EOIS/AD2-ND-149

Network Communications Interface Operations Procedure for NASDA and NASA/NOAA for the ADEOS-II Project

Version 1.0

November 2002
National Space Development Agency of JAPAN
Earth Observation Research Center

Network Communications Interface Operations Procedure for NASDA and NASA/NOAA for the ADEOS-II Project

Version 1.0

November 2002

APPROVED BY:

Mitsunori Yamauchi

Mitsunori Yamauchi
EOC Senior Engineer

Date '02.11.29

Abstract

This procedure (NIOP) is for online data transfer for the ADEOS-II project. The NIOP is based on the Network Communications Interface Control Document between NASDA and NASA/NOAA (EOIS/AD2-ND-009), and describes normal and anomalous operating procedures. The ADEOS-II operators at NASA/NOAA and NASDA will perform their duties based on this NIOP.

Table of Contents

Abstract ii
Table of Contents iii
1. Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Document Maintenance Policy 1
2. Related Documentation 2
2.1 Parent Documents 2
2.2 Reference Documents 2
3. Operation Procedure During Nominal Operation 3
3.1 Daily Operation 3
3.2 Notification for Planned Outage 3
3.3 Password change 3
3.3.1 NASDA/EOC 3
3.3.2 ASF 4
3.3.3 WFF 5
3.3.4 JPL/SeaPAC 6
3.3.5 JPL/PO.DAAC 7
3.3.6 NOAA 7
4. Anomalous Operation Procedure 8
4.1 Major Anomaly Cases Overview 8
4.2 Troubleshooting Flows 8
• 11
4.3 Detailed Procedures 11
4.3.1 Problem Discovery 11
4.3.2 Trouble occurrence notification 11
4.3.3 Restoration 12
4.3.4 Restoration and move to normal operation 12
5. Failover Mode Operation 13
5.1 NASDA/EOC NGN 13
5.2 ASF 14
5.2.1 ASF (MOIF) 14
5.2.2 ASF/SAFS 15
5.3 WFF 15

5.3.1 DSMC/WSC 15
The DSMC WOTIS has a failover capability on the front-end. This failover should be non-impacting to customers..... 15
5.3.2 CSAFS/GSFC..... 15
5.4 JPL/SeaPAC 15
5.5 JPL/PO.DAAC..... 16
5.6 NOAA 17
6. MOIF Backup Operation..... 18
6.1 Backup Operations Overview (applies only to MOIF file transfers) 18
6.1.1 InetB 18
6.1.2 ~~Media shipment operation~~ (Deleted)..... 20
6.1.3 How to Move to Backup Operation 20
6.1.4 Return from Backup Operation to Normal Operation 21
6.2 Backup Operation Method for Each Facility 22
7. Network Security 23
7.1 ADEOS-II Network Security Policy 23
7.2 Major network security and operation policy 23
8. Operation Time and Personnel..... 26
8.1 NASDA/EOC 26
8.2 ASF..... 27
8.3 WFF 27
8.4 JPL/SeaPAC 29
8.5 JPL/PO.DAAC..... 29
8.6 NOAA 30
9. Points of Contact..... 31

1. Introduction

1.1 Purpose

The NIOP is the network operations procedure for the ADEOS-II online data transfer system and is based on the Network ICD (EOIS/AD2-ND-009). The NIOP describes NASDA-NASA/NOAA network operations for normal and anomalous operations. The ADEOS-II operators will perform their duties based on this document.

1.2 Scope

This document applies to the ADEOS-II nominal operation phase. This document also applies to NASA/NOAA facilities that interface with EOC/Data Distribution Subsystem (DDS). NASA internal data transfer is out of scope for this document.

1.3 Document Maintenance Policy

NASDA is responsible for management of the NIOP. If changes to this document are necessary, the revised document will be issued by NASDA.

If any ADEOS-II agency wants to change this document, the agency will issue an OCL that includes the change(s), reason(s) for the change(s), and actual wording to revise this document. Affected agencies will agree to the change(s); NASDA will update the document and issue a revised version by OCL.

If coordination is necessary for any agency to change this document, it will be discussed at a MOM or in another appropriate way.

2. Related Documentation

2.1 Parent Documents

(1) ADEOS-II Mission Operations Interface Specification (Common Part) (AD2-EOC-96-054)

(2) ADEOS-II Mission Operations Interface Specification (NASDA-NASA/NOAA) (AD2-EOC-97-046)

(3) Network Communications Interface Control Document Between NASDA and NASA/NOAA for the ADEOS-II Project (EOIS/AD2-ND-009)

2.2 Reference Documents

(1) ADEOS-II Contact Points Document (AD2-EOC-96-124)

(2) Operations Procedure (OP) for the Management and Operation of the ATM Service Between NASDA and NASA (EOIS/AD2-ND-116)

3. Operation Procedure During Nominal Operation

This section describes the procedure for nominal operation phase.

3.1 Daily Operation

All ADEOS-II facilities are capable of automated online data transfer. Therefore, NASDA and NASA/NOAA do not plan to have staff watch daily operations for network data transfer.

3.2 Notification for Planned Outage

In cases of planned outages of service, data transfers will be handled by procedures for anomalous operations with prior arrangements. Anomalous operations are described in section 4.

Notes:

- NASDA will provide draft wording for NASDA notification of pending outage and recovery of outage.
- NGN will get input for other US agencies.
- Each agency will provide an address for receiving OCLs.
- Contact points to be given to Nakamura.

3.3 Password change

The operations lead at each site shall set the same password for both primary and secondary servers following the procedures described below.

3.3.1 NASDA/EOC

NASDA/EOC Data Distribution Subsystem (DDS) has accounts for each facility, and these passwords are effective for 90 days from the last password change. If the password has not been changed in more than 90 days, the ftp account will be disabled. In this case, password must be changed . The password changing procedure is shown below. When the password is changed for the primary DDS, the secondary DDS password is changed automatically.

(1) (Deleted)

The DDS operator will notify each agency by E-mail that "password will expire in next 5 days".

(2) Using telnet

DDS opens the telnet service to change passwords for external users. The telnet is only a service for password changing. If users access DDS by telnet, the password changing script will work automatically. Telnet users will not be able to issue any other command. Note that NOAA machines do not support telnet; SSH may be used instead. The password changing procedure is shown below:

a) User log-in by telnet command.

b) Password changing script will work automatically, and will require old password. User must enter the old password.

c) If user enters the old password correctly, new password entering requirement is shown in the display. User will enter the new password.

d) To verify, password re-entering request message will be shown in the display. User will re-enter the new password.

e) If user enters the password two times correctly, password change is successful and will be handled as "Authentication has succeeded." The password changing script will be run again. The user will then issue the "ctrl+C" command and disconnect from telnet.

The DDS operator will notify each agency by E-mail that "password will expire in next 5 days".
Note: NOAA does not use telnet.

(3) Using FAX

For users who cannot utilize telnet, manual password change by FAX to the DDS operator is available. FAX password changing method is described below:

a) If external agencies want to change the DDS password, they send a FAX to the DDS operator. The FAX format is free form but should include at a minimum the organization name, sender's name, sender's e-mail address, and the new password.

b) When the DDS operator receives the FAX, the operator will acknowledge receipt by e-mail. The e-mail will include when the password will change. The password will be changed between 00:00 and 00:01 UT from receipt of FAX.

c) The DDS operator changes the password, and notifies the user that the password has been changed.

3.3.2 ASF

ASF has two hosts: ASF/MOIF for Mission Operation Information Files (MOIF) transfer, and ASF/SAFS for Level 0 data transfer. The password treatment methods for both hosts are described below.

3.3.2.1 ASF/MOIF

ASF provides an account on their MOIF file machines for NASDA's use to ftp files from ASF in response to a DRN message. The account provided to NASDA is a full user account, and, as such, NASDA has the ability to change the password at their convenience. This should be done via ssh as ASF blocks telnet access to systems at ASF for security reasons. This is done by:

1. Access the ASF MOIF system using ssh with the NASDA username (mmoheoc) and current password.
2. Use the UNIX "passwd" command to change the password.
3. Log out of the system.

Note that ASF is investigating the possibility of implementing a password change script similar to that employed at NASDA and SeaPac. If ASF were to implement a password change script, the instructions would be the same as those for Seawinds MOIF files.

3.3.2.2 ASF/SAFS

The ASF SAFS allows access via ftp with host/password authentication.

3.3.3 WFF

WFF has two hosts: DSMC/WSC for MOIF transfer, and CSAFS/GSFC for Level 0 (and also SeaWinds MET data from NOAA) data transfer. The password treatment methods for both hosts are described below.

3.3.3.1 DSMC/WSC

DSMC assigns an account/password for NASDA to access the DSMC system. DSMC will routinely change the password assigned to NASDA sometime between 30 days to 60 days as dictated by NASA security regulations, and will notify NASDA of the new password via FAX method. The FAX format is TBD, but should include at a minimum the NASDA receiving organization name, the new password, and the sender's name with associated phone number and e-mail address.

3.3.3.2 GSFC/CSAFS

The CSAFS allows customers to access their data by either pushing the files to the customer via FASTcopy or allowing customer to pull files via ftp. NASDA has chosen to ftp pull process as their primary access method. Any given password (ftp or FASTcopy) will be changed by the CSAFS administrator upon the request of the

individual customer. Passwords are the same on the Central SAFS (CSAFS) and the CSAFS hot backup.

Several ADEOS-II customers use the same account to pull files from the CSAFS. Therefore, no single customer is allowed to change the password unilaterally, as that could prevent other ADEOS-II customers from accessing the data. Customers may request a password change by sending an e-mail to the CSAFS administrator identifying a date and time for the password change (minimum of 48 hours for normal business hours, US Eastern time).

A. Upon receipt of the password change request, the CSAFS administrator e-mails all ADEOS-II customers to notify them of the planned date and time for their concurrence.

B. All ADEOS-II customers will respond by e-mail acknowledging the upcoming change. This should be done as soon as possible within 48 hours.

C. The CSAFS administrator will notify all customers of the new password and effective date and time via FAX. The FAX will be sent to the FAX number for the customers listed in the ADEOS-II Contact Points document.

In case of a security emergency, the CSAFS administrator reserves the right to take immediate corrective action including changing the password. The administrator will follow-up notifying the ADEOS-II customers via FAX as described in paragraph C above.

3.3.4 JPL/SeaPAC

SeaPAC has three hosts: primary SMTP server, secondary SMTP server, and ftp server. The ftp server is the only password server. The password treatment method for the ftp server is shown below.

MOIF files that are transferred from SeaPAC to DDS are maintained on seapacftp.jpl.nasa.gov for the life of the mission. Files can be retrieved by ftp. Password change is by ssh.

To change password:

a) Access seapacftp using ssh.

b) Password change script will run automatically. Either change password or "ctrl+C" out of password script.

c) User is then automatically logged out. No other operations are permitted.

3.3.5 JPL/PO.DAAC

No external agencies have access to the PO.DAAC servers, so password management is out of scope.

3.3.6 NOAA

NOAA has two file server hosts for receiving MOIF and Level 0 data: one is MOIF and Level 0 data receiving server primary, and the other is the secondary. NOAA uses CSAFS to transfer SeaWinds MET data to NASDA. GSFC/CSAFS password handling method is described in 3.3.3.2. MOIF/Level 0 receiving host (adeosfs) password handling method is shown below.

NOAA receives MOIF and Level 1 DCS, SeaWinds and GLI files from DDS via DRN/RCN and DCS, SeaWinds, GLI Level 0 files from CSAFS and ASAFS and AMSR files from PO.DAAC via FASTCOPY. NOAA sends MetFile to EOC via CSAFS.

Only CSAFS, ASAFS and PO.DAAC have accounts on adeosfs and adeosfsb. These passwords can be changed by these three agencies using ssh. Telnet is not permitted.

4. Anomalous Operation Procedure

This section describes the anomalous operation procedure.

4.1 Major Anomaly Cases Overview

Cases of failed automatic online data transfers using DRN/RCN protocol fall into one or more of the following categories:

(1) Hardware problem of DDS or external agency's host
(2) Software problem of DDS or external agency's host
(3) Network trouble (communication line/network equipment)
(4) Other

While reasons for failure are varied, the basic procedure for resolving the anomaly remains the same for all categories.

4.2 Troubleshooting Flows

Figure 4-1 describes the troubleshooting procedure. These scenarios are shown below.

4.2.0 NGN Wide Area Network (WAN) Anomalies

(1) Suspected NGN WAN anomalies should be reported to the GSFC Communications Manager (Commgr.) at 301-614-6141. The Commgr. will notify the GSFC IPNoc to check WAN status.
(2) The GSFC IPNoc shall follow established procedures to determine if a NGN WAN problem exists.
(3) If a NGN WAN problem does exist the IPNoc or the Commgr. will notify the ADEOS II location that reported the problem and keep them apprised on progress towards restoration.
(4) If a WAN problem is isolated to the US/JAPAN TransPacific link the Commgr and IPNoc will follow procedures documented in the Operations Procedure (OP) for the Management and Operation of the ATM Service Between NASDA and NASA (EOIS/AD2-ND-116).

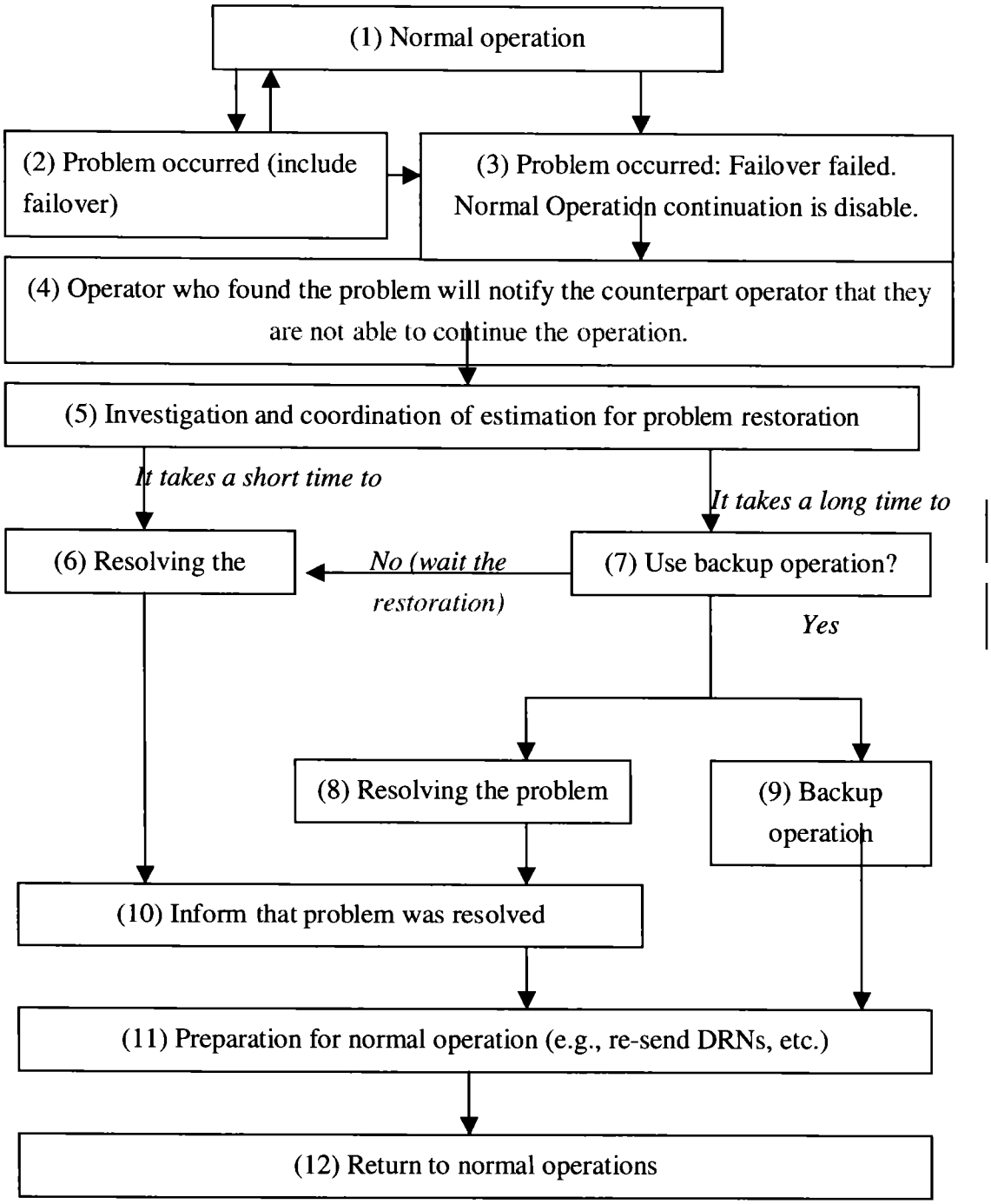


Figure 4-1. Troubleshooting Procedure

4.2.1 NASDA troubleshooting procedure

(1) Something happens during the nominal operations (move to (2) or (3)).

(2) System will perform the failover capability, and operations will continue by secondary server (move to (1)). Detailed procedures are described in section 5. If failover capability cannot recover the problem, move to (3).

(3) Problems must be investigated manually (move to (4)).

(4) The first operator who finds the problem will notify the operator of the related agency (move to (5)). The methods to contact operators are shown in section 4.3.

(5) Both agencies confirm the problem, and decide how long it will take to repair the problem. If the problem can be repaired in less than 24 hours, move to (6). If the problem correction will take more than 24 hours, move to (7).

(6) Operator fixes the problem. Move to (10).

(7) If the problem correction is estimated to take a long time, both agencies will discuss whether backup operation should be applied in this case. If both agencies agree to move to backup operation, the operation will be moved to backup operation. If both agencies agree that it is not necessary to move to the backup operation, move to (7) and wait for the problem to be fixed.

(8) The agency that has the problem will take the action to resolve the problem. Backup operation will be performed in parallel.

(9) Backup operation will be started. Detailed procedures for backup operations are described in section 6. Backup operations will continue until the problem is resolved. If problems are corrected, the troubleshooting agency will notify the counterpart agency, and move to (11).

(10) If the problem is fixed, the agency operator will notify the counterpart agency of restoration of operations. Move to (11). Notification method is shown in section 4.3 in this document.

(11) Both operators will prepare for normal operation. If necessary, confirmation testing will be performed in advance (e.g., DRN re-sending, etc.). Move to (12).

(12) Normal operation will be re-started.

4.2.2 NOAA troubleshooting procedure

NOAA is a receiving node for ADEOS files from EOC/DDS, CSAFS, ASAFS and PO.DAAC. OPLN files are parsed in order to derive the anticipated schedule of arrival of the files. The NOAA processing system creates a warning message to alert NOAA operators in case files fail to arrive before the latest expected time of arrival (ETA). The operator is expected to verify:

1. The NOAA processors are up and running, and there are no problems with disk storage.

•

4. Call or FAX the POC at the sending agency.
5. Plan to manually recover the lost files after the anomaly is resolved.

4.3 Detailed Procedures

4.3.1 Problem Discovery

Although troubleshooting is performed differently at each agency, the situations listed below can be used as guidelines for troubleshooting.

(1) When received RCNs with status of 2 or 3.
(2) RCN timeout occurred.
(3) DRN not received for a long time.
(4) Operator finds another situation preventing successful data transfer.

4.3.2 Trouble occurrence notification

When an operator discovers a problem similar to those listed above, he/she will notify the operator at the affected agency. Examples of when to contact an agency counterpart are listed below:

(1) Problems are found in an agency's systems

When an operator discovers problems in his/her system, the operator will notify his/her counterpart of the following, if necessary:

- Do not continue normal operations due to system error.
- Expected time to restore the problem.
- Necessity for backup operation.
- Any other information, if necessary.

After notification, both operators will coordinate and determine how to proceed (see 4.2 (4) and (5)).

(2) Problems are found but causes are unknown

If problems are detected but are not found in the systems themselves, or the operator has discovered problems with another agency's systems, or causes are unknown, the operator will notify his/her counterpart. The operator receiving the trouble report will investigate his/her systems and report the results. After notification, the procedure will be the same as (1) above.

The operator can choose the appropriate method of contact: Email, FAX, or telephone.

4.3.3 Restoration

System restoration is different for each facility according to local procedures. If necessary, operators will report on system restoration to counterparts.

4.3.4 Restoration and move to normal operation

When system restoration is complete, the operator will notify his/her counterpart by E-mail, FAX, or telephone. After that, both operators will prepare to move from anomaly operation to normal operation. Basically, DRN sender will re-send the interface failed DRNs, and if they are correctly sent and RCNs received, it can be determined that the problem has been fixed.

If backup operations, such as media shipment or InetB (see section 6), are in effect, they can be discontinued and the system can move to normal operation.

5. Failover Mode Operation

This section describes each party's action for the operation when the failover capability is working. Details of failover systems are described in the Network ICD (see 2.1 (3)). Section 5.1 describes NASDA/EOC/DDS operator action for failover, and after 5.2 describes the related external system operator action when failover system is (?) working.

5.1 NASDA/EOC NGN

NASDA/EOC/DDS utilizes cold failover, and has RCN timeout detection capability. In case of failover, DDS must perform the following manual operations:

(1) Failover mode is ongoing (i.e., interface between DDS and hot failover secondary of external facility), and their primary will do the restoration, change the DDS configuration of interface host from external secondary to external primary.

(2) Switch DDS itself from primary to secondary (or secondary to primary).

(3) Failover will be failed.

5.1.1 Switch the interfaces

If failover mode is ongoing, and restart of primary server for external agency is complete, both operators will take the following action:

(1) If external primary is restored and operational, the operator of external facility will notify DDS operator to change the DRN destination of DDS from external secondary to primary.

(2) DDS operator receives this notification, and changes the DDS configuration.

(3) DDS operator notifies external operator that the switching has been done.

5.1.2 DDS switching

(1) Primary server contingency discovery and contact

NASDA/EOC/DDS utilizes cold failover. In case of cold failover, the DDS operator will perform the following actions:

a) DDS operator will recognize the DDS primary server trouble in any of the following ways:

- Dialog displayed on DDS monitor when DDS detected any errors.
- Handshaking error between DDS and EOC internal/external system.
- No data sent/received for long time (3 hours or so).
- Sent/received RCNs with status of 2 or 3.

The DDS operator will check DDS status, and if there are any errors or problems with the DDS primary server, operator will shut down the primary, and boot the secondary computer as "primary". After that, operator will notify the related external agencies that DDS will change over the server from primary to secondary. (This notification includes DDS down time; i.e., when DDS is down, and when DDS secondary is up). If the DRNs were sent from external agency to DDS during this down time, external agency will re-send the DRNs to DDS. Also, DDS will send the DRNs that could not be sent when the system was down.

b) External or internal system operator recognizes trouble in DDS

EOC internal and/or external agencies can recognize problems in DDS in the following ways:

- DDS did not return RCNs a long time after any system has sent the DRNs.
- DDS returns RCNs with status 2 or 3.
- The system does not receive any DRNs from DDS for long time.

In this case, the operator who recognizes the anomaly will notify the DDS operator (on duty 24/7). DDS operator will investigate this report and if DDS operator finds the error or trouble in DDS, DDS primary will be shut down, and secondary will switched to "primary".

5.1.3 Failover failure

In case of failover failure, move to anomaly operation (see section 4).

5.2 ASF

ASF has two systems that have backups: ASF/MOIF and ASF/SAFS. As both systems are cold failover, there is no need for any agencies external to ASF to change parameters in the case of a failover at ASF. ASF has no RCN timeout capability, so ASF cannot detect failures at sites using the DRN/RCN protocol. ASF/SAFS can detect failures at sites using the FDN/RCN protocol (JPL/SeaPac and NOAA).

5.2.1 ASF (MOIF)

The ASF MOIF system has a cold backup. When a failure is detected either by ASF operations or by an external agency that notifies ASF, the cold backup is brought online and operation continues with the backup system while the primary is repaired.

5.2.2 ASF/SAFS

The ASF SAFS has a cold backup. When a failure is detected either by ASF operations or by an external agency that notifies ASF, the cold backup is brought online and operation continues with the backup system while the primary is repaired. As all Level 0 files are stored on the SAFS RAID, if a DRN message is not sent due to the failure, the receiving agency can login to the ASF SAFS to retrieve the file.

5.3 WFF

5.3.1 DSMC/WSC

The DSMC WOTIS has a failover capability on the front-end. This failover should be non-impacting to customers.

5.3.2 CSAFS/GSFC

The central SAFS utilizes a hot-failover capability. Under nominal operations, the primary machine will receive all the files from the ground station and send out all files to the customers. Only when the primary machine has failed to receive the files three times will the secondary machine begin receiving that particular file. Failover to secondary is determined on a per-file basis.

5.4 JPL/SeaPAC

JPL SeaPAC utilizes a hot-failover capability. For operations between SeaPAC and DDS, there are two systems that will be retrieving files from DDS. Under nominal operations, the primary machine will retrieve all the files. Only when the primary machine has unsuccessfully retrieved files for 24 hours will the secondary machine begin retrieving files.

For sending MOIF files to DDS, the SeaPAC primary machine will send all emails to DDS. The DDS machine will retrieve files from the SeaPAC ftp server. Failure to deliver MOIF files to DDS by primary AND secondary systems will result in transfer by InetB procedures, covered in section 6.1.1.

Failures on the DDS side are invisible to SeaPAC since the DDS primary and secondary systems appear identical from the outside.

5.4.1 DDS to SeaPAC Transfers

Steps for DDS detecting SeaPAC failure and sending to secondary:

1) Possible failure of the SeaPAC primary is noticed by DDS when RCNs are not returned.
2) If late RCNs are returned within 24 hours, then there is NO FAILOVER and it is assumed that the SeaPAC primary machine has recovered by itself and picked up all missing files. No action by DDS is required.
3) If RCNs are NOT returned after the 24 hours time limit has expired, then DDS will re-send all unanswered DRNs to the SeaPAC secondary and designate the SeaPAC secondary as the "current" machine. All new DRNs will then be sent to the SeaPAC secondary.
4) When SeaPAC primary has been restored to service, SeaPAC will send an OCL to DDS operations indicating that the SeaPAC primary should be the "current" machine. All new DRNs will then be sent to the SeaPAC primary.

5.4.2 SeaPAC to DDS Transfers

Steps for failure to successfully send the weekly SeaWinds REQQ file (the only file sent from SeaPAC to DDS):

1) An REQQ file is placed on SeaPAC ftp server and a DRN is sent at 00:00 UT each Thursday.
2) DDS retrieves REQQ file and processes it.
3) If DDS can not successfully retrieve the file OR there is an error in the file, DDS will send an REQA OCL to SeaPAC, with a complete description of the specific problem, by 14:00 UT Thursday.
4) SeaPAC will make any necessary changes and attempt to re-send the DRN by 23:00 UT Thursday.
5) If SeaPAC detects that the re-send is not successfully accomplished by 23:00 UT Thursday, SeaPAC will send the REQQ using InetB procedures, by 23:00 UT Thursday.

5.5 JPL/PO.DAAC

The JPL PO.DAAC system has a hot failover capability. If the primary server (aoi.jpl.nasa.gov) fails or there is a local JPL network failure, then the secondary server (shiro.jpl.nasa.gov), which is on a non-JPL network, is available for operational use.

Under normal operational conditions, DDS sends a DRN to PO.DAAC's primary server, which in turn, retrieves AMSR L1A files from DDS and sends an RCN to DDS. DDS will detect a failure of PO.DAAC's primary server when no RCN is received within a specified time out period (currently 1

hour) is exceeded. When a failure is detected, DDS will resend the same DRN, and future DRNs, to PO.DAAC's secondary server. In the meantime, PO.DAAC's operator and/or system engineers will correct the problem with PO.DAAC's primary system. After the problem is corrected the PO.DAAC operator (or system engineer) will contact the DDS operator by E-mail, FAX or telephone and request that DRNs are sent to PO.DAAC's primary server.

If both PO.DAAC's primary and secondary servers fail, the PO.DAAC operator will inform the DDS operators of the expected down time. If the down time exceeds 7 days, then DDS will send data via tape media, as specified in the backup procedures (section 6).

If PO.DAAC does not receive a DRN from DDS for over 24 hours and if the PO.DAAC operators have received no communication from the DDS operator, PO.DAAC will assume DDS is in backup mode. PO.DAAC operators will then contact the DDS operator for a DDS status report.

5.6 NOAA

NOAA uses hot failover. NOAA has two file servers, adeosfs.nascom.nasa.gov and a hot backup adeosfsb.nascom.nasa.gov. NOAA is set up to respond to DRNs from DDS and FASTCOPY push from CSAFS, ASF/SAFS and PODAAC.

In the case where DDS sends a DRN to the primary server adeosfs, and adeosfs is down, the DDS will time out. DDS will then resend the same DRN to the hot backup adeosfsb, which will perform the get/mget of the file(s), and send an RCN. In case the second DRN times out, the DDS operator will notify the NOAA operator by FAX or telephone. The NOAA operator will initiate a manual procedure to rectify the condition.
If EOC/DDS goes down, the NOAA server will do nothing in response; it will simply wait for DDS to come back up.

There are no files sent from NOAA to DDS directly, so the NOAA computers do not need to send DRNs. Agencies pushing files using FASTCOPY will send the files to the backup secondary when they are unable to reach the primary. In case both the primary and the secondary are down, a FDN will notify NOAA operation to fetch the files.

6. MOIF Backup Operation

If any trouble transferring MOIF files has occurred, and it takes a long time (> 24H) to repair, backup operations will be utilized. This section describes details of backup operations.

6.1 Backup Operations Overview (applies only to MOIF file transfers)

6.1.1 InetB

When the primary (ATM) circuit between EOC and NASA/NOAA fails, EOC will switch to InetB as a backup after consensus among operators. Following is the InetB procedure:

(1) The sender sends the files as attachments to E-mail via the Internet usingEudora with Return Receipt option selected.

(2) The receiver checks the contents (i.e., the file name and file size), then repliesto notify whether expected files were received successfully by E-mail.

(3) If the original sender does not receive a receipt, she/he should contact the receiver by phone.

(4) If the receiver does not receive expected information, she/he should contact the sender by phone.

The attachment should be a) a text file (the same as is sent in the DRN/RCN system); and b) a MIME attachment. (Note: For avoiding compatibility problems Eudora is designated for every InetB mail exchanges.)

Subjects of InetB are Mission Operation Information Files, and if need be, multi-file attachments are permitted.

The rules of E-mail for InetB are shown below.

(1) E-mail Address for InetB

The E-mail addresses for InetB are listed in Table 6-1.

Table 6-1. E-mail Address for InetB

Agency	E-mail Address for InetB
NASDA/EOC	Inetbkup@eoc.nasda.go.jp
NOAA/NESDIS	nesdis.osdpd.ibnet@noaa.gov
JPL/PO.DAAC	N/A
JPL/SeaPAC	operations@seawinds.jpl.nasa.gov
ASF	opsgang@asf.alaska.edu
DSMC	wsnso@mail.wsc.nasa.gov

(2) Subject field of InetB

The envelope Subject format is as follows.

```
AAAAAAAAAAA:BBBBBBBBB-CCCCCCCCC
      |          |          └ Computer ID of Receiver
      |          └ Computer ID of Sender
      └ Title
```

A. Title (11 bytes fixed)

MOIF-Backup

B. Computer ID of Sender (maximum 9 bytes)

HEOC_0701 : for NASDA/EOC

NOAA_0701 : for NOAA/NESDIS

SPAC_0701 : for JPL/SeaPAC

ASF_0701 : for ASF

WFF_0701 : for WFF

C. Computer ID of Receiver (maximum 9 bytes)

Same as above.

(3) E-mail contents for backup

Contents are free form, but must include file name with file size.

Example of Backup Transfer

Sending MOIF files from NASDA/EOC to NOAA/NESDIS

From: inetbkup@eoc.nasda.go.jp
To: nesdis.osdpd.ibnet@noaa.gov
Subject: MOIF-backup:HEOC_0701-NOAA_0701

Sending Data Name Operation plan
File Name OPLN000001
File Size 100KB

From: nesdis.osdpd.ibnet@noaa.gov
To: inetbkup@eoc.nasda.go.jp
Subject: RE:MOIF-backup:HEOC_0701-NOAA_0701

The file was received successfully.

>Sending Data Name Operation plan
>File Name OPLN000001
>File Size 100KB

6.1.2 ~~Media shipment operation~~ (Deleted)

6.1.3 How to Move to Backup Operation

If it has been determined that data transfer will not resume in a timely manner, operators will coordinate on whether to switch to backup operation. If one wants to move to backup operation, she/he will send an Initial Request to initiate the switch via e-mail with confirmation. And her/his counterpart(s) will send an Acceptance Reply iff such propose is acceptable. After the Acceptance Reply is sent both agencies may begin communicating in backup mode according to the information in Sections 6.1 and 6.2. Details for the Initial Request and Acceptance Reply are as follows:

(1) Initial Request

The initiating operator will send an initial request to his counterpart via e-mail to their InetB mail account. This request mail is free form but must include the following items, and if it is capable, return receipt request must be attached with initial requests, and if it is not capable, sender must confirm reachability by phone call.

1) Reason to switch to InetB
2) Expected response

If one dose not receives expected responses within 24 hours (TBD), one must make urging requests via phone call every 24 hours (TBD) until receiving expected responses.

(2) Acceptance Reply

The operator who receives the InetB initial request replies via e-mail to their InetB mail account if she/he agrees. The reply is free form but must include the following item, and if it is capable, return receipt request must be attached with initial requests, and if it is not capable, sender must confirm reachability of acceptance reply by phone call.

Approval for switching to InetB

6.1.4 Return from Backup Operation to Normal Operation

When it has been determined that data transfers can return to normal (ATM) operation, operators will coordinate on switching to normal operation. First, one will send a "Return to Normal" Request via e-mail with confirmation, then the receiver will send a Return to Normal Acceptance Reply if the request is acceptable. After the Return to Normal Acceptance Reply is sent both agencies will stop InetB operations. Details for the Return to Normal Request and Return to Normal Acceptance Reply are as follows:

(1) Return to Normal Request

The initiating operator will send a "return to normal" request to her/his counterpart via e-mail to InetB mail account. This request mail is free form but must include the following items, and if it is capable, return receipt request must be attached with initial requests, and if it is not capable, sender must confirm reachability by phone call.

1) Reason to stop InetB operations
2) Expected response

If one dose not receives expected response within 24 hours (TBD), one must make urging requests via phone call every 24 hours (TBD) until receiving expected responses.

(2) Return to Normal Acceptance Reply

The operator who receives the InetB "Returns to Normal" request replies via e-mail to InetB mail account if she/he agrees. The reply is free form but must include the following item, and if it is capable, return receipt request must be attached with initial requests, and if it is not capable, sender must confirm reachability by phone call.

Approval to stop InetB operation

6.2 Backup Operation Method for Each Facility

Table 6-2 shows the backup method for MOIFs, and Table 6-3 shows the NRT data backup method.

Table 6-2. MOIF (Computer_ID is xxxx_0701) Backup Method

From	To	Backup Method	Remarks
EOC	ASF	InetB	
	DSMC (WFF)	InetB	
	SeaPAC	InetB	
	PO.DAAC	N/A	
	CSAFS	N/A	
	NOAA	InetB	
ASF	EOC	InetB	
DSMC (WFF)		InetB	
SeaPAC		InetB	
PO.DAAC		N/A	
CSAFS		N/A	
NOAA		N/A	

Table 6-3. NRT (Computer_ID is xxxx_0703) Backup Method

From	To	Backup Method	Remarks
EOC	ASF	N/A	
	DSMC (WFF)	N/A	
	SeaPAC	8mm	
	PO.DAAC	8mm	
	CSAFS	N/A	
	NOAA	8mm	
ASF	EOC	D1 tape shipment	
DSMC (WFF)		D1 tape shipment	
SeaPAC		N/A	
PO.DAAC		N/A	
CSAFS		N/A	
NOAA		N/A	

7. Network Security

7.1 ADEOS-II Network Security Policy

Every ADEOS-II ground network support facility is supported by wide area and local area network connections designed to support their own unique requirements. Because of the diversity in requirements the network equipment and supporting software vary from location to location. Enforcing network security associated with network routers, servers, hosts and other information systems will require coordination and cooperation among ADEOS-II network systems administrators and users. Local network administrators will be primarily responsible for ensuring network safety and preventing hostile attacks from unauthorized sources into their respective information systems. NASA ADEOS-II ground network elements, including wide area networks, shall comply with NASA security policies defined in NPD and NPG 2810.1, Security of Information Technology. To the extent possible NASDA and NOAA facilities shall also comply with NPD and NPG 2810.1 for those systems that interface directly to NASA-provided networks and information systems.

7.2 Major network security and operation policy

This section describes the security-related operations for each facility.

7.2.1 NASDA/EOC

External users have to go through the firewall and the router, which control access to DDS. EOC rejects all access except the connection from authorized hosts. If the firewall or DDS detects unauthorized access, the DDS operator will do TBD.

7.2.2 ASF

All ADEOS-II related systems at ASF are protected by a firewall and router settings. Only mission essential services (SMTP, FTP, Fastcopy, and SecureShell) are allowed to the machines from pre-authorized hosts at external agencies. ASF follows NASA policies upon detection of unauthorized access, which includes reporting the incident to the appropriate authorities.

7.2.3 WFF

7.2.3.1 DSMC/WSC

DSMC systems are protected by a firewall on the closed IONet in accordance with NASA security regulations. Access to DSMC is allowed only to pre-authorized users.

Upon detection of an unauthorized access, DSMC follows NASA policies, which includes reporting the incident to the appropriate authority.

7.2.3.2 CSAFS

Security for the CSAFS is outlined in the official CSAFS security document, on file with CSOC. It adheres to all standard NASA and CSOC security procedures, and the only user on the system is the SAFS administrator. Upon detection of an unauthorized access, the CSAFS administrator follows NASA policies, which includes reporting the incident to the appropriate authority.

7.2.4 JPL/SeaPAC

Security at JPL/SeaPAC is accomplished by a JPL Lab-wide firewall, by authorized routing paths in JPL routers, and by a local SeaPAC firewall. Detection of unauthorized access will be reported to JPL Network Security and is subject to reporting to the U.S. Federal Bureau of Investigation.

7.2.5 JPL/PO.DAAC

JPL/PO.DAAC conforms to NASA NPD and NPG 2810.1 under the guidance of JPL IT security.

7.2.6 NOAA

1. It is assumed that all file transfers will use EMSnet unless otherwise specified.
2. Only pre-authorized hosts will be allowed connectivity to NOAA systems.
3. Only those services that are used to meet mission requirements will be implemented by NOAA adeos-II hosts.
4. Access to services implemented on NOAA hosts is configured separately for each user.
5. NOAA controls user account IDs and requires password authentication.
6. Communications to NOAA hosts via the Internet are allowed only from SwaPAC.
7. Security events detected on EMSnet by NOAA will be handled according to NOAA policy.

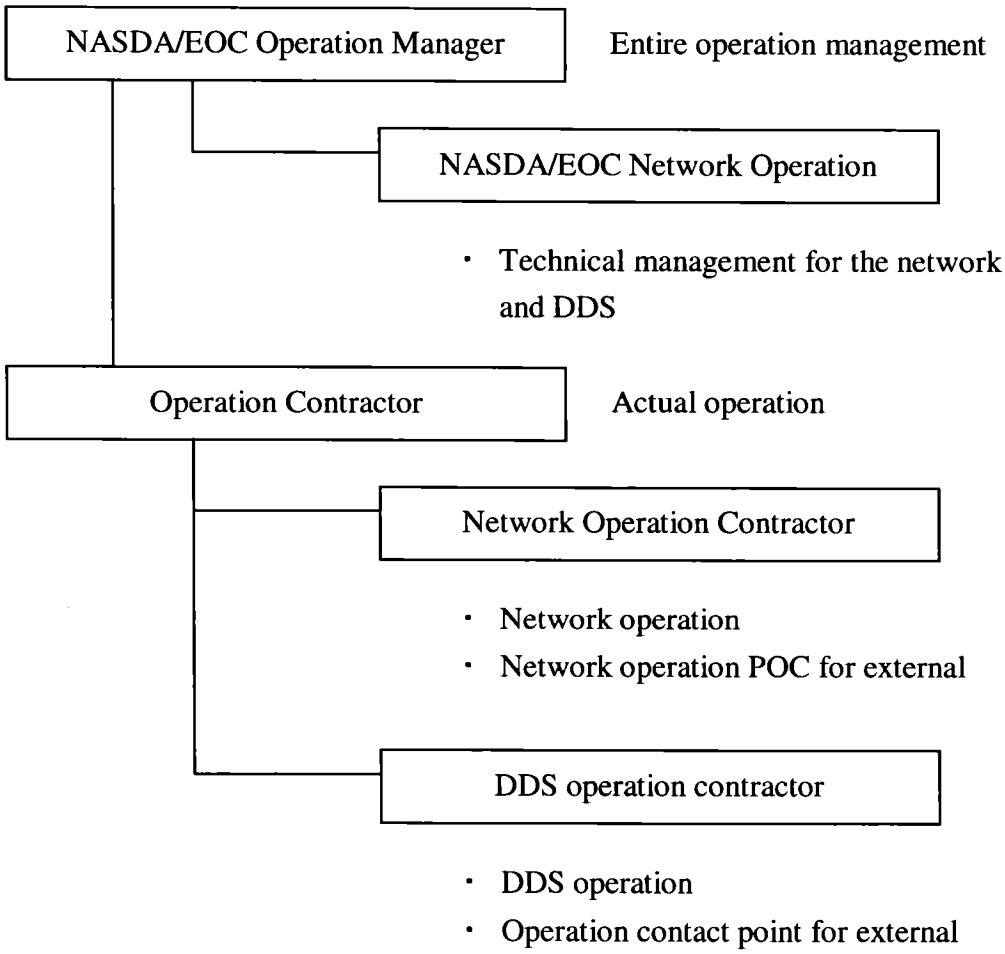
8. Operation Time and Personnel

This section describes the organization, system working time, and operator working time for ADEOS-II online data transfer operations.

8.1 NASDA/EOC

(1) Operational Organization

NASDA network and DDS operational organizations are shown below.



(2) System working time

NASDA/EOC/DDS operates 24/7 (except in case of maintenance or power outage).

(3) Operator working hours

DDS operator working hours are 0:20-8:35(UT), everyday. An EOC recording system operator also monitors the DDS 24/7. If the recording system operator detects a problem on the system when the DDS operator is not available, he/she can notify the DDS operator on call.

8.2 ASF

Operations at ASF work 24 x 7 x 365. There are eig ht operators assigned who work set shifts of 10 hrs x 4 days. Support personnel, such as engineering, system analysts, and software developers, work standard 8/5 but have personnel on call.

8.2.1 ASF (MOIF)

(1) Operational organization

Operations have eight operators. Two operators work on each 10-hour shift. They report to the Operations Center Lead

(2) System working time

The primary system is operational 24 x 7. The secondary system is a cold backup and will be brought up when necessary.

(3) Operator working time

Operators work 10-hour shifts. Each shift has two operators assigned. There are four operators on shift crossover days. These occur on Tuesday nights and Wednesday days.

8.2.2 ASF/SAFS

(1) Operational organization

Operations have eight operators. Two operators work on each 10-hour shift. They report to the Operations Center Lead.

(2) System working time

The primary system is operational 24 x 7. The secondary system is a cold backup and will be brought up when necessary.

(3) Operator working time

Operators work 10-hour shifts. Each shift has two operators assigned. There are four operators on shift crossover days. These occur on Tuesday nights and Wednesday days.

8.3 WFF

8.3.1 DSMC/WSC

(1) Operational organization

WSC Operations Manager

DSMC Lead Scheduler

DSMC Schedulers

(2) System working time

The DSMC is operational 24/7, ideally with no interruption of service at all.

(3) Operator working time

The SAFS system administrator can be reached any time by contacting the White Sands Operations Supervisor as shown in the Points of Contact Document. The SAFS administrator is generally available during normal working hours (0830-1630) US Eastern Time."

8.3.2 CSAFS/GSFC

(1) Operational organization

There is only one operator for the SAFS, the SAFS system administrator designated by CSOC. Generally, the SAFS is an automated system that requires no operator at all.

(2) System working time

The SAFS is operational 24/7, ideally with no interruption of service at all.

(3) Operator working time

The SAFS system administrator can be reached any time by contacting the White Sands Operations Supervisor as shown in the Points of Contact Document. The SAFS administrator is generally available during normal working hours (0830-1630) US Eastern Time."

8.4 JPL/SeaPAC

(1) Operational organization

There are three JPL operations personnel: a Science Processing Operator, a Science Analyst, and an Engineering Analyst. These three report directly to the SeaWinds Ground System Manager who reports to the SeaWinds Project Manager and Deputy Project Manager. If needed additional engineering support can be brought in from Project Engineering, Instrument Engineering, and Software Engineering.

(2) System working time

The JPL SeaPAC systems are operational 24/7. Hot secondary machine will receive files if primary server fails or is inaccessible because of network problems.

(3) Operator working time

JPL operations for Science Processing work a standard 8/5 shift. JPL operations for Engineering Analysis work a standard 8/5 shift, but are supplemented by automated analysis of the engineering telemetry for each file as it is received. Out-of-limit indications result in automatic paging of the Engineering Analyst to determine if there is a problem.

8.5 JPL/PO.DAAC

(1) Operational organization

JPL/PO.DAAC support for ADEOS-II consists of a system operator, a systems engineer, and a backup systems engineer. These three report directly to the PO.DAAC manager and deputy manager.

(2) System working time

JPL/PO.DAAC's operational system (OCEANIDS) is operational 24/7. This system is automated and requires minimal human interaction. If the primary system or a network fails then a hot secondary system is automatically available.

(3) Operator working time

JPL/PO.DAAC operators work a standard 8/5 shift. In the event of a system failover or anomaly condition, an automatic page is sent to either the system operator or systems engineer, who can respond to any out-of-hour problems.

8.6 NOAA

(1) Operational organization

ADEOS-II processing is designed for hands-off, script-driven automated operation. Files are obtained either via FASTCOPY push from NGN SAFS or via DRN/RCN from DDS. The planned schedule of file arrivals is derived from OPLN file.

(2) System working time

NOAA maintains a 24/7 team of operators who monitor abnormal events. Operator interface has predefined procedures for operator response. Operators can respond to FAX or telephone queries regarding the status of processing

(3) Operator working time

Operators are available 24/7. Analysts and system administrators work 8/5.

9. Points of Contact

See section 2.2 (1) for points of contact.