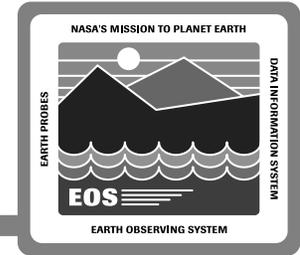


FOS Failure Recovery

Andy Miller

13 December 1994

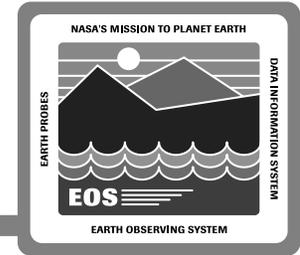
FOS Failure Recovery



Driving Requirements

- **No single point of failure for functions associated with real-time operations of the spacecraft and instruments**
- **Critical real-time functions**
 - **99.98% operational availability (99.997% design goal)**
 - **Mean downtime of one minute or less (30 second design goal)**
- **Non-critical real-time functions**
 - **99.925% operational availability (99.997% design goal)**
 - **Mean downtime of five minutes or less (30 second design goal)**

FOS Availability Assumptions



RMA data was based on generic or “Similar To” type of data

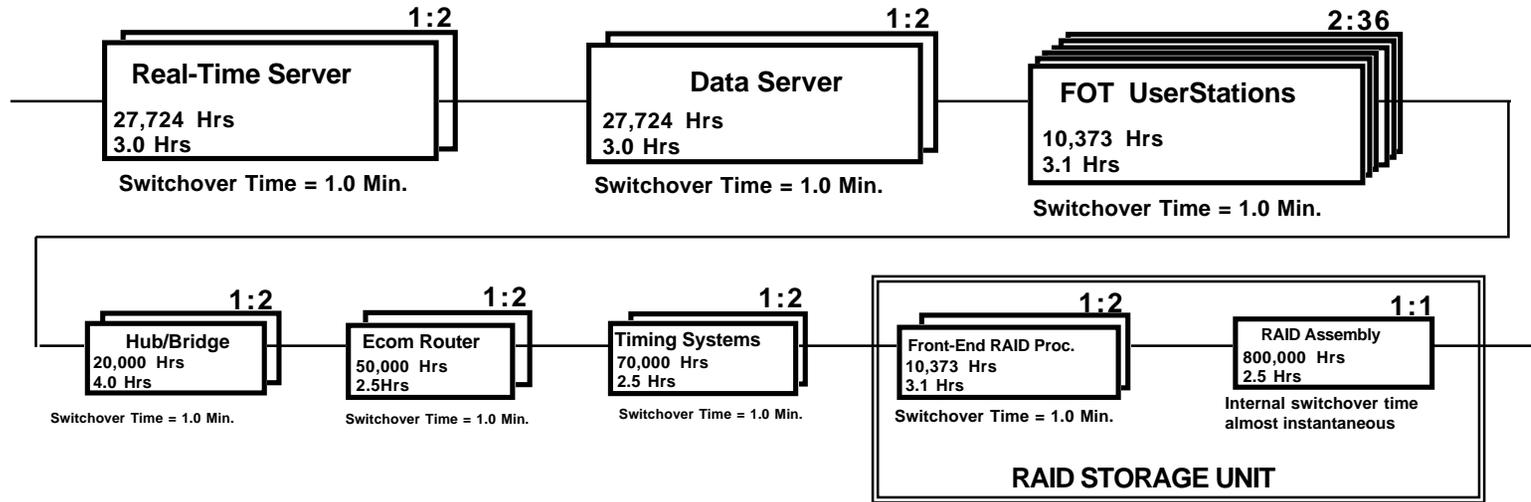
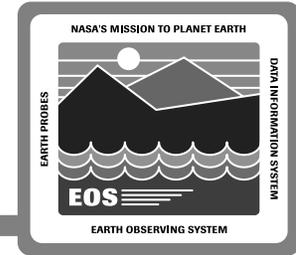
Availability results were based on software simulation

- **Using ARAM (Automated Reliability/ Availability/Maintainability) Software From Cosmic Library**

Using reliability with immediate repair model for redundant system calculation

- **Einhorn Equations**

FOS Availability Modeling Results



Release A/B FOS Critical Real-Time Functional Hardware Reliability Block Diagram

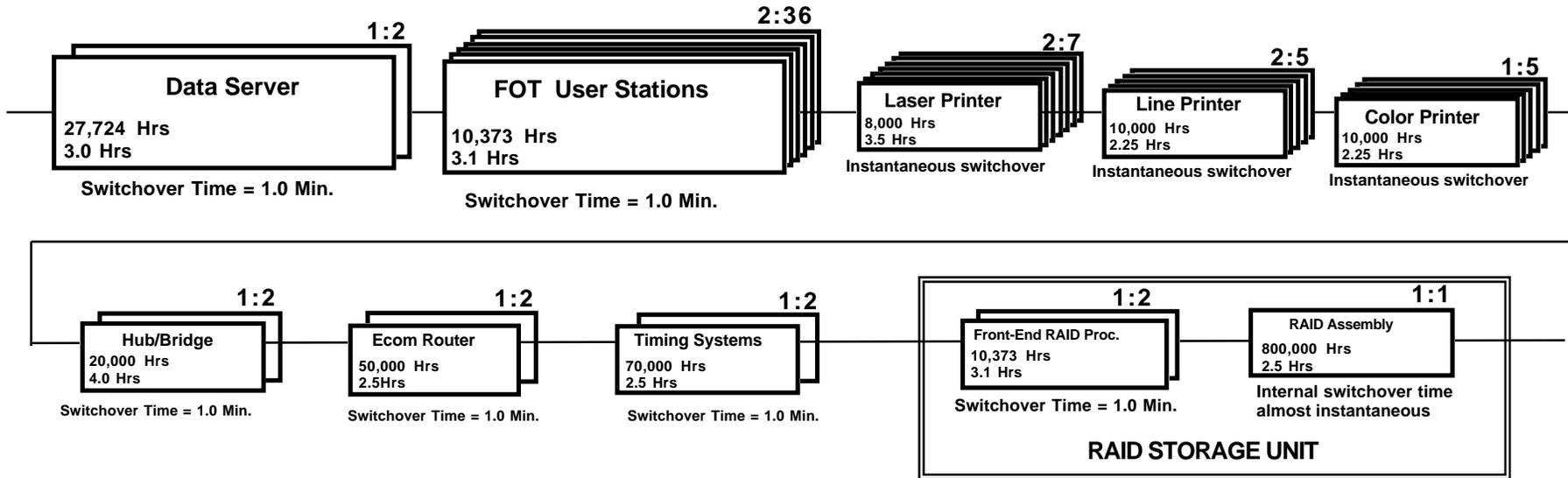
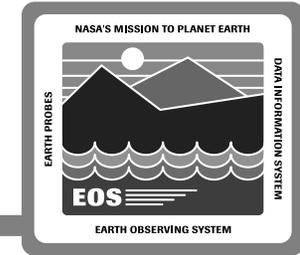
EOSD 3800: Required Ao = .99980000, MDT = 1 Min or less
 Predicted Ao = .99999970, MDT= 1.0 Min.

LEGEND:

# Required	Total
Item Description	
MTBM	
MDT	

MTBM: Mean-Time-Between Maintenance (Hrs)
 MDT: Mean-Down-Time (Hrs)

FOS Availability Modeling Results (cont.)



Release A/B FOS Non-Critical Real-Time Functions Hardware Reliability Block Diagram

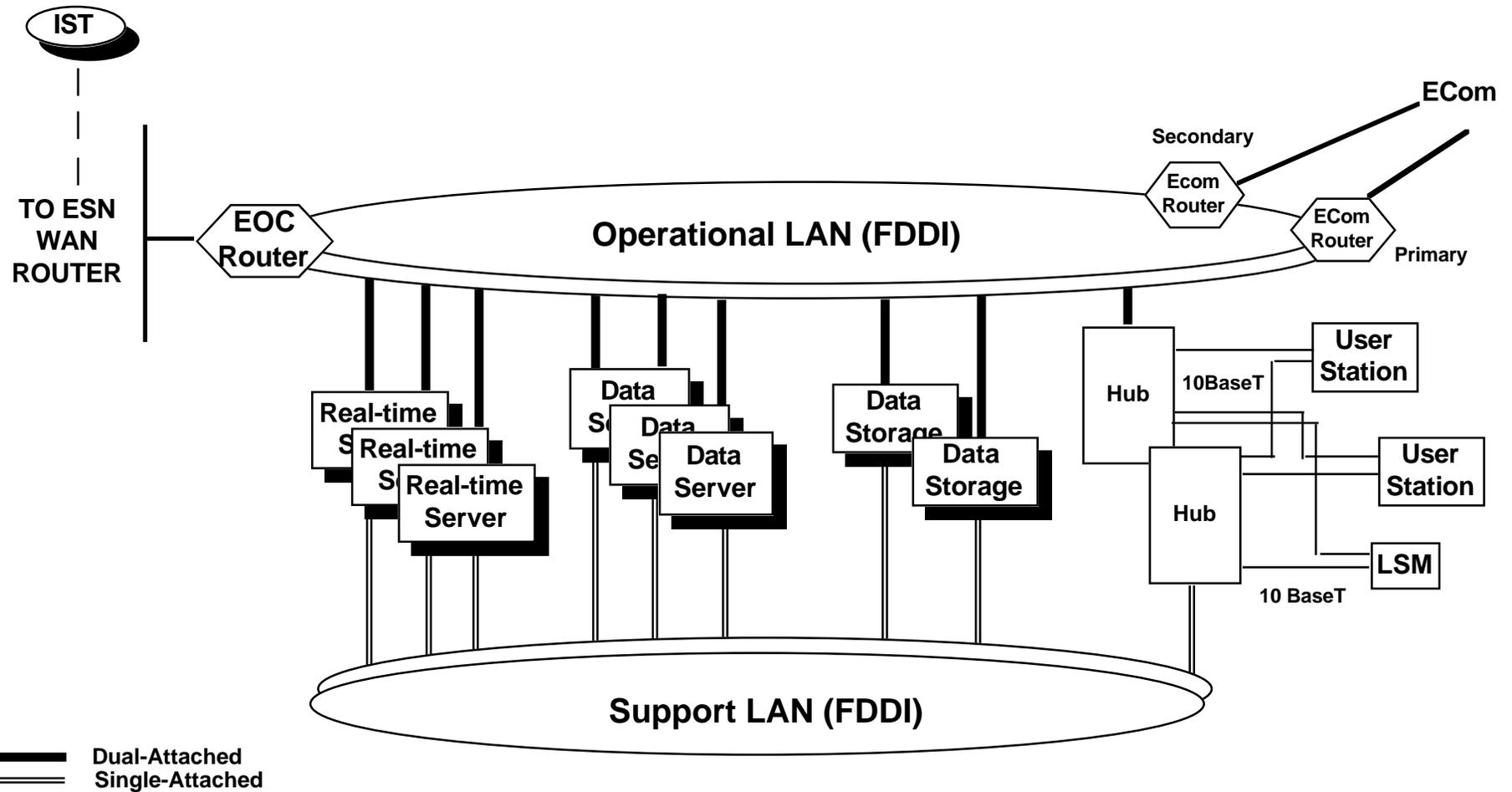
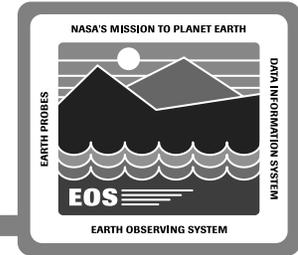
EOSD 3810: Required Ao = .99925000, MDT = 5 Min or less
 Predicted Ao= .99999960, MDT = 1.0 Min.

LEGEND: # Required : Total

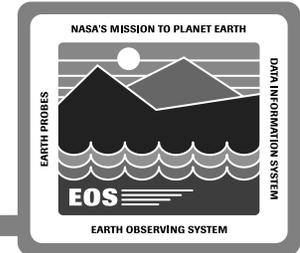
Item Description
MTBM
MDT

MTBM: Mean-Time-Between Maintenance (Hrs)
 MDT: Mean-Down-Time (Hrs)

FOS Block Diagram



Network Fault Recovery



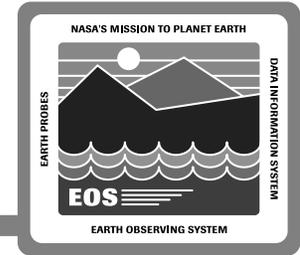
FDDI Failure

- Ring will 'wrap' autonomously with no data loss
- Applications continue as normal

Ethernet Failure

- Single User Station on segment affected
- Operator must move to new User Station and re-establish session
- No other hosts affected

Network Fault Recovery (cont.)



Hub Failure

- FDDI ring wraps and all applications continue as normal

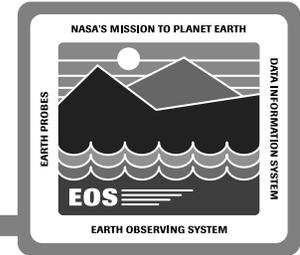
Ecom Router Failure

- Ecom will execute fault recovery plan
 - No FOS reconfiguration required

EOC Router Failure

- Router must be restored
- No FOS reconfiguration required
- ISTs will re-establish sessions

Real-Time Server Failure Recovery



Scenario

- **User Station executing the ground script, sending real-time commands via the Real-Time Server and receiving telemetry packets**

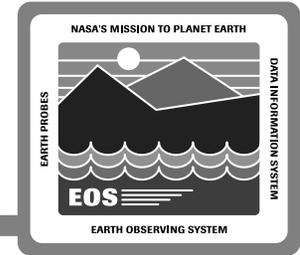
Failure

- **Real-Time Server fails**

Failure Detection

- **User detects telemetry data dropout**
- **Event message generated and displayed on the User Station**

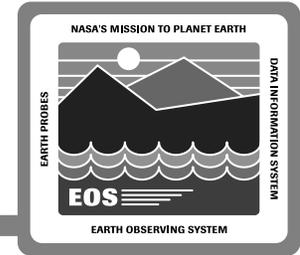
Real-Time Server Failure Recovery (cont.)



Failure Recovery

- **User requests ground configuration authority**
- **User enters directive to transfer control to the backup**
 - **Specifies Real-Time Server that is to receive control**
 - **Specifies if checkpoint information (TLM and CMD) is to be applied**
- **Backup logical string(s) are converted to active**
- **User requests command authority**

User Station Failure Recovery



Scenario

- **User Station executing the ground script and sending real-time commands via the Real-Time Server**

Failure

- **User Station fails**

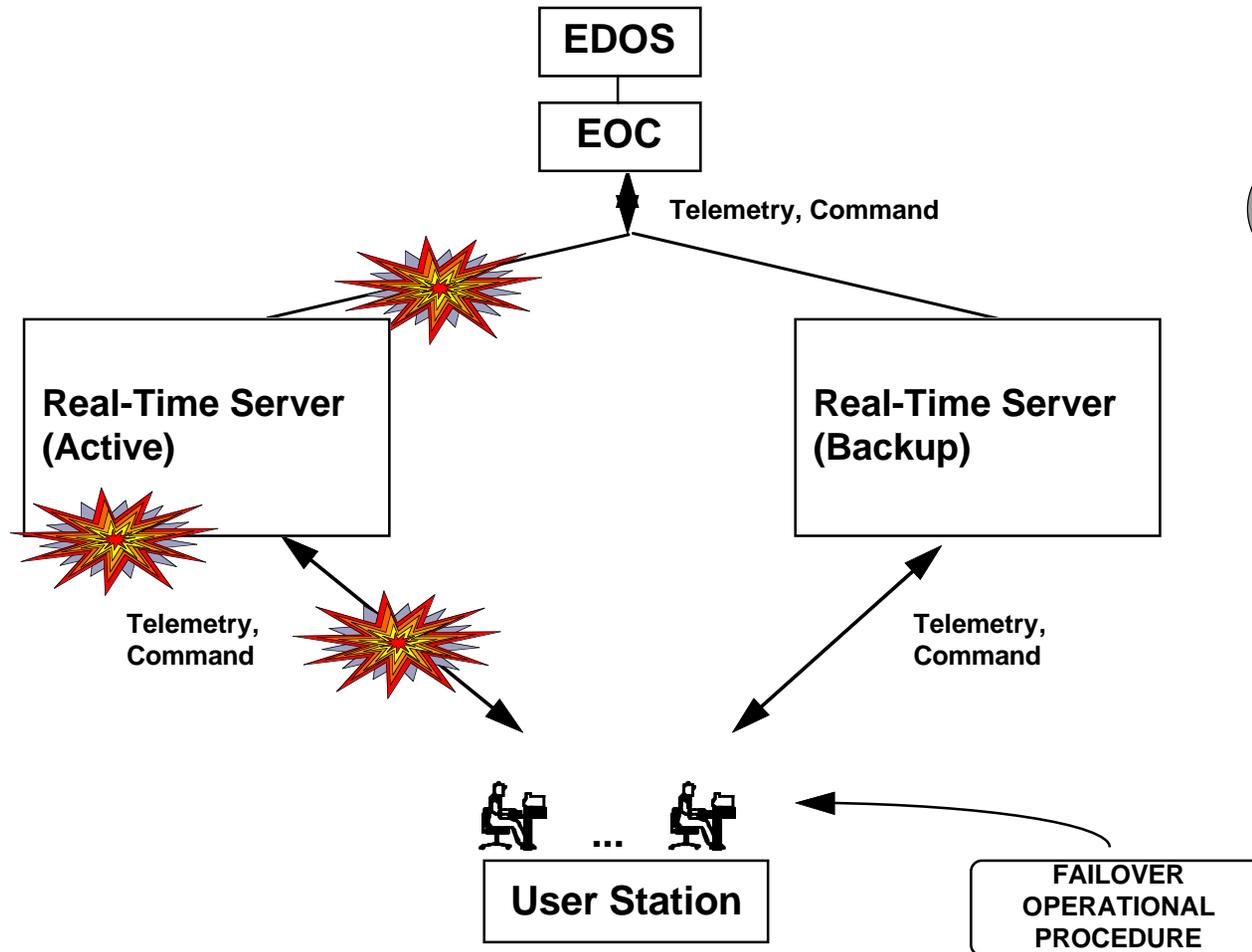
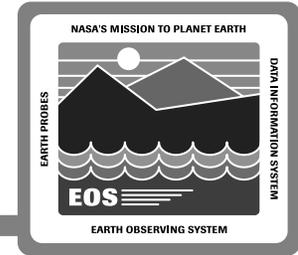
Failure Detection

- **User Station stops updating**

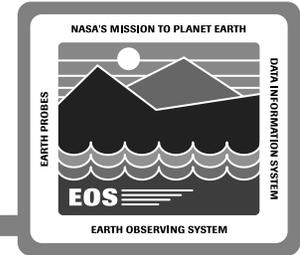
Failure Recovery

- **User switches to another User Station**
- **User requests command authority**
- **User applies checkpoint information to the ground script**

Real-Time Failure Recovery



Data Server Failure Recovery



Scenario

- **User Station requested historical telemetry for analysis purposes**
- **Data Server servicing the historical data to the User Station**

Failure

- **Data Server fails**

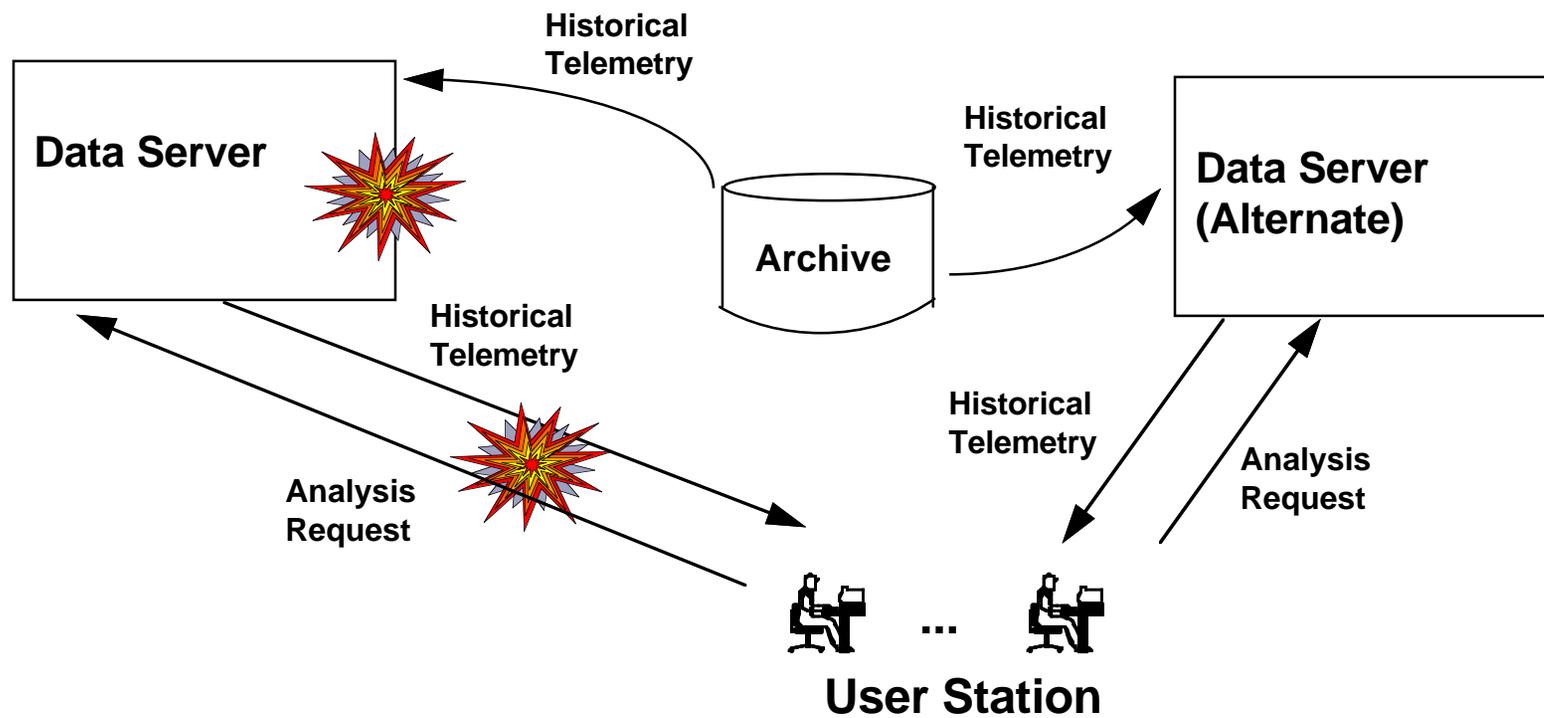
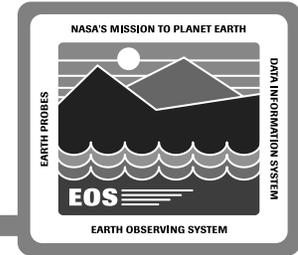
Failure Detection

- **Communication failure detected**
- **Event message generated and displayed on the User Station**
 - **User is informed how much data was processed**

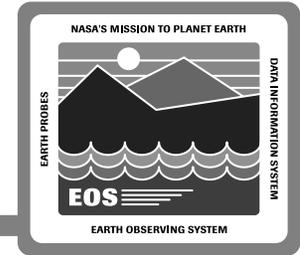
Failure Recovery

- **User sends configuration request to be serviced by another Data Server**
- **User receives historical telemetry from the alternate Data Server based on the user's request**

Data Server Failover



RAID Disk Failure Recovery



Scenario

- **User Station requested historical telemetry for analysis purposes**
- **Data Server servicing the historical data to the User Station from the Data Storage Unit (RAID disks)**

Failure

- **Disk failure**

Failure Detection

- **Data Storage Unit detects the failure**
 - **i.e., driver on the operating system**
- **Operator notified of the error via an event message**

Failure Recovery

- **Other disks in the RAID utilize the error correcting codes to access the data, which was stored on the faulty disk**
- **Physically replace the unit**
 - **Operating system rebuilds the disk with the error correcting codes**