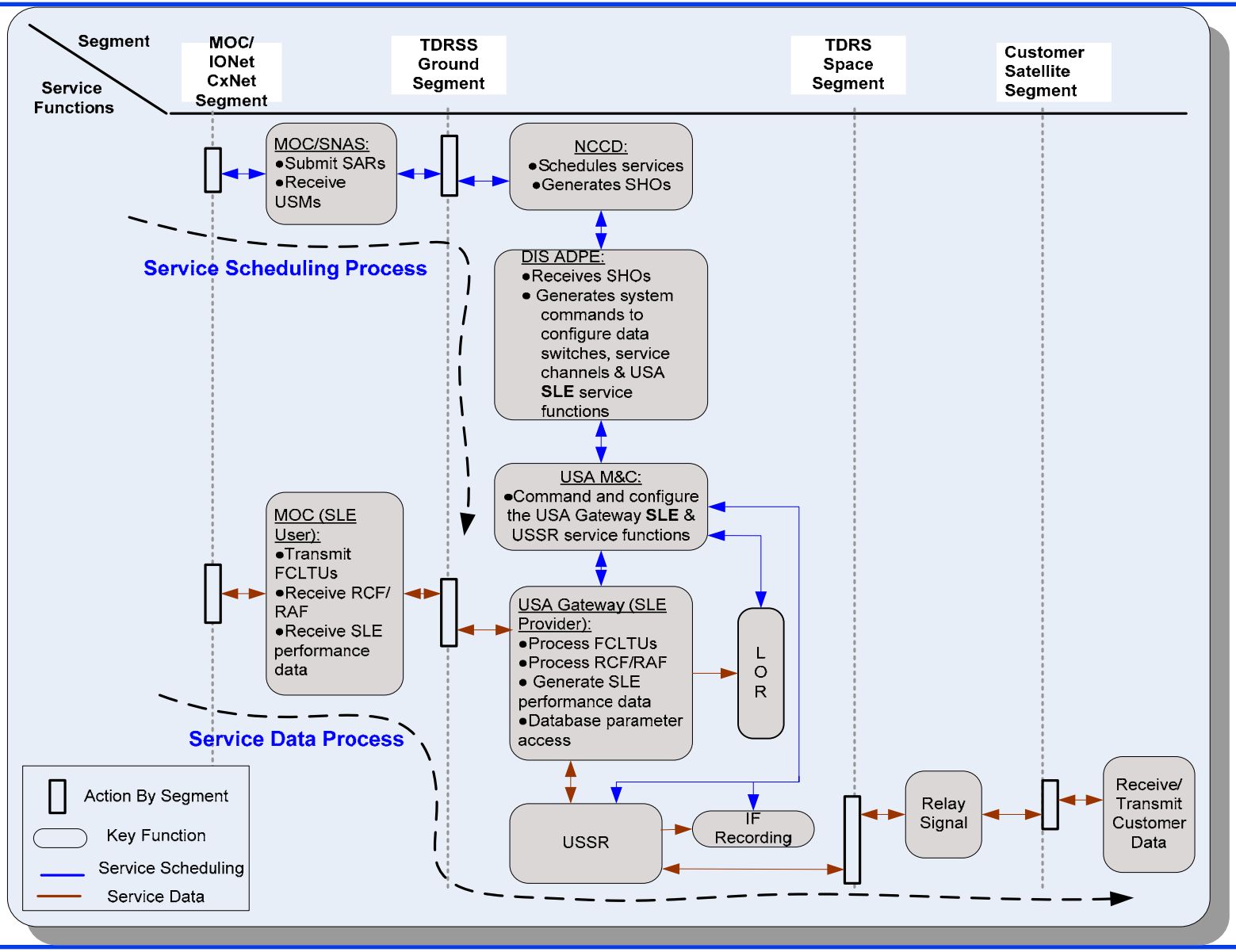
USA Service M&C and CxP TDMs Operational Flows



USA Service Scheduling & Data Operational Flows (WDISC)



USA Service Scheduling & Data Operational Flows (SLE)



Section 6
Requirements Under Study

SN Assumptions on CxP Interface
SN Questions & Clarifications for CxP
Requirements Under Study

SN-CxP Assumptions

- Low Density Parity Check (LDPC) Codec
  - Return Services
    - SN **WILL** discard LDPC blocks (AOS Frames) that have uncorrectable frames.
    - An AOS frame could contain a portion of one or more IP Packet(s).
  - LDPC encoding (on or off) selection is made prior to the actual event
  - LDPC functionality is not reconfigurable (via GCMR) in real-time
- IP Packet Processing
  - SN will only affect Layer One (Physical) and Layer Two (Data Link) of the ISO stack
  - The SN will perform High-Level Data Link Control (HDLC)/Multiple Protocol Over Frame Relay (MPoFR) handshaking between the CxP router and WSC equipment.
  - SN will not prioritize or drop IP packets based on CxP's Quality of Service (QoS) policies.
  - SN will not perform IP Header compression
- CCSDS Encapsulation Services
  - Encapsulates IP Packets into AOS Frames
  - Extracts IP Packets from AOS Frames
  - Detects when AOS Frames are missing (e.g., dropped by the LDPC decoder)
  - Incomplete IP packets shall be discarded
  - Must perform link layer negotiations that are required to support IP header compression

SN Assumptions (Continued)

- CxP Router
  - SN assumes that CxP will use commercially available routers with standard router serial interfaces (e.g., such as HSSI/ECL or RS-422).
  - The CxP routers are going to be located at White Sands Test Facility (WSTF).
  - SN assumes that each router will have only one full duplex physical interface (e.g., serial) per bidirectional RF link (e.g., SSAF/SSAR, KaSAF/KaSAR).
  - Based on the following assumptions, the SN assumes that it will need to have a maximum of 12 redundant interfaces with the CxP router(s):
    - Three RF links per vehicle (e.g., two links for the CEV and one link for the CLV).
    - A maximum of two simultaneous vehicles.
    - All interfaces are redundant.
  - The SN will not impact the end-to-end Maximum Transmission Unit (MTU).
  - The router performs IP header compression.

CxP Responsibilities

- CxP Router Management
  - Administration and Configuration
  - Firmware and Hardware Maintenance
  - Testing and Troubleshooting
- Quality of Service (QoS)
  - Bandwidth Management
  - Packet Prioritization
- IP-level Security
  - IPSec/VPN tunneling
  - Public Key Infrastructure (PKI) and associated infrastructure
  - Certificate Authority (CA)
- IP Header Compression

SN/ CxP Issues and Concerns (1 of 2)

Issue	Proposed Solution	Rationale
1. SN/ CxP Router Demarcation Point	CxP router will be physically located at JSC WSTF facility, interfacility cabling will be the responsibility of CxP.	The SN does not have control of interfacility links between WSTF and the SN (STGT, WSGT) terminals.
2. IP Header Compression	SN will not perform IP header compression, MPoFR will require some bit manipulation.	The SN is only responsible for layer 1, layer 2 protocol layers, IP routing and header compression are at layer 3 and above.
3. CCSDS AOS Encapsulation Service	This CCSDS Encapsulation Service will not effect lower level data (IP packets).	
4. The C3I specification calls out RFC 2507 and RFC 2508 for IP header compression. Are there any other relevant IETF RFCs ?		
5. CxP does not require SLE or AOS bitstream services	CCSDS AOS Encapsulation Service will be the only supported configuration for initial SN support of CxP services.	
6. SN will support RS/Convolutional codes for CxP emergency voice modes.	SN will support this mode (assuming CxP SNUG compliance) in addition to LDPC CxP support.	Necessary for emergency voice communication.

SN/ CxP Issues and Concerns (2 of 2)

Issue	Proposed Solution	Rationale
7. IP over CCSDS spacelink support of IPv4 .	If using IPv4 and the IP header is compressed, will use AOS encapsulation service. If IP header is not compressed, will use native IP service.	Would be provisioned in the SN USA CxP Gateway solution.
8. IP over CCSDS spacelink support of IPv6.	If using IPv6, AOS encapsulation is required.	Would be provisioned in the SN USA CxP Gateway solution.
9. CCSDS AOS Encapsulation service protocol handshake with the CEV	Being evaluated in ongoing CxP working group.	
10. CCSDS AOS Frame Length = 2048 bits (with LDPC) , AOS Frame Length = 1024 (w/o LDPC).	SN will support frame sized of 1024 and 2048 bits for CxP missions.	This can be accommodated in the SN USSR modem solutions. SN will need to know when LDPC is enabled/disabled only via a SHO (pre-pass support).
11. How will CxP manage router failovers ?	SN would recommend use of routers with automatic failover capability.	Best commercial practice within the networking community.
12. SN is responsible for providing clocking signals for the forward/ return data services	Support of MPoFR services requires different clock rates, these can be generated with the SN.	As long as the SN has knowledge of the frame lengths, derivation of these clock rates is relatively straightforward.

Section 6. USA Requirements Under Study

USA will continue to evolve as the rest of the SN evolves and these are some of the requirements that we are looking at:

Requirements will be levied and the design will follow.

1. Local Monitor and Control (tied to SN Modernization's broader SN Modernization Monitor and Control (EMC)(e.g. LMC with EMC details are unknown)
2. SN support of Lights Out Operations (for MOCs) – customer self service
3. Support of 1.2 Gbps service (per USSR implementation)
4. MDM Replacement
5. Operational Scenario for playback of CxP TDMs

Section 7
Requirements Management

Performance Verification Matrix (PVM)
Requirements Traceability and Verification Matrix (RTVM)
Development, Test, and Training (DT&T) Facility

Performance Verification Matrix (PVM)

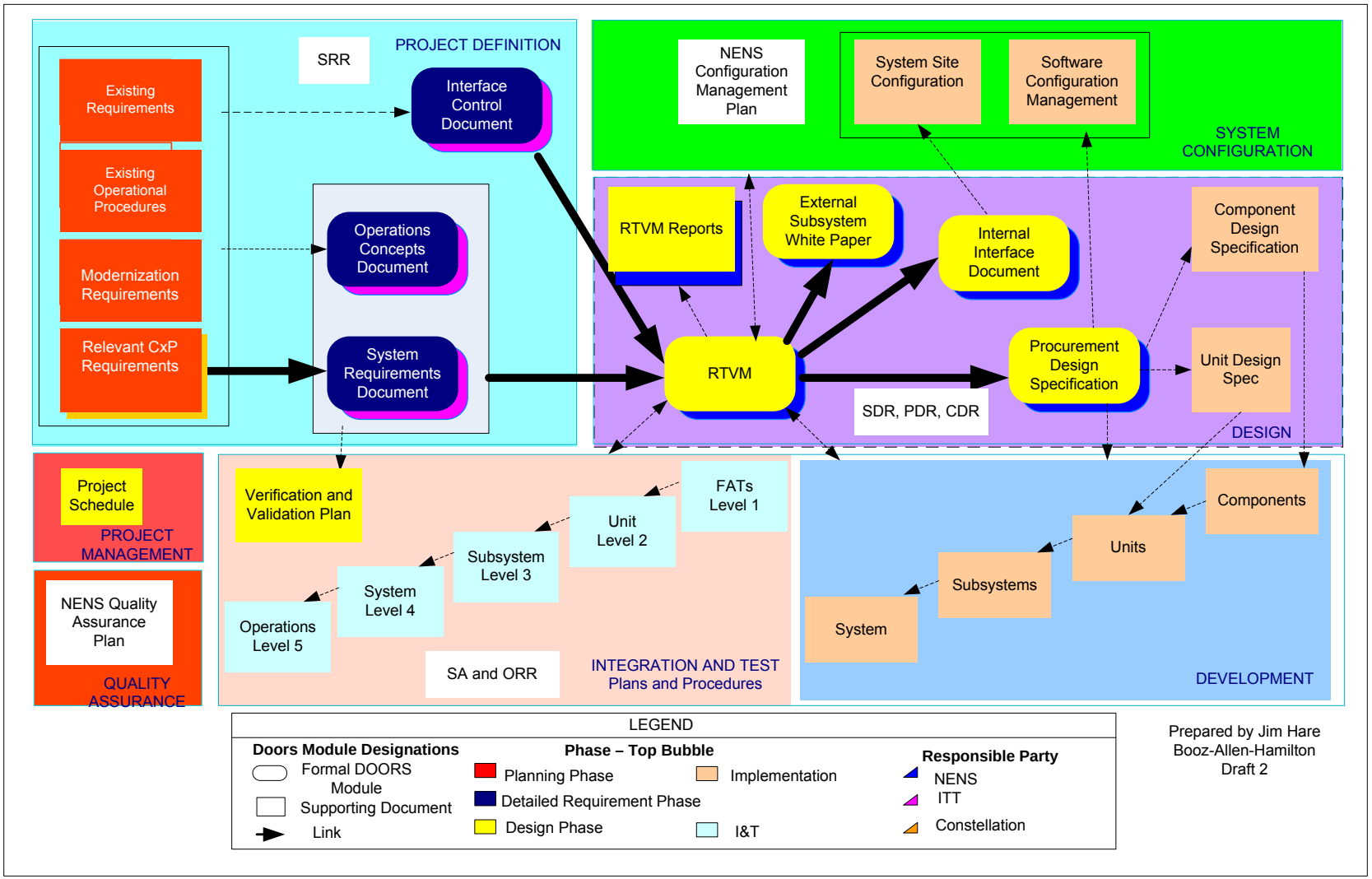
- Performance Verification Document has been populated with system level requirements.
- There are approximately 246 requirements at this time
- The PVM has been populated with the verification methods for these system level requirements
- Identified standard verification methods are:
  - Demonstration
  - Inspection
  - Analysis
  - Test
  - Combination of above (e.g., Demonstration/Inspection)
- Some system evel Requirements will be verified in the Development, Test, & Training (DT&T) facility at GSFC/Building 3/14

The USA Requirements Management (RM) Plan implemented with DOORS

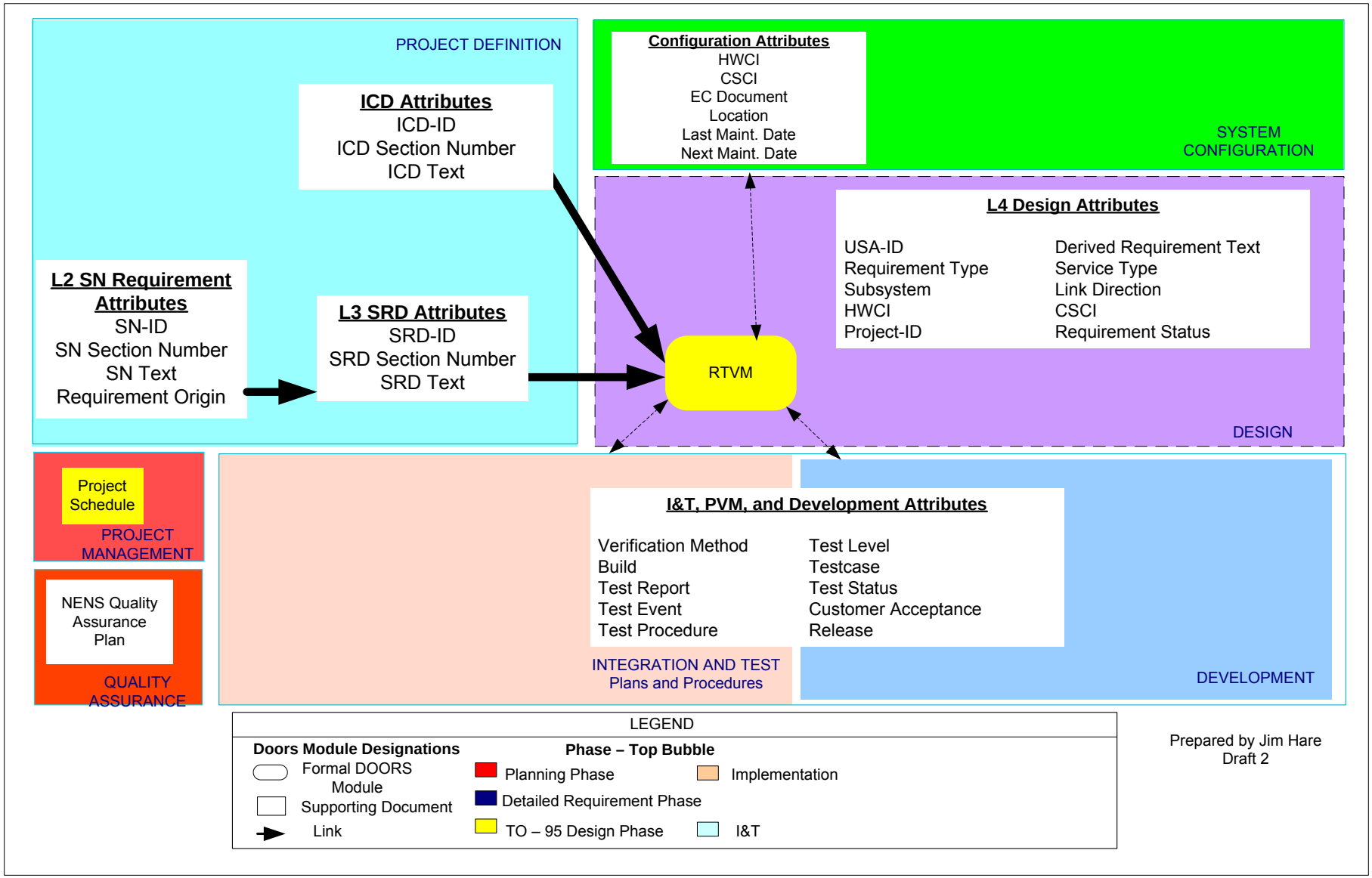
- Why the Dynamic Object Oriented Requirements System (DOORS)?
  - Maintain traceability of Stakeholders to the System Requirements Document (SRD), then down to the Requirements Traceability and Verification Matrix (RTVM) the Derived requirements and the Performance Verification Matrix.
  - Provides for an autonomous, unified approach for Modernization
  - Addresses the full project lifecycle of requirements management
  - Traceability to External ICDs (eg. USA and USSR)
- Perform change management for the baseline RTVM with Configuration Working Groups (CWGs)
  - History of changes maintained in DOORS
- Develop automated processes to produce project documentation
  - Report status metrics for requirements volatility, design maturity, and test verification.
  - Populate templates for procedure and test report documentation.
  - Produce requirements ‘shreds’ for custom views and documents

Draft USA Project Schema

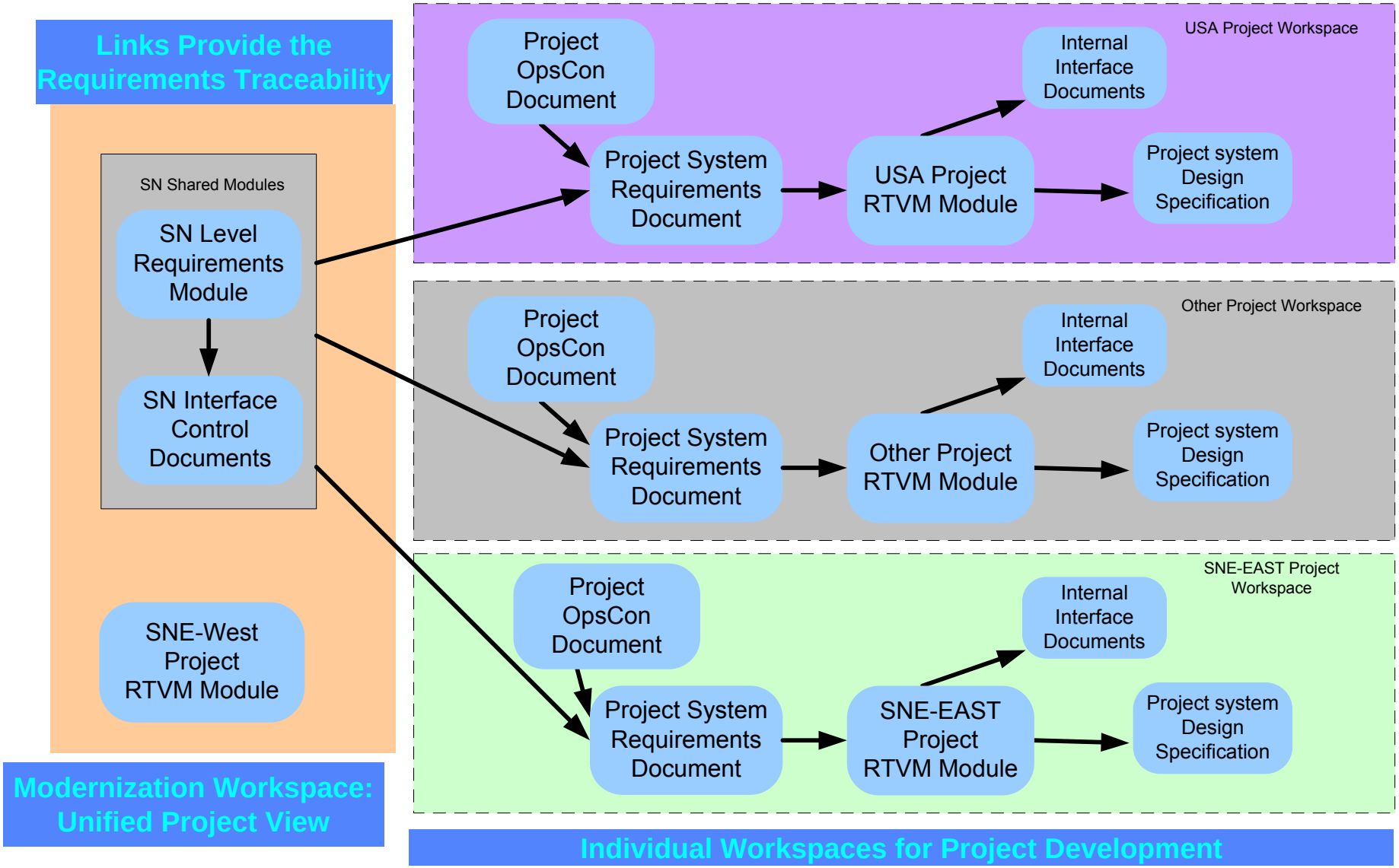
Improved USA Process: Based on SNE-W Lessons Learned



Key attributes linked across modules



Space Network Unified Project Approach



Development, Test, and Training (DT&T) Facility

Vision for the DT&T

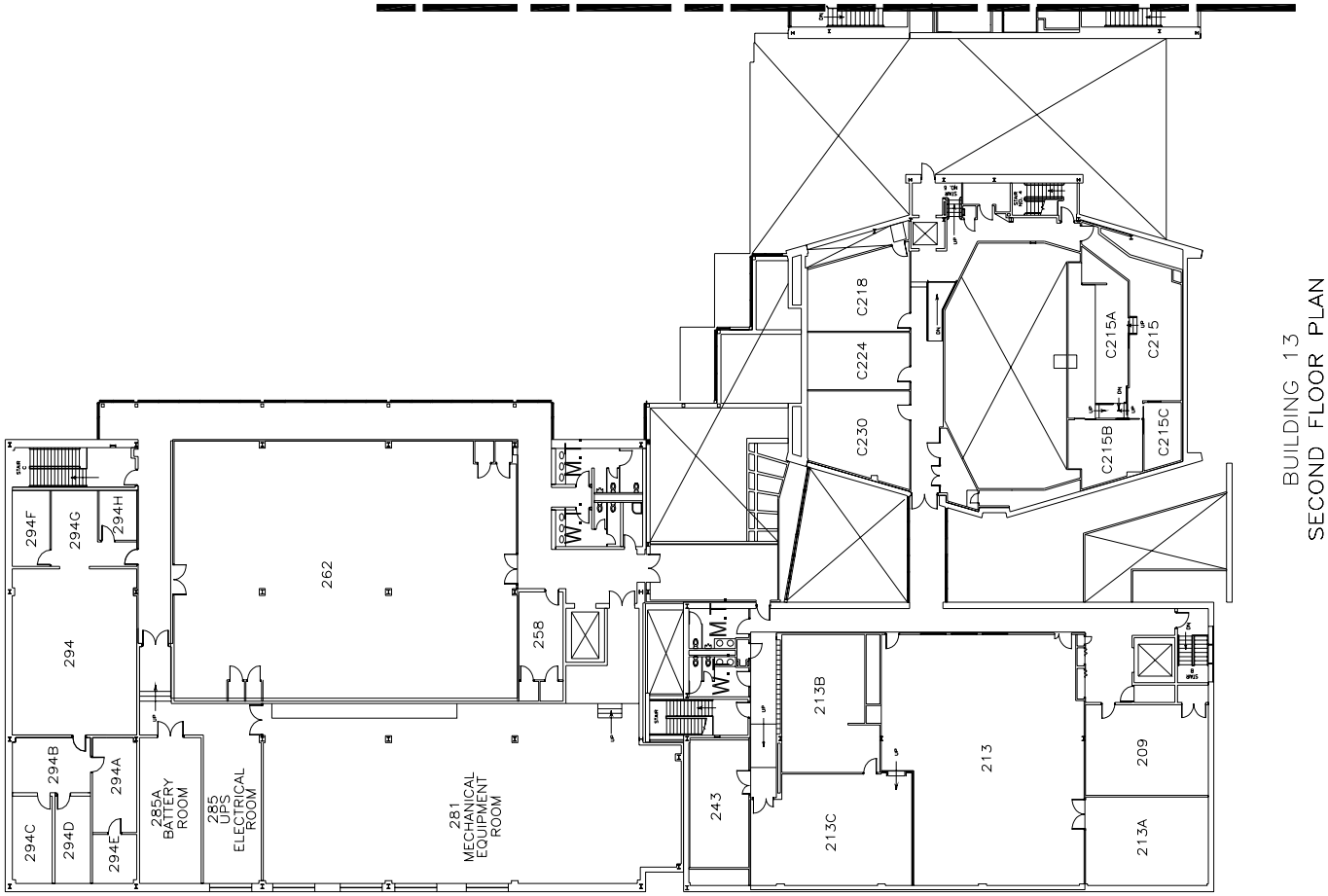
- The DT&T will be the primary facility for developing, testing, integrating and training for the capabilities associated with the USA, USSR and SN Modernization efforts.
- The DT&T alleviates the need for using constrained operational SN resources.
- The DT&T will be available throughout the life cycle of the USA, USSR and SN Modernization efforts.

DT&T Capabilities

- Development of new systems, network interfaces and resources.
- Testing:
  - **Verifies system integration.**
  - **Facilitates verification of requirements.**
- Training:
  - **Software and Sys Admin training for sustaining engineering.**
  - **Development of training materials.**
  - **Use for "Train the trainers" concept.**

DT&T Location

The facility will be located in Building 13 at GSFC. Room 262 will house the equipment racks and workstations with classroom space and a software development suite residing in Rooms 213, 213B and 213C.



Initial DT&T Concepts

- Suite of Test Equipment.
- Simulators.
- System Workstations.
- Interface with WSC.
- Fiber Optic interface to Building 25.

Planned NENS DT&T Formulation Activities

- NENS Deliverables under this task are:
  - **Operations Concept Document to show how the DT&T facility will be used throughout the life cycle.**
  - **Requirements Specification for the DT&T facility.**
  - **Develop cost estimate to establish the initial installation of the facility and for subsequent sustaining costs.**

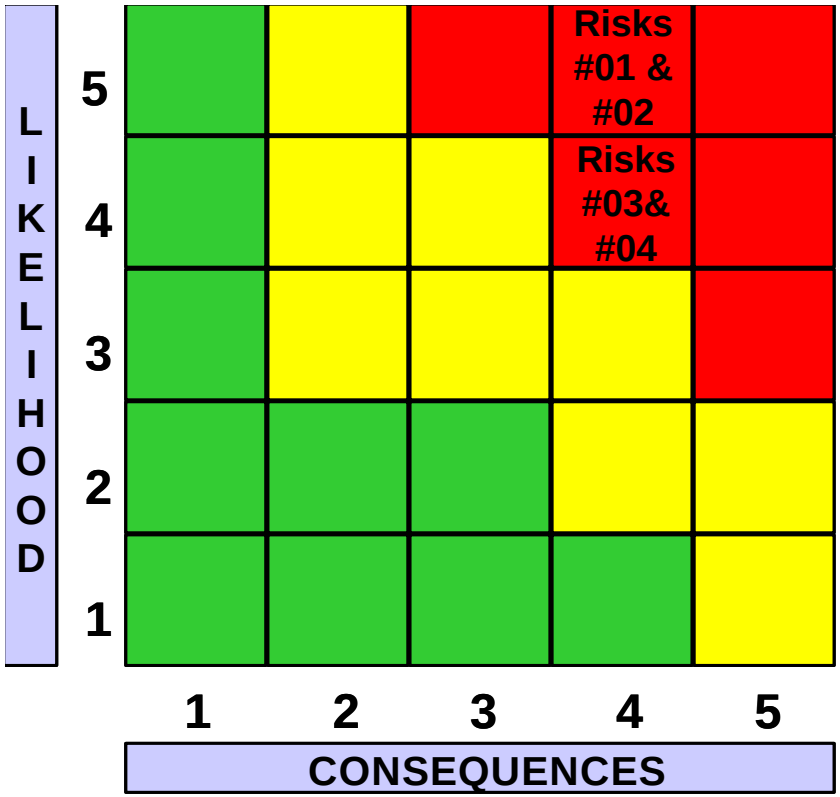
Section 8
Product Implementation

Risk Management
Detailed Schedule

USA Risk Management

- USA's risk management will be performed in accordance with:
  - NPR 7120.5C NASA Project Management Procedure Requirement
  - NPR 8000.4 NASA Risk Management Procedural Requirements
  - GPR 7120.4A Risk Management
- USA will conduct continuous risk management throughout its lifecycle to:
  - Enable early identification of potential problems and will continue with risk analysis, planning, tracking, and control.
  - Increase chances of USA success
  - Enable more efficient use of resources
  - Provide information tradeoffs based on priorities and quantified assessment
  - Provide information necessary for decision making
- Regular status meetings are used to manage risks
- Items resulting from reviews and that periodically merit attention will be added or deleted from the risk list as required.

USA Risks - Severity



5 - Very High

4 – High

3 – Moderate

2 – Low

1 – Very Low

Legend:

a. Red – Classified as High Risks.

b. Yellow – Classified as Medium Risks.

c. Green – Classified as Low Risks.

Risks & Mitigation

Criticality	LxC Trend	Risk ID	Approach	Risk Title
	➡	001	W	Constellation Requirements Volatility
	➡	002	A	SN Customer Impact
	➡	003	M	White Sands Software Modifications
	➡	004	M	USA Schedule Compression

Criticality	L x C Trend	Approach
High	⬇ Decreasing (Improving)	M – Mitigate
Med	⬆ Increasing (Worsening)	W – Watch
Low	➡ Unchanged	A – Accept
	*New since last month	R – Research

Risks & Mitigation

Risk # 001 – Constellation Requirements Volatility

- Risk: Given that many of the USA functions are tailored to the Constellation requirements and that Constellation's requirements are still changing there may be requested modifications to the system after System Requirements Review (SRR) and possibly continuing for some time exists.
- **Likelihood:** 5 **Consequence:** 5
- **Approach & Plan:**
  - Conduct SRR to baseline known requirements
  - Drive CxP requirements stability by identifying SN's planned solution and by working with CxP during the RFA Process
  - Implement Requirements Management Process to manage implementation of evolving requirements
- **Status:**
  - SRR is being conducted on May 12, 2008
  - Requirements management process, tool and database structure defined
- **Control:** YELLOW
  - Plan identified and will be implemented. However, current state of Constellation requirements indicate they may evolve for some time.

Risks & Mitigation

Risk # 002 – SN Customer Impact

- Risk: The USA must be integrated into an already operational, complex, data services point in the WSC infrastructure. If the USA is not designed and integrated properly, service to current SN customers may be impacted.
- **Likelihood:** 5 **Consequence:** 5
- **Approach & Plan:**
  - Conduct a study to examine and document strategies for the deployment of USA and USSR within the ground station.
  - Conduct System Definition Review (SDR) early in the design process to assess the impact of USA implementation on current SN customers
  - Implement a Design, Test & Training (DT&T) facility to test the impact of USA implementation on current SN customers
- **Status:**
  - NENS is under task to perform the USA/USSR deployment strategy study
  - NENS is under task to develop a DT&T facility design
  - SDR is scheduled for September 2008
- **Control:** YELLOW
  - Plan identified and will be implemented. However, the complexity of incorporating USA & USSR into the SN along with TDRS K & L satellite implementation is unknown at this time

Risks & Mitigation

Risk # 003 – White Sands Software Modifications

- Risk: The USA Monitor & Control (M&C) function requires the modification of relatively old, large and complex software systems. While these applications are known by the White Sands personnel, modifying them may introduce defects, especially latent defects that might be found only during operations. Modifying this software may also impact the operations of current users.
- **Likelihood:** 4 **Consequence:** 4
- **Approach & Plan:**
  - Begin the USA Monitor and Control design immediately after SRR and the baseline of requirements. Begin Software modifications early in the USA implementation phase
  - Implement a Design, Test & Training (DT&T) facility to thoroughly test the USA Monitor & Control software changes.
- **Status:**
  - NENS is under task to identify White Sands software changes necessary to accommodate USA IOC and USSR modifications
  - NENS is under task to develop DT&T specifications to accommodate the modification and testing of White Sands software modifications.
- **Control:** YELLOW
  - Plan identified and will be implemented. However the modification of legacy software normally involves unknowns.

Risks & Mitigation

Risk # 004 – USA Schedule Compression

- Risk: The USA implementation schedule is extremely tight, i.e., there is only 3.5 years to design, integrate and test the system in order to support the Orion 1 manned launch in March 2013. Per Boehm, a project cannot reduce its schedule more than 75% by adding more personnel, equipment, etc. If the USA schedule is compressed too severely, the USA system cannot be adequately tested and integrated into the White Sands Ground Station thus potentially impacting current users and not adequately supporting the Orion 1 manned Launch.
- **Likelihood:** 4 **Consequence:** 4
- **Approach & Plan:**
  - Preserve as much design, development and integration and testing schedule as possible by:
    - Conducting the SRR to baseline known requirements
    - Driving CxP requirements stability by identifying SN's planned solution and by working with CxP to build consensus on the implementation
    - Implementing a Requirements Management Process to manage requirements creep
    - Conducting USA design, development, integration & testing in an evolutionary manner.
  - **Status:**
  - SRR is being conducted on May 12, 2008
  - Requirements management process, tool and database structure defined
- **Control:** YELLOW
  - Plan identified and is being implemented. However, current state of Constellation requirements indicate they may evolve for some time and may have an unknown impact on the USA schedule.

Section 8. Schedule

System Requirements Review	May 12, ’08
RFA Submission	SRR date + 1 day
RFA Proposed Resolution Provided	SRR date + 2 weeks
RFA Originator Acceptance or alternate solution	SRR date + 4 weeks
Documentation update & review	SRR date + 7 weeks
Documentation CCB’s	July 7, ‘08
Preliminary Design Phase	April ’08 to October ’08
System Definition Review (SDR)	September 4, ‘08
Preliminary Design Review (PDR)	April 1, ‘09
Critical Design Review (CDR)	September 1, ’09
Test Readiness Review (TRR)	September 1, ‘11
Operations Readiness Review (ORR)	October 31, ’12

Section 9
Closing Remarks

Frank Herman

Summary and Closing Remarks

Today we have:

- Presented the USA System Requirements
- Presented USA Operational Scenarios
- Presented the USA Overall Schedule

Next Steps:

- Address RFAs
- Develop consensus on CxP Issues/Concerns
- Resolve requirements needing additional study
- Finalize documentation
- Proceed to Design phase with Review Board approval

Backup Material

SRD Appendix A –Baseline, Cx, Supplementary

USA Requirements Traceability
(SRD Appendix A)

The USA requirements are allocated under the following three categories:

B – USA baseline requirement
C – Constellation Program requirement
S – USA supplemental requirement

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.1.1.a	The USA shall support TDRSS KaSA Forward (KaSAF) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.b	The USA shall support TDRSS KaSA Return (KaSAR) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.c	The USA shall support TDRSS KuSA Forward (KuSAF) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.d	The USA shall support TDRSS KuSA Return (KuSAR) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.e	The USA shall support TDRSS SSA Forward (SSAF) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.f	The USA shall support TDRSS SSA Return (SSAR) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.g	The USA shall support TDRSS MA Forward (MAF) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.h	The USA shall support scheduled TDRSS MA Return (MAR) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.1.1.i	The USA shall support TDRSS SMA Forward (SMAF) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.j	The USA shall support TDRSS SMA Return (SMAR) data services.	B	USA, as an SN expansion capability, is required to support all existing services and those services that are currently in planning/implementation phases.
4.1.1.k	The USA shall support TDRSS Demand Access System (DAS) data services.	S	Supplemental capability to expand DAS service capabilities
4.1.1.l	The USA shall support a minimum of 12 **(TBR)** simultaneous TDRSS forward services.	B, C	Minimum number of forward services to support three Cx vehicles simultaneously (6 active channels comprising of 3 SSAF, 1 KuSAF, 2 KaSAF, and 6 standby channels for handover) per Cx-SCAN IRD Vol.1
4.1.1.m	The USA shall support a minimum of 12 **(TBR)** simultaneous TDRSS return services.	B, C	Minimum number of return services to support three Cx vehicles simultaneously (6 active channels comprising of 3 SSAR, 1 KuSAR, 2 KaSAR, and 6 standby channels for handover) per Cx-SCAN IRD Vol.1
4.1.1.n	The USA shall use Coordinated Universal Time (UTC) for all parameters containing a time value.	B	Complies with current WSC requirement in 530-RSD-WSC
4.1.1.o	The USA shall support the Internet Protocol Version 4 (IPv4)	B, C	Requirement to support Cx per Cx-SCAN IRD Vol.1 and other customers using IPv4 data access and data transport services. IPv$ described in ***RFC 791*** *Internet Protocol.*
4.1.1.p	The USA shall support the Internet Protocol Version 6 (IPv6)	B	IPv6 described in ***RFC 2460*** *Internet Protocol, Version 6 (IPv6) Specification.* Internet migration to IPv6 is in process and the requirement accommodates customers needing IPv6 data access and transport services
4.1.1.q	The USA shall provide the capability for remote operation of all USA functions.	B	Requirement to provide added operational flexibility.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.1.1.r	The USA shall deliver all Constellation Customer data products directly to the Constellation router.	C	Satisfy data delivery requirements in Cx-SCAN IRD Vol. 6
4.1.2.a	The USA shall support all TDRSS Forward Service data rates less than or equal to 6 **(TBR)** Mbps.	C	Forward service data rate per high-rate SN forward link specified in Cx-SCAN IRD Vol. 1,2
4.1.2.b	The USA shall support all TDRSS Return Service data rates less than or equal to **25 (TBR)** Mbps.	C	Return service data rate per high-rate SN return link specified in Cx-SCAN IRD Vol. 1,2
4.1.2.c	The USA shall deliver an average bit error probability less than one error in 1012 bits over any 24-hour period at any data rate on a digital connection through the Data Interface System (DIS), including the Guam Data Interface System (GDIS), between the input from the USSR and output to the NISN/Constellation or Local data interface and vice versa.	B	As a minimum, USA is required to meet the existing data quality performance requirements per 530-RSD-WSC.
4.1.2.d	The USA shall be capable of being automatically configured for customer support in no more than 35 seconds prior to start of service in conformance with present WSC hardware specifications.	B	Complies with the current data service capability per 530-RSD-WSC.
4.1.2.e	The USA shall execute changes to pre-established reconfigurable service parameters in response to customer requests within 35 seconds.	B	Complies with the current data service capability per 530-RSD-WSC.
4.1.3.a	The USA shall provide for modular expandability up to a maximum of 46 **(TBR)** simultaneous Return Service links.	S	Based on NENS Table of SN Services (SGLT-1: 9, SGLT-2: 9, SGLT-3: 4, SGLT-4: 9, SGLT-5: 9, SGLT-6: 6)

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.1.3.b	The USA shall provide for modular expandability up to a maximum of 29 **(TBR)** simultaneous Forward Service links.	S	Based on NENS Table of SN Services (SGLT-1: 5, SGLT-2: 5, SGLT-3: 4, SGLT-4: 5, SGLT-5: 5, SGLT-6: 5)
4.1.3.c	The USA shall provide for modular expandability up to a maximum of 14 (TBR) DAS links.	S	Commensurate with the current DAS support (8 at WSC and 6 at GRGT)
4.1.3.d	The USA shall provide for modular expandability to accommodate the maximum data rates specified in the Space Network Users Guide, which are reproduced in Appendix B.3 of this document.	S	Initial USA design need to address future expansion based on the full complement of SN data service capabilities.
4.1.4.a	The USA shall log the following for all functional components: Startup and Shutdown.	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.b	The USA shall log the following for all functional components: Authentication	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.c	The USA shall log the following for all functional components: Authorization/permission granting,	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.d	The USA shall log the following for all functional components: Action by trusted users,	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.e	The USA shall log the following for all functional components: Process invocation,	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.f	The USA shall log the following for all functional components: Unsuccessful data access attempts (threshold = log on five unsuccessful attempts),	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.1.4.g	The USA shall log the following for all functional components: Data deletion,	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.h	The USA shall log the following for all functional components: Data transfer,	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.i	The USA shall log the following for all functional components: Configuration change,	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.j	The USA shall log the following for all functional components: Application of confidentiality or	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.k	The USA shall log the following for all functional components: Override or modification of data labels or markings	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.l	The USA shall log the following for all functional components: Output to removable media,	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.m	The USA shall log the following for all functional components: Output to a printer	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.1.4.n	Log records shall contain the following fields as a minimum: source, severity, timestamp, USA identifier of the person instigating the event or the person in control of the system, text field with the event data or description.	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.o	The USA log files shall be maintained on a central log server.	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.p	The USA shall provide an audit trail in compliance with NPR 2810.1A, Section 21.2, Audit Trail and Accountability Requirements.	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.q	Operations and Maintenance logs shall be archived to protected files in support of audit requirements.	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.r	Access to protected audit files shall be limited to the System Administrator (SA) and the Information System Security Officer (ISSO).	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.1.4.s	The capability to manage protected audit files shall be limited to the SA and the ISSO.	B	Complies with NPR 2810.1A, NIST SP 800-92, NIST SP 800-31, and NIST SP 800-53
4.2.1.a	The USA Switching function shall provide schedulable data paths between external interfaces requiring synchronous serial data and the USSR.	B	Support for customer unique equipment through local interface.
4.2.1.b	The USA Switching function shall provide schedulable data paths between the NISN/Constellation routers and the USA Gateway.	B	USA Gateway provides support for data services requiring link layer processing such as CCSDS ENCAP specified in Cx-SCAN IRD Vol. 1,2
4.2.1.c	The USA Switching function shall transport TDRSS DAS return data to the NISN/Constellation routers.	S	Supplemental requirement to support future expansion of the DAS service.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.2.1.d	The USA Switching function shall transport a single customer's forward data and return data on the same NISN/Constellation router interface.	B	Requirement to minimize interface connections and to provide more efficient link layer processing.
4.2.1.e	The USA Switching function shall configure the forward and return data paths based on commands received from the USA Monitor and Control function.	B	USA and USSR equipment configuration and monitoring are performed by the USA M&C. USSR equipment configuration to satisfies backward compatibility for WDISC service
4.2.1.f	The USA Switching function shall ensure complete separation and isolation between NISN data networks such as NISN Closed IONet, NISN Restricted IONet, and the Constellation network.	B	Network security mandates the isolation of external networks connecting to the SN from each other. The USA switch is the most logical place where the network isolation strategies can be implemented.
4.2.2.a	The USA Switching function shall transport all TDRSS forward and return service data streams at data rates less than or equal to 25 **(TBR)** Mbps.	C	The USA switch must support the maximum Cx return service data rate specified in Cx-SCAN IRD Vol. 1,2
4.2.2.b	The configuration time for the USA switching function shall be less than or equal to 5 seconds in conformance with present WSC hardware specifications.	B	Complies with the current data service capability of the WSC.
4.2.2.c	The USA Switching function shall provide its current Status and Health data to the USA Monitor and Control function every 5 seconds in accordance with present WSC hardware specifications.	B	Complies with current WSC requirement in 530-RSD-WSC
4.3.1.a	All USA Gateway functions shall be capable of being individually and selectively configurable.	B	The USA Gateway is a multi functional concept and its hardware manifestation needs to be configured according to customer data service requirements

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.3.1.b	The USA Gateway function shall automatically configure the individual processing functions based on commands received from the USA Monitor and Control function.	B	USA and USSR equipment configuration and monitoring are performed by the USA M&C.
4.3.1.c	The Gateway function shall provide a Point-to-Point Protocol interface, as specified in RFC-1661 The Point-to-Point Protocol (PPP), to the NISN/Constellation routers.	C	Cx services require IP header compression. PPP can support IP header compression as required in Cx C3I Interoperability Specification Vol. 1, 2
4.3.1.d	The Gateway function shall provide a Frame Relay interface, as specified in RFC-2427 Multiprotocol Interconnect over Frame Relay (MPoFR), to the NISN/Constellation routers.	C, S	Frame relay interface to provide additional flexibility in supporting future customers requiring frame relay based IP services as well as IP header compression per x C3I Interoperability Specification Vol. 1, 2.
4.3.1.e	The USA Gateway function shall provide backward compatibility with the WDISC function specified in WDISC System Requirements document (CSOC-GSFC-RD-002090).	B	The USA Gateway will replace the existing WDISC function. WDISC customers are not expected to modify their equipment/software to connect to the USA Gateway.
4.3.1.f	The USA Gateway function shall implement the SLE Forward Command Link Transfer Unit (FCLTU) service per CCSDS Recommendation 912.2-B-2.	S	SLE is an interoperable standard that help customers to consolidate their data operations through different service providers.
4.3.1.g	The USA Gateway function shall implement the SLE Return All Frames (RAF) Service per CCSDS Recommendation 911.1-B-2.	S	SLE is an interoperable standard that help customers to consolidate their data operations through different service providers.
4.3.1.h	The USA Gateway function shall implement the SLE Return Channel Frames (RCF) Service per CCSDS Recommendation 911.2-B-1.	S	SLE is an interoperable standard that help customers to consolidate their data operations through different service providers.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.3.1.i	The USA Gateway function shall have a client/server relationship with the customer MOC.	B	Requirement to support WDISC and SLE services where TCP/IP connectivity between MOC and USA gateway is required.
4.3.1.j	The USA Gateway function shall act as either the client or the server in the client/server relationship.	B	Requirement to support WDISC and SLE services where TCP/IP connectivity between MOC and USA gateway is required.
4.3.1.k	The USA Gateway function shall implement access control based on the identity of the initiator and the responder. The roles of initiator and responder are played by both the USA Gateway and a remote MOC or user.	B	Requirement to support WDISC and SLE services where TCP/IP connectivity between MOC and USA gateway is required.
4.3.1.l	The USA Gateway function shall implement authentication for invocation of all data transfer services.	B	Requirement to support WDISC and SLE services where TCP/IP connectivity between MOC and USA gateway is required.
4.3.2.a	Prior to scheduling the Gateway function to support a forward service, a forward data channel processing specification as specified in 452-OCD-USA Space Network User Service Access Operations Concept Document shall be defined.	B	Requirement to support WDISC services, and depending on the implementation, possibly SLE services.
4.3.2.b	The forward service data channel processing specification shall include data processing requirements, link layer specification, and a valid MOC IP address.	B	Requirement to support WDISC services, and depending on the implementation, possibly SLE services.
4.3.2.c	Prior to the scheduled service start time, a forward data channel processing specification shall be activated.	B	Requirement to support WDISC services, and depending on the implementation, possibly SLE services.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.3.2.d	If indicated by the active forward service data channel processing specification, the Gateway function shall initiate a TCP/IP connection with the customer MOC.	B	Requirement to support WDISC and SLE functions.
4.3.2.e	If indicated by the active forward service data channel processing specification, the Gateway function shall accept forward data flow configuration control information from the customer MOC.	B	Requirement to support WDISC and SLE.
4.3.2.f	The USA Gateway function shall receive forward packet data from the USA Switch function using the link layer protocol specified in the forward service data channel processing specification. The forward service data can be IP packets destined to customer platforms, 4800 bit blocks, or customer data encapsulated in IP packets.	B, C	Requirement to support WDISC, SLE, and CCSDS ENCAP specified in Cx-SCAN IRD Vol. 1,2
4.3.2.g	If indicated by the active forward service data channel processing specification, the USA Gateway function shall transfer IP packets using the CCSDS encapsulation (CCSDS ENCAP) service over AOS Virtual Channel Packets VCP) as specified in ***CCSDS 702.1-R-2*** *IP Over CCSDS Space Links*	C	Requirement per Cx-SCAN IRD Vol. 1,2,

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.3.2.h	If indicated by the active forward service data channel processing specification, the USA Gateway function shall perform link layer protocol translation between PPP/MPoFR and CCSDS ENCAP to support IP header compression as specified in RFC 2507 IP Header Compression and RFC 2508 Compressing P/UDP/RTP Headers for Low-Speed Serial Links.	C	As specified in Cx-SCAN IRD Vol. 1,2, IP header compression is required by Cx. IP header compression depends on the link layer protocol. The link layer protocol used by the Cx router is not transparent over the space link and hence requires adaptation.
4.3.2.i	If indicated by the active forward service data channel processing specification, the USA Gateway function shall encapsulate forward service data inside CCSDS AOS frames as specified in the CCSDS 701.0-B-3 Advanced Orbiting Systems, Networks and Data Links: Architectural Specification at the request of the customer.	B, C	Support for CCSDS AOS framing required by Cx, SLE, and other customers using CCSDS protocols.
4.3.2.j	The Gateway function shall perform idle pattern generation according to the forward service data channel processing specification.	B, C	Idle pattern generation to fill gaps between IP packets and other packet data services.
4.3.2.k	The USA Gateway function shall present the forward service data to the USSR as a synchronous serial bit stream.	B	USA/USSR interface requirement.
4.3.2.l	If indicated by the active forward service data channel processing specification, the Gateway function shall provide periodic system status information to the customer MOC.	S	SLE requirement.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.3.3.a	Prior to scheduling the Gateway function to support a return service, one or more return data channel processing specifications must be defined.	B	Requirement to support WDISC services, and depending on the implementation, possibly SLE services.
4.3.3.b	The return service data channel processing specification shall include data processing requirements, data monitoring requirements, data recording requirements, link layer specification, and a valid MOC IP address.	B	Requirement to support WDISC services, and depending on the implementation, possibly SLE services.
4.3.3.c	Prior to the scheduled service start time, a return data channel processing specification shall be activated.	B	Requirement to support WDISC services, and depending on the implementation, possibly SLE services.
4.3.3.d	If indicated by the active return service data channel processing specification, the Gateway function shall establish a TCP/IP connection request to the MOC server.	B	Requirement to support WDISC and SLE services.
4.3.3.e	The USA Gateway function shall receive return service data from the USSR as a synchronous serial bit stream.	B	USA/USSR interface requirement
4.3.3.f	For each active return data channel processing specification, the Gateway function shall convert the CCSDS compliant return service data from serial form to encapsulated form.	B	Requirement to support WDISC and SLE services

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.3.3.g	If indicated by the active return service data channel processing specification, the USA Gateway function shall extract data packets encapsulated inside CCSDS AOS frames as specified in the ***CCSDS 701.0-B-3*** *Advanced Orbiting Systems, Networks and Data Links: Architectural Specification* at the request of the customer.	B, C	Support for CCSDS AOS framing required by Cx, SLE, and other CCSDS protocol customers (as specified in Cx-SCAN IRD Vol. 1,2,2)
4.3.3.h	If indicated by the active return service data channel processing specification, the USA Gateway function shall extract IP data packets encapsulated inside CCSDS AOS VCP/ENCAP frames as ***specified in*** *CCSDS 702.1-R-2 IP Over CCSDS* Space Links at the request of the customer.	C	Cx requires the use of CCSDS IP encapsulation service as specified in Cx-SCAN IRD Vol. 1,2.
4.3.3.i	If indicated by the active return service data channel processing specification, the USA Gateway function shall perform link layer protocol translation between CCSDS ENCAP and PPP/MPoFR to support IP header compression as specified in ***RFC 2507*** *IP Header Compression* and ***RFC 2508*** *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links.*	C	Requirement to support IP header compression per Cx-SCAN IRD Vol. 1,2.
4.3.3.j	If indicated by the active return service data channel processing specification, the Gateway function shall perform time tagging of data frames with an accuracy of at least 10 ms	B	Requirement to support WDISC and SLE services

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.3.3.k	If indicated by the active return service data channel processing specification, the Gateway function shall:	B	Requirement to support WDISC and SLE services
4.3.3.l	The USA Gateway function shall forward the return service data packets to the NISN/Constellation Routers using the link layer protocol identified in the return service data channel processing specification.	B, C	Requirement to support WDISC, SLE, and as required by the Cx C3I specification and the Cx-SCAN IRD Vol. 1,2
4.3.3.m	The USA Gateway function shall provide the return service data streams to the USA return service recorders.	B	Line outage recording is required on all return data services as a protection against terrestrial network failures. The USA Gateway is the data source delivering the data to the terrestrial network interface.
4.3.4.a	The USA Gateway function shall support all TDRSS Forward service data rates less than or equal to 6 (TBR) Mbps.	C	Supports Cx maximum forward data rate as specified in Cx-SCAN IRD Vol. 1,2
4.3.4.b	The USA Gateway function shall support all TDRSS Return service data rates less than or equal to 25 **(TBR)** Mbps.	C	Supports Cx maximum return data rate as specified in Cx-SCAN IRD Vol. 1,2
4.3.4.c	The USA Gateway function shall provide its current Status and Health data to the USA Monitor and Control function every 5 seconds.	B	Complies with current WSC requirement in 530-RSD-WSC
4.4.1.a	All USA Monitor and Control functions shall be capable of being scheduled, controlled, and monitored through the DIS ADPE or its equivalent.	B	Complies with the current WSC operational requirements.
4.4.1.b	All USA DAS related functions shall be capable of being scheduled, controlled, and monitored through the DASCON.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.4.1.c	The USA Monitor and Control function shall use an open-standards-based architecture built on IP technology.	B	Open-standards-based architecture built on IP technology will reduce the risks associated with M&C system maintenance and upgrade.
4.4.2.a	The USA Monitor and Control function shall indicate via an operator alert when abnormalities are detected in USA operations and/or resources.	B	Complies with the current WSC operational requirements.
4.4.2.b	The USA Monitor and Control function shall indicate via an operator alert when abnormalities are detected in USSR operations and/or resources.	B	Complies with the current WSC operational requirements.
4.4.2.c	The USA Monitor and Control function shall accept customer set(s) of USA resource configuration parameters.	B	Complies with the current WSC operational requirements.
4.4.2.d	The USA Monitor and Control function shall accept updates to existing sets of customer USA reconfigurable parameters.	B	Complies with the current WSC operational requirements.
4.4.2.e	The USA Monitor and Control function shall configure the USSR resources based on the accepted set(s) of resource configuration parameters.	B	Complies with the current WSC operational requirements.
4.4.2.f	The USA Monitor and Control function shall accept updates to existing sets of customer USSR reconfigurable parameters.	B	Complies with the current WSC operational requirements.
4.4.2.g	The USA Monitor and Control function shall collect and log status of each scheduled event.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.4.2.h	The USA Monitor and Control function shall collect and log status on each customer's allocated network interface.	B	Complies with the current WSC operational requirements.
4.4.2.i	The USA Monitor and Control function shall generate USA resource allocation status reports.	B	Complies with the current WSC operational requirements.
4.4.2.j	The USA Monitor and Control function shall collect and log status on each customer's allocated USSR resources.	B	Complies with the current WSC operational requirements.
4.4.2.k	The USA Monitor and Control function shall generate USSR resource allocation status reports.	B	Complies with the current WSC operational requirements.
4.4.2.l	The USA Monitor and Control function shall receive Customer Tracking Data from the USSR.	C, S	Requirement to support CxP 70118-6 requirement on TDM delivery
4.4.2.m	The USA Monitor and Control function shall format Customer Tracking Data into Tracking Data Messages (TDM) using the TDRSS Universal Tracking Data Format (UTDF)	C, S	Tacking data message format per 452-ICD-SN/FDF, 530-ICD-NCC-FDF/WSC
4.4.2.n	The USA Monitor and Control function shall log the Customer TDMs.	C, S	Requirement to support CxP 70118-6 requirement on TDM delivery
4.4.2.o	The USA Monitor and Control function shall time-tag all logged items.	B	Complies with the current WSC operational requirements.
4.4.2.p	The USA Monitor and Control function shall provide the capability for operators to selectively extract logged data.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.4.2.q	The USA Monitor and Control function shall provide the capability for operators to archive all of the logged data items to removable media.	B	Complies with the current WSC operational requirements.
4.4.2.r	The USA Monitor and Control function shall enable operators to View logged data on workstation display screens.	B	Complies with the current WSC operational requirements.
4.4.2.s	The USA Monitor and Control function shall enable operators to Print-out hard copies of logged data.	B	Complies with the current WSC operational requirements.
4.4.3.a	The USA functions shall be allocated and configured to support a service request such that the reaction time does not exceed the allocation of service response times specified in 530-RSD-WSC Requirements Specification for the White Sands Complex.	B	Complies with the current WSC operational requirements.
4.4.3.b	The USA Monitor and Control function shall reject Resource Allocation modifications within one minute prior to the time that the service is terminated.	B	Complies with the current WSC operational requirements.
4.4.3.c	The USA Monitor and Control function shall automatically log Resource Allocation and Configuration status at one minute intervals.	B	Complies with the current WSC operational requirements.
4.4.3.d	The USA Monitor and Control function shall log performance status of all components that constitute the USA once per second.	B	Complies with the current WSC operational requirements.
4.4.3.e	The USA Monitor and Control function shall log performance status of all components that constitute the USSR once per second.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.4.3.f	The USA Monitor and Control function shall provide the monitor and control parameters through existing planning and scheduling and real-time messages, as defined in 452-ICD-SN/CSM, Interface Control Document between the Space Network and Customers for Service Management or in 452-ICD-DAS/SNAS, Interface Control Document between DAS and the Space Network Access System (SNAS).	B	Complies with the current WSC operational requirements.
4.4.3.g	The USA Monitor and Control function shall provide performance status data to the NCCDS at 5 second intervals starting at the commencement of service.	B	Complies with the current WSC operational requirements.
4.4.3.h	The USA Monitor and Control function shall send the Constellation Customer TDMs to the Constellation router at least every 10 (TBR) seconds.	C, S	Requirement to support CxP 70118-6 requirement on TDM delivery
4.4.3.i	The USA Monitor and Control function shall send the recorded Constellation Customer TDMs to the Constellation router within 1 (TBR) hours of receipt of a valid request.	C, S	Requirement to support CxP 70118-6 requirement on TDM delivery
4.4.3.j	The USA Monitor and Control function shall retain system status log data for at least one (1) year.	B	Complies with the current WSC operational requirements.
4.5.1.a	All USA Return Service Recording functions shall be capable of being individually and selectively configurable.	B	The USA Return Service Recording is a multi functional concept and its hardware manifestation needs to be configured according to customer data service requirements

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.5.1.b	The USA Return Service Recording function shall automatically configure the individual data recording functions based on commands received from the USA Monitor and Control function.	B	USA equipment configuration and monitoring are performed by the USA M&C.
4.5.2.a	The USA Return Service Recording function shall receive the S-band Single Access (SSA) return service channel from the USSR at an Intermediate Frequency	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)
4.5.2.b	The USA Return Service Recording function shall sample the SSA return service IF channel over a bandwidth of TBD MHz	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)
4.5.2.c	The USA Return Service Recording function shall receive the K-band Single Access (KSA) return service channel from the USSR at an Intermediate Frequency of TBD MHz:	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)
4.5.2.d	The USA Return Service Recording function shall sample the KSA return service IF channel over a bandwidth of TBD MHz	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)
4.5.2.e	The USA Return Service Recording function shall perform analog-to-digital conversion of the IF samples with a minimum bit resolution of 14 (TBR) bits.	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)
4.5.2.f	The USA Return Service Recording function shall record IF return service samples in terms of identifiable, time tagged data blocks with a not to exceed length of 3 (TBR) hours.	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.5.2.g	The USA Return Service Recording function shall retain each recoded IF data block for a minimum period of 2 (TBR) hours before discarding or over-writing the data block.	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)
4.5.2.h	Upon request, the USA Return Service Recording function shall provide a copy of the IF recording of the customer's return service IF channel on physical recording media.	C	IF data recording is required for Cx missions that are considered critical (specified in Cx-SCAN IRD Vol. 1,2)
4.5.2.i	The USA Return Service Recording function shall receive customer return service data frames from the USA Gateway function.	B	The USA return service LOR will perform a function similar to that of the existing WSC LOR. However, recording of individual return services (instead of the existing LOR for multiplexed return services) must be performed.
4.5.2.j	The USA Return Service Recording function shall record the customer return service data frames received from the Gateway in terms of identifiable, time tagged data files, which are collectively termed as Line Outage Recording (LOR).	B	The USA return service LOR will perform a function similar to that of the existing WSC LOR. However, recording of individual return services (instead of the existing LOR for multiplexed return services) must be performed.
4.5.2.k	The USA Return Service Recording function shall retain each LOR data file for a minimum period of 7 days.	B	The USA return service LOR will perform a function similar to that of the existing WSC LOR. However, recording of individual return services (instead of the existing LOR for multiplexed return services) must be performed.
4.5.2.l	The USA Return Service Recording function shall retain a LOR data file for a period (in days) specified by the customer up to a maximum of 30 days.	B	The USA return service LOR will perform a function similar to that of the existing WSC LOR. However, recording of individual return services (instead of the existing LOR for multiplexed return services) must be performed.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.5.2.m	The USA Return Service Recording function shall provide LOR data playback at the request of the customer. LOR operation is described in the USA Operations Concept Document (452-OCD-USA).	B	The USA return service LOR will perform a function similar to that of the existing WSC LOR. However, recording of individual return services (instead of the existing LOR for multiplexed return services) must be performed.
4.5.3.a	The USA Return Service Recording function shall support TDRSS return service data rates less than or equal to 25 (TBR) Mbps.	C	Maximum return service data rate as specified in Cx-SCAN IRD Vol. 1,2
4.5.3.b	The USA Return Service Recording function shall support data retrieval per USA Operations Concept Document (452-OCD-USA).	B	The USA return service LOR will perform a function similar to that of the existing WSC LOR. However, recording of individual return services (instead of the existing LOR for multiplexed return services) must be performed.
4.5.3.c	The USA Return Service Recording function shall be configured prior to the scheduled service start time.	B	Complies with the current WSC operational requirements.
4.5.3.d	The USA Return Service Recording function shall provide its current Status and Health data to the Monitor and Control function every 5 seconds in accordance with present WSC hardware specifications.	B	Complies with the current WSC operational requirements.
4.6.1.a	The USA shall interface with the NISN networks in accordance with the specifications in the Interface Control Document between the Space Network User Service Access and the NASA Integrated Services Network, 452-ICD-USA/NISN.	B	

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
4.6.2.a	The USA shall interface with the Constellation network in accordance with the specifications in the Interface Control Document between the Space Network User Service Access and the Constellation Ground Network, 452-ICD-USA/CxNet.	C	
4.6.3.a	The USA shall interface with the USSR in accordance with the USSR Interface Description given in Appendix B.	B	
5.1.1.a	The Parts Count Reliability prediction method of MIL-HDBK-217 shall be used in the initial stages of system design to determine the MTBF.	B	Complies with the current WSC operational requirements.
5.1.1.b	The reliability prediction method shall shift to the Parts Stress Analysis Prediction method, or other reliability modeling technique approved by NASA, at the time when a firm, detailed parts list is available to determine the MTBF.	B	Complies with the current WSC operational requirements.
5.2.1.a	USA shall have an MTTR not exceeding 30 minutes during the expected 15 year lifetime of the USA.	B	Complies with the current WSC operational requirements.
5.2.1.b	The maximum time to repair shall not exceed 1 hour for 90 percent of failures.	B	Complies with the current WSC operational requirements.
5.2.2.a	Failures shall be isolated to one chassis or Line Replaceable Unit (LRU), whichever is smaller. Manual intervention can be used to isolate failures to below the chassis or LRU level.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
5.2.2.b	Modes shall be provided to enable the repeating and/or bypassing of tests to check the operation of the subsystems while using internal or external test equipment.	B	Complies with the current WSC operational requirements.
5.3.a	The inherent availability for any period of 10,000 hours shall be 0.9998.	B	Complies with the current WSC operational requirements.
5.4.a	There shall be a communications path from the output of the TDRSS legacy or DAS return service to the NISN/Constellation interface, such that the operational availability, measured over a 10,000 hour interval is 0.9999. Redundant paths may be used in achieving this Ao.	B	Complies with the current WSC operational requirements.
5.4.b	There shall be a communications path from the NISN/Constellation interface to the TDRSS forward service input, such that the operational availability, measured over a 10,000 hour interval is 0.9999. Redundant paths may be used in achieving this Ao.	B	Complies with the current WSC operational requirements.
6.1.a	NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.3.5.2, ISSO.	B	Complies with the current WSC operational requirements.
6.1.b	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.3.5.3, Ensuring User Accounts.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
6.1.c	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.3.6, System Administrator.	B	Complies with the current WSC operational requirements.
6.1.d	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.4.9, User Community and NASA Customers.	B	Complies with the current WSC operational requirements.
6.1.e	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 11.2, NIST Security Controls	B	Complies with the current WSC operational requirements.
6.1.f	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 11.3, NASA-Wide Common Security Controls, except 11.3.9, 11.3.10, 11.3.11, and 11.3.12, which are not applicable.	B	Complies with the current WSC operational requirements.
6.1.g	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.1.3, Routine Monitoring.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
6.1.h	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.1.9, Records Requirements.	B	Complies with the current WSC operational requirements.
6.1.i	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.1.11.6 [Responsibilities of] NASA and Center monitoring personnel.	B	Complies with the current WSC operational requirements.
6.1.j	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.2, Periodic Testing and Security Controls Requirements.	B	Complies with the current WSC operational requirements.
6.1.k	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 17.2, Incident Handling and Reporting Requirements.	B	Complies with the current WSC operational requirements.
6.1.l	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 18.2, Awareness and Training Requirements.	B	Complies with the current WSC operational requirements.
6.1.m	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 19.2, Account Management Requirements.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
6.1.n	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 20.2, Logical Access Requirements.	B	Complies with the current WSC operational requirements.
6.1.o	The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 21.2, Audit Trail and Accountability Requirements.	B	Complies with the current WSC operational requirements.
6.1.p	The USA shall adhere to the security requirements specified in the Goddard Procedures and Requirements (GPR) 2810.1, *Security of Information Technology.*	B	Complies with the current WSC operational requirements.
6.1.q	The USA shall adhere to the security requirements specified in the 452-SP-USA, *Space Network IP in Space System Security Plan.*	B	Complies with the current WSC operational requirements.
6.1.r	The USA shall adhere to the security requirements specified in the 290-003, *IP Operational Network (IONet) Security Plan, Section 3.5.3 Operational Controls.*	B	Complies with the current WSC operational requirements.
6.1.s	The USA shall adhere to the security requirements specified in the 290-003, *IP Operational Network (IONet) Security Plan, Section 3.11 Technical Controls.*	B	Complies with the current WSC operational requirements.
6.1.t	The USA shall adhere to the security requirements specified in the 290-003, *IP Operational Network (IONet) Security Plan, Section A.1.9 System Users.*	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
6.1.u	The USA shall adhere to the security requirements specified in the WSC-PLN-0072, White *Sands Complex (WSC) Data Services Management Center (DSMC) Security Plan.*	B	Complies with the current WSC operational requirements.
6.1.v	The USA shall adhere to the security requirements specified in the 290-004, IP *Operational Network (IONet) Access Protection Policy and Requirements,* Section 2.45 System Administrators and System Security Administrators.	B	Complies with the current WSC operational requirements.
6.1.w	The USA shall adhere to the security requirements specified in the 290-004, *IP Operational Network (IONet) Access Protection Policy and Requirements,* Section 2.6 System Users.	B	Complies with the current WSC operational requirements.
6.1.x	The USA shall adhere to the security requirements specified in the 290-004, *IP Operational Network (IONet) Access Protection Policy and Requirements,* Section 3.1 General IONet Security.	B	Complies with the current WSC operational requirements.
6.1.y	The USA shall adhere to the security requirements specified in the *Constellation Command, Control, Communication, and Information (C3I) Interoperability Standards Book, Volume 1: Interoperability Specification section.*	C	Adheres to security requirements in the specified CxP document.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
6.1.z	The USA shall adhere to the security requirements specified in the *Constellation Command, Control, Communication, and Information (C3I) Interoperability Standards Book, Volume 5: Data Exchange Protocol Specification for all inter-system exchanges of the security policy information used by application layer security functions.*	C	Adheres to security requirements in the specified CxP document.
6.2.1.a	Any communications between USA, as a trusted entity, and any untrusted entity shall be initiated by the trusted USA entity.	B	Complies with the current WSC operational requirements.
6.2.1.c	The USA shall enforce the security requirements as specified in 452-SP-USA, and NPR 2810.1.	B	Complies with the current WSC operational requirements.
6.2.1.d	The USA shall ensure that customers are only able to access services for which they are authorized.	B	Complies with the current WSC operational requirements.
6.2.1.e	The USA shall ensure that customer access is limited to the specific network for which the customer is authorized.	B	Complies with the current WSC operational requirements.
6.2.1.f	The USA shall create/maintain audit files to include both activity and error logging.	B	Complies with the current WSC operational requirements.
6.2.1.g	The USA shall provide the capability for SN O&M personnel to manage all passwords.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
7.1.a	All chassis, subsystems and systems of new design or significantly modified design shall be designed and constructed to comply with the requirements of STDN-SPEC-4, GSFC General Requirements for STDN Electronic Equipment, or best commercial practices.	B	Complies with the current WSC operational requirements.
7.1.b	Connectors, cable, wires and other materials listed in STDN-SPEC-8, GSFC Specification for Electronic Equipment Installation Materials or best commercial practices shall be used in the design and construction of SA equipment, unless a waiver is received from the USA Product Design Lead.	B	Complies with the current WSC operational requirements.
7.1.c	All controls and displays shall be fully accessible during setup and normal operation of the USA.	B	Complies with the current WSC operational requirements.
7.1.d	All USA subsystem technical manuals shall be prepared in accordance with STDN-SPEC-1,Specification Preparation and Acceptance of Technical Manuals.	B	Complies with the current WSC operational requirements.
7.2.a	USA equipment shall be mounted in Electronic Equipment Racks which conform to the interface requirements of EIA-310-D, Cabinets, *Racks, Panels and Associated* Equipment.	B	Complies with the current WSC operational requirements.
7.2.b	Racks shall include tapped panel mounting holes.	B	Complies with the current WSC operational requirements.
7.2.c	Racks shall accommodate standard 19-inch EIA equipment panels.	B	Complies with the current WSC operational requirements.
7.3.a	All cable fabrication shall be in accordance with the requirements of STDN-SPEC-4, Section 3.7.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
7.3.b	All power and signal cables necessary for equipment operations shall be provided.	B	Complies with the current WSC operational requirements.
7.3.c	All cabling between USA delivered systems and subsystems and WSC/GRGT systems shall be provided.	B	Complies with the current WSC operational requirements.
7.3.d	All mating connectors shall be supplied.	B	Complies with the current WSC operational requirements.
7.3.e	All cabling required for configuring the systems and subsystems for checkout and in-plant testing shall be provided. This includes cabling required at the WSGT/STGT and GRGT sites for all special test equipment.	B	Complies with the current WSC operational requirements.
7.3.f	Cable color coding for Open IONet cables shall be blue.	B	Complies with the current WSC operational requirements.
7.3.g	Cable color coding for Closed IONet cables shall be red.	B	Complies with the current WSC operational requirements.
7.3.h	Cable color coding for Restricted IONet cables shall be pink (hot pink).	B	Complies with the current WSC operational requirements.
7.4.a	USA equipment conducted and radiated emissions shall not affect existing equipment.	B	Complies with the current WSC operational requirements.
7.4.b	USA equipment shall not be affected by conducted or radiated emissions resulting from the operation of existing WSC equipment.	B	Complies with the current WSC operational requirements.
7.4.c	Electromagnetic Interference (EMI) racks and filtering shall be used as required.	B	Complies with the current WSC operational requirements.
7.4.d	All USA equipment shall comply with the above EMI requirements without using rack front doors or hiding controls and displays.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
7.4.e	All USA equipment shall comply with the requirements of Part 1, General Requirements, and Part 3, for Class A2b ground support equipment, including requirement CS01, of MIL-STD-461, Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference.	B	Complies with the current WSC operational requirements.
7.5.a	USA shall use modular hardware and software that allows changes and enhancements to the USA system.	B	Complies with the current WSC operational requirements.
7.5.b	USA hardware shall use functional modules that allow replacement to improve performance, reliability or for other reasons.	B	Complies with the current WSC operational requirements.
7.5.c	USA software shall use documented modules and a structure that allows maintenance and enhancements.	B	Complies with the current WSC operational requirements.
7.6.a	The USA computer processors shall provide CPU reserve capacity > 100% of the CPU capacity required to meet the USA system and subsystem performance requirements. The USA computer processors shall provide memory reserve capacity > 100% of the memory capacity required to meet the USA system and subsystem performance requirements. The USA computer processors shall provide disk storage reserve capacity > 100% of the disk storage capacity required to meet the USA system and subsystem performance requirements.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
7.6.b	The USA computer processors shall provide memory reserve capacity ≥ 100% of the memory capacity required to meet the USA system and subsystem performance requirements.	B	Complies with the current WSC operational requirements.
7.6.c	The USA computer processors shall provide disk storage reserve capacity ≥ 100% of the disk storage capacity required to meet the USA system and subsystem performance requirements.	B	Complies with the current WSC operational requirements.
8.2.1.2.a	Preventive maintenance shall be performed in accordance with manufacturers' specifications and recommendations.	B	Complies with the current WSC operational requirements.
8.2.1.2.b	Components selected for the implementation of USA shall incorporate built-in test and diagnostic features that allow fault isolation to an LRU.	B	Complies with the current WSC operational requirements.
8.2.1.3.a	Second level maintenance capabilities to support the achievement of the required operational availability of all ground systems over the lifecycle of the systems including achievement of first level maintenance requirements shall be provided.	B	Complies with the current WSC operational requirements.
8.2.2.1.a	Includes the resources required to affect desired changes to operational and non-operational software.	B	Complies with the current WSC operational requirements.
8.2.2.1.b	Includes the testing resources required to ensure that new and modified software meets all existing functional and performance specifications and, in the case of enhancements, meets all newly defined functional and performance requirements.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
8.2.2.1.c	Includes the verification resources required to ensure that the delivery of software modifications to operational systems will not compromise the required operational availability of those systems.	B	Complies with the current WSC operational requirements.
8.2.2.1.d	Includes the capabilities required to maintain and protect the software baseline for all locally maintained software components.	B	Complies with the current WSC operational requirements.
8.2.2.1.e	Includes all capabilities required to produce, deliver and document corrections, modifications, adaptations, and enhancements of existing software for the USA.	B	Complies with the current WSC operational requirements.
8.2.2.1.f	Includes the capabilities required for the adaptation of third party software for use in USA.	B	Complies with the current WSC operational requirements.
8.2.2.2.a	Software change control and configuration status accounting.	B	Complies with the current WSC operational requirements.
8.2.2.2.b	Software Quality Assurance (QA).	B	Complies with the current WSC operational requirements.
8.2.2.2.c	Software tools for the automation of SCM functions..	B	Complies with the current WSC operational requirements.
8.2.2.2.d	Maintenance of all final design source code and executable code.	B	Complies with the current WSC operational requirements.
8.2.2.2.e	Facilities to store the latest versions of software for the USA in a manner secure from alteration by malicious tampering or destruction by fire, flood, or other disaster.	B	Complies with the current WSC operational requirements.

Rqmnt. #	Requirement	Allocation	Rationale/Assumptions
8.2.2.a	For all software components that are not maintained by external parties (i.e. operating system, Commercial-off-the-shelf (COTS) software products), the software maintenance function shall include all hardware and development software that is required to generate all system software components from the source code that is maintained by the SCM function for that component.	B	Complies with the current WSC operational requirements.
8.2.3.a	Spares provisioning plan for the USA shall be determined and provided by the development contractor for approval by NASA.	B	Complies with the current WSC operational requirements.
8.2.3.b	The proposed spare parts and quantities shall be based upon satisfying the availability and maintainability requirements of this Requirements Document.	B	Complies with the current WSC operational requirements.
8.2.3.c	It shall be ensured that either spare parts are available for a period of 15 years after Final Acceptance Testing or that NASA be provided advance notice of intent to discontinue manufacture of parts/components by all levels of subcontractors.	B	Complies with the current WSC operational requirements.

Reliability, Maintainability, Availability Requirements

Reliability, Maintainability, and Availability Requirements

Further definitions/requirements for RMA:

Reliability

- The measure of reliability for the USA shall be the Mean Time Between Failures (MTBF)
- MTBF for any identified equipment group is defined as the life cycle period of the equipment divided by the predicted number of failures
  - MTBF for any equipment group shall be determined during the initial stages of system design in accordance with the Parts Count Reliability prediction method of MIL-HDBK-217, Reliability Prediction of Electronic Equipment
  - MTBF for any equipment group shall shift to the Parts Stress Analysis Prediction method, or other reliability modeling technique approved by NASA, at the time when a firm, detailed parts list is available for the equipment group

Reliability, Maintainability, and Availability Requirements (continued)

Maintainability

- Maintainability is characterized by the Mean Time to Repair (MTTR) and the maximum time to repair
- MTTR, as a measure of maintainability of an individual equipment group, is defined as the sum of corrective maintenance times, to include Level-1 maintenance only, divided by the total number of failures within that equipment group during a particular interval under stated conditions
- MTTR is 30 minutes during the expected lifetime of USA
- Maximum time to repair shall not exceed 1 hour for 90 % of failures

Availability

- Inherent Availability
  - Inherent Availability (A_i) is a measure of the probability that a system or equipment group, when used under stated conditions in an ideal support environment (i.e., using available tools, spares, and personnel) will operate within specifications at any time
  - The A_i of an equipment group is defined per the expression:
    - $$A_i = \frac{MTBF}{MTBF + MTTR}$$

      for any period of 10,000 hours

- Design of all USA equipment shall meet the following Inherent Availability requirements:
  - A_I = .9998 (for any 10, 000-hour period)

Reliability, Maintainability, and Availability Requirements (continued)

Availability (cont'd)

- Operational Availability
  - Operational Availability (A_o) for any system is a measure of the percentage of time the system is available to support the service or support function for which the system is intended, and to perform that function within all specifications defined by these functional and performance requirements
  - The A_o of an equipment group is defined per the expression:
    - $$A_o = \frac{Time\ Service\ is\ Available}{Time\ Service\ is\ Available\ +\ Time\ Service\ is\ Not\ Available}$$

      over a contiguous 10,000 hour interval except that any loss of availability due to loss of facility services such as power or air conditioning will not be counted
- All USA equipment shall meet the following Operational Availability requirements:
  - Ao = .9999 per 10,000 hours

  For both forward paths and return paths from both NISN and CxP routers

Security Requirements

Security Requirements (1 of 5)

- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.3.5.2, ISSO.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.3.5.3, Ensuring User Accounts.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.3.6, System Administrator.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 2.4.9, User Community and NASA Customers.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 11.2, NIST Security Controls
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 11.3, NASA-Wide Common Security Controls, except 11.3.9, 11.3.10, 11.3.11, and 11.3.12, which are not applicable.

Security Requirements (2 of 5)

- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.1.3, Routine Monitoring.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.1.9, Records Requirements.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.1.11.6 [Responsibilities of] NASA and Center monitoring personnel.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 16.2, Periodic Testing and Security Controls Requirements.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 17.2, Incident Handling and Reporting Requirements.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 18.2, Awareness and Training Requirements.

Security Requirements (3 of 5)

- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 19.2, Account Management Requirements.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 20.2, Logical Access Requirements.
- The USA shall adhere to the security requirements specified in the NASA Procedural Requirements (NPR) 2810.1A, *Security of Information Technology,* 21.2, Audit Trail and Accountability Requirements.
- The USA shall adhere to the security requirements specified in the Goddard Procedures and Requirements (GPR) 2810.1, *Security of Information Technology*.
- The USA shall adhere to the security requirements specified in the 452-SP-USA, *Space Network IP in Space System Security Plan*.
- The USA shall adhere to the security requirements specified in the 290-003, *IP Operational Network (IONet) Security Plan, Section 3.5.3 Operational Controls*.
- The USA shall adhere to the security requirements specified in the 290-003, *IP Operational Network (IONet) Security Plan, Section 3.11 Technical Controls*.

Security Requirements (4 of 5)

- The USA shall adhere to the security requirements specified in the 290-003, *IP Operational Network (IONet) Security Plan, Section A.1.9 System Users.*
- The USA shall adhere to the security requirements specified in the WSC-PLN-0072, Wh*ite Sands Complex (WSC) Data Services Management Center (DSMC) Security Plan*.
- The USA shall adhere to the security requirements specified in the 290-004, I*P Operational Network (IONet) Access Protection Policy and Requirements,* Section 2.45 System Administrators and System Security Administrators.
- The USA shall adhere to the security requirements specified in the 290-004, *IP Operational Network (IONet) Access Protection Policy and Requirements,* Section 2.6 System Users.
- The USA shall adhere to the security requirements specified in the 290-004, *IP Operational Network (IONet) Access Protection Policy and Requirements*, Section 3.1 General IONet Security.
- The USA shall adhere to the security requirements specified in the *Constellation Command, Control, Communication, and Information (C3I) Interoperability Standards Book, Volume 1: Interoperability Specification section.*
- The USA shall adhere to the security requirements specified in the *Constellation Command, Control, Communication, and Information (C3I) Interoperability Standards Book, Volume 5: Data Exchange Protocol Specification for all inter-system exchanges of the security policy information used by application layer security functions.*

Security Requirements (5 of 5)

- Any communications between USA, as a trusted entity, and any untrusted entity shall be initiated by the trusted USA entity.
- The USA shall automate enforcement of password requirements specified in NPR 2810.1A including as a minimum length, composition constraints, longevity (how frequently the password is changed) and constraints on re-using passwords.
- The USA shall enforce the security requirements as specified in 452-SP-USA, and NPR 2810.1.
- The USA shall ensure that customers are only able to access services for which they are authorized.
- The USA shall ensure that customer access is limited to the specific network for which the customer is authorized.
- The USA shall create/maintain audit files to include both activity and error logging.
- The USA shall provide the capability for SN O&M personnel to manage all passwords.

Equipment Design, Construction, and Installation Requirements

SRD Section 7 Equipment Design & Construction

- **General electrical and mechanical design and construction requirements for the USA chassis, subsystems, and racks.– are consistent with standard WSC definitions**
  - **General Requirements for Electronic Equipment**
    - All chassis, subsystems and systems of new design or significantly modified design shall be designed and constructed to comply with the requirements of STDN-SPEC-4, GSFC General Requirements for STDN Electronic Equipment, or best commercial practices.
    - Connectors, cable, wires and other materials listed in STDN-SPEC-8, GSFC Specification for Electronic Equipment Installation Materials or best commercial practices shall be used in the design and construction of USA equipment, unless a waiver is received from the USA Product Design Lead.
    - All controls and displays shall be fully accessible during setup and normal operation of the USA.
    - All USA subsystem technical manuals shall be prepared in accordance with STDN-SPEC-1,Specification Preparation and Acceptance of Technical Manuals.
  - **Electronic Equipment Racks**
    - USA equipment shall be mounted in Electronic Equipment Racks which conform to the interface requirements of EIA-310-D, *Cabinets, Racks, Panels and Associated Equipment*.
    - Racks shall include tapped panel mounting holes.
    - Racks shall accommodate standard 19-inch EIA equipment panels.

- **Cabling and Connectors**
  - All cable fabrication shall be in accordance with the requirements of STDN-SPEC-4, Section 3.7.
  - All power and signal cables necessary for equipment operations shall be provided.
  - All cabling between USA delivered systems and subsystems and WSC/GRGT systems shall be provided.
  - All mating connectors shall be supplied.
  - All cabling required for configuring the systems and subsystems for checkout and in-plant testing shall be provided. This includes cabling required at the WSGT/STGT and GRGT sites for all special test equipment.
  - Cable color coding for Open IONet cables shall be blue.
  - Cable color coding for Closed IONet cables shall be red.
  - Cable color coding for Restricted IONet cables shall be pink (hot pink).
- **Electromagnetic Interference**
  - USA equipment shall not be affected by conducted or radiated emissions resulting from the operation of existing WSC equipment.
  - Electromagnetic Interference (EMI) racks and filtering shall be used as required.
  - All USA equipment shall comply with the above EMI requirements without using rack front doors or hiding controls and displays.
  - All USA equipment shall comply with the requirements of Part 1, General Requirements, and Part 3, for Class A2b ground support equipment, including requirement CS01, of MIL-STD-461, Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference.

- **Modularity and Expandability**
  - USA shall use modular hardware and software that allows changes and enhancements to the USA system.
  - USA hardware shall use functional modules that allow replacement to improve performance, reliability or for other reasons.
  - USA software shall use documented modules and a structure that allows maintenance and enhancements.
- **Computer Processor Reserve Capacity**
  - The USA computer processors shall provide CPU reserve capacity $\geq$ 100% of the CPU capacity required to meet the USA system and subsystem performance requirements.
  - The USA computer processors shall provide memory reserve capacity $\geq$ 100% of the memory capacity required to meet the USA system and subsystem performance requirements.
  - The USA computer processors shall provide disk storage reserve capacity $\geq$ 100% of the disk storage capacity required to meet the USA system and subsystem performance requirements.

Maintenance Requirements

SRD Sect. 8 : Maintenance Requirements

The objective of the maintenance functions is to support achievement of the required USA operational availability.

Standard hardware definitions apply.

- **Hardware Maintenance** is conducted at two levels: First level and second level maintenance
- **Line Replacable Unit (LRU) Identification** is first performed to achieve 1st and 2nd level maintenance

First Level Maintenance

- Includes scheduled preventive maintenance and fault isolation to the lowest feasible level of LRU.
  - Preventive maintenance shall be performed in accordance with manufacturers' specifications and recommendations.
  - Components selected for the implementation of USA shall incorporate built-in test and diagnostic features that allow fault isolation to an LRU.

Second Level Maintenance

- Includes restoration of a malfunctioning LRU to serviceable condition,
- Includes the diagnosis and restoration of a malfunctioning equipment or system when the fault isolation capabilities of first level maintenance are incapable of localizing a failure to a line replaceable item within the equipment or system.
  - Second level maintenance capabilities to support the achievement of the required operational availability of all ground systems over the lifecycle of the systems including achievement of first level maintenance requirements shall be provided.

Software Maintenance (1 of 3)

- **Software Maintenance**
  - The purpose of the Software Maintenance function is to provide the ability to ***maintain, modify, and enhance*** the software of all systems that make up the USA; (non-operational systems as well as operational systems).
  - No distinction is made between software and firmware unless that distinction is explicitly stated.
  - To the extent feasible the capabilities of the existing Software Maintenance and Test Facility (SMTF) at the WSC will be used.

Software Maintenance

- **General Requirements: – SM Function requirements are consistent with standard WSC definitions**
- A software maintenance function shall be provided that:
  - Includes the resources required to affect desired changes to operational and non-operational software.
  - Includes the testing resources required to ensure that new and modified software meets all existing functional and performance specifications (and, in the case of enhancements, meets all newly defined functional and performance requirements.)
  - Includes the verification resources required to ensure that the delivery of software modifications to operational systems will not compromise the required operational availability of those systems.
  - Includes the capabilities required to maintain and protect the software baseline for all locally maintained software components.
  - Includes all capabilities required to produce, deliver and document corrections, modifications, adaptations, and enhancements of existing software for the USA.
  - Includes the capabilities required for the adaptation of third party software for use in USA.

Software Maintenance

- **Software Configuration Management (SCM) – are consistent with standard WSC definitions**
- Shall be capable of:
  - Software change control and configuration status accounting.
  - Software Quality Assurance (QA).
  - Software tools for the automation of SCM functions.
  - Maintenance of all final design source code and executable code.
  - Facilities to store the latest versions of software for the USA in a manner secure from alteration by malicious tampering or destruction by fire, flood, or other disaster.
- **Software Baseline (definition of)**
  - "For all software components that are not maintained by external parties (i.e. operating system, Commercial-off-the-shelf (COTS) software products), the software maintenance function shall include all hardware and development software that is required to generate all system software components from the source code that is maintained by the SCM function for that component."

Maintenance: Spares Provisioning

- **Spares Provisioning – are consistent with standard WSC definitions**
  - Spares provisioning plans are to be provided by the development contractor for approval by NASA.
  - Proposed spare parts and quantities shall be based upon satisfying the requirements of this Requirements Document.
  - Shall be ensured that either spare parts are available for 15 years or NASA given notice of intent to discontinue

CxP Discrete Data Rates

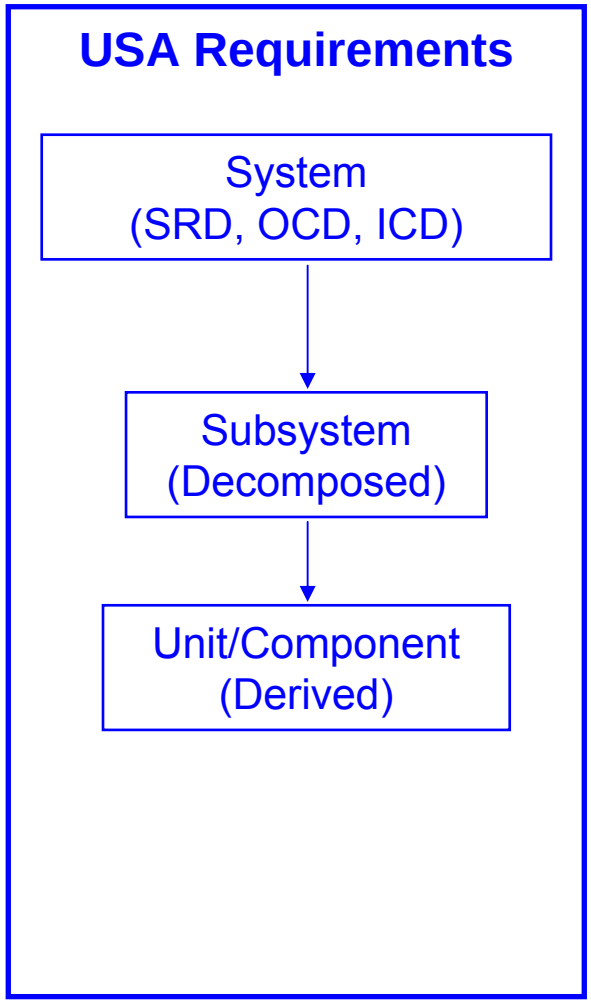
SN Assumptions (Concluded)

- Discrete CxP Data Rates
  - Operational Point-to-point (IP over CCSDS Space Links)
    - SSAF: 1 Mbps, 72 kbps, 18 kbps
    - SSAR: 1 Mbps, 192 kbps, 24 kbps
  - High Rate (IP over CCSDS Space Links)
    - KaSAR: 25 Mbps
    - KaSAF: 6 Mbps
  - Dissimilar Voice (Non IP/AOS)
    - SSAF: 10.2 kbps
    - SSAR: 10.2 kbps
  - Emergency Communications (Non IP/AOS)
    - SSAF: 10.2 kbps
    - SSAR: 10.2 kbps
  - Post-Landing Communications (Non IP/AOS)
    - SSAF: 10.2 kbps
    - SSAR: 10.2 kbps

Requirements Management

Requirements Development Flow

Requirement Type	Definition	Timeframe
System	Requirements directly from SRD, ICD, OCD, and other sources, levied upon USA	
Decomposed	Requirements decomposed from system requirements. These are USA's interpretation of system requirements and are generally subsystem requirements	Preliminary Design Review
Derived	Requirements derived from decomposed requirements. These are a subsystem's interpretation of decomposed requirements and are generally unit/component requirements	Critical Design Review



Draft USA RM Process Phases

Ingest = Project Definition

- Ingest the SRD into the DOORS SRD Module
- Ingest the OCD into the DOORS OCD Module
- Ingest ICDs into DOORS ICD Modules

Note: Captured after the SRR Milestone

Decompose = System Design

- Define the Database Schema and Attributes in the DOORS RTVM Module
- Decompose & derive SRD, OCD, and ICD requirements
- Baseline the RTVM
- Define Internal ICDs, allocate sub-systems requirements

Link = Trace Definition to Design

- Define links from 'parent' document modules (SRD, OCD, ICD) to 'children' in the RTVM
- Define links from the RTVM to the System SDS and Internal ICDs

Manage = RM Lifecycle

- Control changes to requirements post baseline with CWGs
  - Includes a change history
- Report status metrics for requirements volatility and design maturity
- Coordinate requirements with weekly RTVM distribution
- Produce requirements 'shreds' for custom views
- Backup the database with automated backups and after CWGs

Abbreviations and Acronyms

Abbreviations and Acronyms

A_i	Inherent Availability
A_o	Operational Availability
ADPE	Automated Data Processing Equipment
API	Application Programmer Interface
AOS	Acquisition of Signal
AOS	Advanced Orbiting Systems
AWGN	Additive White Gaussian Noise
BGP	Border Gateway Protocol
C3I	Command, Control, Communication, and Information
CA	Certificate Authority
CANDOS	Communication and Navigation Demonstration On Shuttle
CCB	Configuration Control Board
CCR	Configuration Change Request
CCSDS	Consultative Committee for Space Network Data Systems
CLTU	Command Link Transmission Unit
COTS	Commercial-Off-The-Shelf

Abbreviations and Acronyms

CPU	Central Processing Unit
CTFS	Common Time and Frequency System
Cx	Constellation Program
DAS	Demand Access System
DASCON	DAS Controller
DCN	Document Control Notice
DIS	Data Interface System
DOORS	Dynamic Object Oriented Requirements System
DSMC	Data Services Management Center
DT&T	Development, Test and Training
DTN	Disruption Tolerant Network
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Electro Magnetic Interference
ENCAP	Encapsulation (packet service)
ESCPD	Exploration and Space Communications Projects Division
Exec ADPE	Executive ADPE
FCLTU	Forward Command Link Transmission Unit

Abbreviations and Acronyms

FDF	Flight Dynamics Facility
FEC	Forward Error Correction
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FOC	Full Operations Capability
GDIS	Guam Data Interface System
GN	Ground Network
GMCS	Ground Monitor and Control Subsystem
GPG	Goddard Procedures and Guidelines
GRGT	Guam Remote Ground Terminal
GSFC	Goddard Space Flight Center
HDLC	High-level Data Link Control
HDR	High Data Rate
HMD	Hardware Maintenance Depot
ICD	Interface Control Document
IEC	International Electrotechnical Commission
IF	Intermediate Frequency

Abbreviations and Acronyms

IOC	Interim Operations Capability
IONet	Internet Protocol (IP) Operational Network
IP	Internet Protocol
IPv4	Internet Protocol, Version 4
IPv6	Internet Protocol, Version 6
ISO	International Organization for Standardization
ISSO	Information System Security Officer
IT	Information Technology
ITSSP	Information Technology Systems Security
KaSA	Ka Band Single Access
KaSAF	Ka Band Single Access Forward
KaSAR	Ka Band Single Access Return
KSA	K-Band Single Access
KuSA	Ku Band Single Access
KuSAF	Ku Band Single Access Forward
KuSAR	Ku Band Single Access Return
LDR	Low Data Rate

Abbreviations and Acronyms

LDPC	Low Density Parity Check
LI	Local Interface
LOR	Line Outage Recording
LRUs	Line Replaceable Units
M&C	Monitor and Control
MA	Multiple Access
MAF	Multiple Access Forward
MANET	Mobile Ad hoc Networking
MAR	Multiple Access Return
Mbps	Megabits per second
MOC	Mission Operations Center
MPDU	Monitor and Control Protocol Data Unit
MPoFR	Multi Protocol over Frame Relay

Abbreviations and Acronyms

MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
MS	Mission Systems (similar to a MOC)
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NB	Narrow Band
NCC	Network Control Center
NCCDS	Network Control Center Data System
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
NPG	NASA Procedures and Guidelines
NPR	NASA Procedural Requirements
NRZ	Non-Return to Zero
NTP	Network Time Protocol
O&M	Operations and Maintenance

Abbreviations and Acronyms

OCD	Operational Concept Document
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PI	Principal Investigator
POA&M	The Plan of Action and Milestones
PPP	Point-to-Point Protocol
PVM	Performance Verification Matrix
QA	Quality Assurance
QOS	Quality of Service
RAF	Return All Frames
RAR	Resource Allocation Request
RCF	Return Channel Frames
RF	Radio Frequency
RFC	Request For Comment
RIP	Routing Information Protocol
RMA	Reliability, Maintainability, and Availability
RS	Reed-Solomon

Abbreviations and Acronyms

RSR	Return Service Recording
RTVM	Requirements Traceability Verification Matrix
SA	System Administrator
SCaN	Space Communication and Navigation
SCM	Software Configuration Management
SCP	Secure Copy Protocol
SCaN	Space Communication and Navigation System
SFTP	Secure File Transfer Protocol
SGLT	Space-Ground Link Terminal
SLE	Space Link Extension
SHO	Schedule Order
SMA	S-Band Multiple Access
SMTF	Software Maintenance and Training Facility
SN	Space Network
SNAS	Space Network Access System
SNUG	Space Network Users' Guide

Abbreviations and Acronyms

SPEC	Specification
SPTR	South Pole TDRSS Relay
SRD	System Requirements Document
SSA	S-Band Single Access
SSAF	S-Band Single Access Forward
SSAR	S-Band Single Access Return
SSL	Secure Socket Layer
STDN	Space Flight Tracking and Data Network
STGT	Second TDRSS Ground Terminal
SWSI	Space Network Wed Services Interface
TBD/TBR	To Be Determined/To Be Reviewed
TBS	To -Be Supplied
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Tracking Data Message

Abbreviations and Acronyms

TDRS	Tracking and Data Relay Satellite
TDRSS	Tracking and Data Relay Satellite System
TOCC	TDRSS Operations Control Center
UDP	User Datagram Protocol
UPD	User Performance Data
USA	User Service Access
USS	User Service Subsystem
USSR	User Service Subsystem Replacement
UTC	Universal Time Coordinated
VCA	Virtual Channel Access
VCP	Virtual Channel Packet
WB	Wide Band
WDISC	WSC TCP/IP Data Interface Services Capability
WSC	White Sands Complex
WSGT	White Sands Ground Terminal

RFA Sample

REQUEST FOR ACTION (RFA)		
1. Review Type **USA System Requirements Review**	2. RFA No.	3. Review Date **5/12/08**
4. Title		
5. Action		
Reference		
6. Originator/Organization/Telephone No./E-mail		
7. Assigned To/Organization/Telephone No./E-mail		Due Date
8. Response		
9. Response By/Organization/Telephone No./E-mail		Date Prepared
10. Originator Contacted	☐ No ☐ Yes	Date
11. Disposition	☐ Open ☐ Deferred ☐ Closed	☐ Withdrawn
12. Comments		
13. Approval	_____	_____ Date