IT Security Plan for IMAGE/LENA

Summary of Critical Functions

Overall responsibility for all LENA operational and data issues lies with the LENA co-investigator, Thomas Moore, Code 692, Goddard Space Flight Center, Greenbelt, Maryland 20833, (301) 286-5236.

Monitoring the health of the instrument: Timely receipt of the LENA real time data stream (via GSEOS) is critical during instrument commanding exercises involving the high voltage power supplies. Commanding of this type is required very infrequently and only during instrument restarts. Universal Data Format (UDF) data files are important for monitoring quickly changing conditions at the spacecraft due to extreme geophysical conditions. This additional level of monitoring is required several times per year. Level Zero (LZ) and UDF data files are important for the routine daily monitoring of instrument health.

Generating command sequences: LENA instrument team software exists for generating instrument specific commanding sequences (STOL procedures) and for analyzing orbital parameters for the optimal timing of commands. Routine daily or weekly commanding is not required for LENA operation. Periodically, special operations commanding may be performed by generating and submitting weekly STOL command files; these files are typically generated by the LENA instrument scientist, Michael Collier, or the LENA instrument engineer, Michael Johnson. This occurs approximately three months of the year.

Transfer of commanding sequences to mission operations personnel: STOL command files, once generated, can be transferred to the IMAGE operations team by a variety of means. Routine transfer is by email to IMAGE operations personnel (mtapley@swri.edu and richard.burley@gsfc.nasa.gov). This method is the most reliable. Commanding has also been accomplished in the IMAGE operations center by LENA staff conveying verbal and written commands to IMAGE flight console personnel. Additionally, commands have been conveyed from the LENA instrument scientist or engineer to flight operations personnel via telephone. These methods are not considered to be error-free and therefore used only when necessary.

Maintenance of support equipment: Development, support and maintenance of LENA supporting hardware and software is the responsibility of the LENA participating scientist, Barbara Giles, the LENA software administrator, Judith Johnson, and the LENA lead programmer, Evelyn Lee Ho.

Summary of Other, Non-Critical But Important Functions:

The IMAGE/LENA team is also responsible for the supply of analysis software, graphic files and associated data dumps to the various LENA and IMAGE science teams. LENA data analysis, display, and data download software resides on a Sun Ultra 60 (goewin.gsfc.nasa.gov) which acts as the primary processing machine and web server. An attached RAID system supplies storage for the graphics, LZ and UDF data files. Various minor Sun workstations and/or desktop machines support commanding or development work (xombul.gsfc.nasa.gov, pcmaj.gsfc.nasa.gov, and iis1990537.gsfc.nasa.gov). Primary responsibility for the maintenance of these servers resides with the LENA software administrator, Judith Johnson.

LENA Backup and Recovery Policies:

The LENA team has general policies in place that apply to all the servers and software under its responsibility.

All servers and workstations are maintained according to the regulations and directives of GSFC IT security policies. The responsible GSFC system administrator is Jennifer Ash-Poole.

All information content on the GSFC server supporting LENA is backed up on a weekly schedule under the direction of Thomas Vollmer. The most current tape backups are stored in an office area separate from the computer systems (Building 2, room S101). Older backup sets rotate to an office area in Building 23 and an off-site location. Full backups are performed weekly, rotating through 4 sets of tapes. There are 3-month, 6-month, 9-month, and yearly sets of tapes stored for retrieval of old information if necessary. The backup tapes are readable with the Unix ufsrestore command. The Level Zero data also reside on DVDs which serve as additional backup.

At least quarterly, a restore is performed from the backup tapes to verify backup integrity.

Passwords for key machines and accounts are held by at least two people. Root passwords for the server and important workstations are known to both the system administrator, Jennifer Ash-Poole, and the software lead, Judith Johnson. Passwords to key software and analysis accounts are held by Evelyn Lee Ho and Richard West.

For critical instrument monitoring and commanding functions: Software (IMAGE GSEOS) to receive the LENA data stream resides on two PCs in GSFC's building 2 (pcmaj and iis1990537) and can be used on either machine at will. This software is also on several computers in the IMAGE Spacecraft Mission Operations Center (SMOC) in GSFC's building 3 and the instrument engineer, Michael Johnson, maintains off-site access to IMAGE GSEOS for remote monitoring of LENA instrument health.

For data service functions: Recovery of data services will be provided by the use of backup tapes to restore data download/production processes to existing or newly procured servers. Restoration of the files from tape could be accomplished in a day or two and any minor adjustments due to recent modifications would require approximately 1 man-week of an experienced senior programmer's time.

Documentation: LENA software is documented in the following electronic manuals:

LENA User's Guide
Programmer's Reference Manual/Detailed Design Document
LENA Data Production User's Guide
Goewin Web Server Statistics Generator User's Guide

These manuals are available through the LENA web server (http://lena.gsfc.nasa.gov), are included within the normal backup procedures, are maintained by the GSFC lead LENA programmer, Evelyn Lee Ho, and also reside with the MSFC LENA programmer, Dick West.

IMAGE/LENA Backup and Recovery Plan:

GSFC security personnel have identified seven levels of security threat to be addressed by NASA mission security plans. Definitions of these threat levels are listed at the end of this document and at http://eiger.gsfc.nasa.gov/burst/. Backup and recovery plans to be applied for LENA, with regard to these levels of threat, are as follows:

7. Credible threat

Instrument commanding sequences can be remotely generated via network connections to the GSFC machines and submitted to the GSFC SMOC via normal email channels. The instrument scientist and instrument engineer maintain off-site network access for this function. In addition, the instrument engineer, Michael Johnson, maintains off-site access to IMAGE GSEOS data for remotely monitoring instrument health.

Most science data processing and data access procedures are automatically performed by the GSFC server. Service to these should continue uninterrupted even in the event of an absence of IT system personnel. Some maintenance can be performed by remote access by the GSFC system administrators and the MSFC LENA programmer.

6. Data loss/corruption

Recovery of software, data, and data processing functions can be provided by the use of backup tapes and existing or newly procured servers. Backup tapes stored off-site are available if access to the center stored tapes is not possible.

System and software backup procedures should be adequate such that LENA ground system machines could be restored or duplicated within 1 day to 1 week time depending on the extent the machines are affected and the availability of experienced personnel, hardware, and space resources. New servers and a DLT tape drive for a temporary facility could be acquired in approximately one week or tapes could be shipped to the MSFC LENA programmer for use on borrowed servers.

Replacement of the primary GSFC server, data archive and commanding PCs would cost approximately $100k.

Instrument commanding sequences can be remotely generated until the GSFC machines are restored. It is also possible, though not optimal, to command the instrument from within the GSFC mission operation center if experienced LENA commanding personnel have access to that facility.

5. Loss of one or more critical systems
same as above

4. Extended power outage/cyber attack
same as above

3. Localized destruction or contamination
same as above

2. Widespread destruction
same as above

1. Complete devastation

a. Including substantial loss of life

The LENA instrument scientist and the LENA instrument engineer at GSFC have unique and primary knowledge of instrument behavior and safe commanding procedures that co-investigators do not. However, in the case of loss of experienced personnel at GSFC, instrument commanding can be competently assumed by the IMAGE/LENA co-investigator at the University of Maryland (Douglas Hamilton). Data serving and programming responsibility can be resumed at a temporary site by GSFC personnel or can be assumed by MSFC under the supervision of IMAGE co-investigator Dennis Gallagher and LENA programmer, Dick West. Commanding of the instrument occurs infrequently so that loss of this capability during a transition period should not be critical. Basic LENA command information is available at the IMAGE SMOC (GSFC, building 3) or the IMAGE operations area (SWRI); either of these groups could issue emergency commands if necessary. Transfer of programming or command responsibility to MSFC or SWRI would require additional funding at those institutions equal to that supporting the GSFC personnel replaced (approx. 2 man-years).

b. Little or no loss of life

same as above

Contact Information:

Thomas Moore/GSFC/(301) 286-5236
Barbara Giles/GSFC/(301) 286-0447
Michael Collier/GSFC/(301) 286-5256
Michael Johnson/GSFC/(301) 286-3170
Evelyn Lee Ho/GSFC/(301) 286-1487
Richard West/MSFC/(256) 961-7657
Jennifer Ash-Poole/GSFC/(301) 286-9650
Judith Johnson/GSFC/(301) 286-4888
Dennis Gallagher/MSFC/(256) 961-7687
Douglas Hamilton/UMD/

Threat Definitions

Last revised: 11/14/01 (from http://eiger.gsfc.nasa.gov/burst/)

1. **Complete devastation** – Involved institution is entirely, or nearly entirely unusable, whether because of destruction of facilities or contamination with long-lasting agents (*e.g.* radioactive materials). This condition is likely only in the event of a terrorist-type attack, hurricane, tornado or an earthquake.

Including substantial loss of life – devastation occurred during a prime, weekday shift; critical oversight as well as operations personnel lost

b. **Little or no loss of life** – devastation occurred during night/weekend shift or after evacuation of personnel; critical operations could be resumed at remote sites if surviving personnel were able to relocate

2. **Widespread destruction** – Several critical facilities (*cf.* list of critical facilities) inoperable/unrecoverable, but some critical facilities still in working order, and at least some critical personnel available to continue operations. This level of destruction could be caused by a smaller-scale terrorist attack or, more likely, by a smaller scale weather related disaster. This would depend on the durability of individual buildings and IT systems to the conditions imposed. Critical operations could be resumed in on-site or (more likely) remote locations.

3. **Localized destruction or contamination** – Some buildings destroyed or rendered unusable, possibly with some loss of key personnel. This condition could be caused by a tornado, by a fire or by application of chemical or biological agents to a limited number of workplaces. In either case, the affected facilities would be unavailable for an indeterminate length of time. Critical operations could be resumed in on-site locations if backup facilities were available.

4. Extended power outage/cyber attack – Due to terrorist action, natural phenomena, extreme space weather, or simple miscalculation, the electric power grid could be disabled for longer than the period covered by the diesel fuel supply for on-site generators. If widespread, such a loss of power could lead to civil disorder, making resumption of power supply or refilling of fuel supplies unpredictable. Similarly, a successful cyber attack against local area networks or the entire Internet could bring down many critical systems, with no short-term recovery options. Either of these cases would require remote, secure facilities for the resumption of critical operations.

5. Loss of one or more critical systems – Loss of critical operations facilities (*e.g.* Buildings, etc.) or power plant(s) due to physical system failure (*e.g.* water pipe bursting), extreme weather, earthquake, or terrorist/disgruntled employee/former employee action. Critical operations could be resumed on-site if backup facilities were available.

6. Data loss/corruption – Significant mission-critical, financial, or scientific data system data loss and/or corruption, due to any of 1-5, or other causes (*e.g.* sabotage or component failure). Data and software could be reproduced if verified backups were in place, on-site or off.

7. **Credible threat –** Institutional management may have to make decisions on the basis of advice from security, law enforcement agencies, and/or other national authority that it is unsafe for the non-essential workforce, or any of the workforce, to report to work. No loss of facilities, infrastructure or life may occur, but physical access to facilities is denied or limited to a small number of essential personnel.