IT Security Plan for Polar/TIDE and Polar/PSI

Summary of Critical Functions

Overall responsibility for all Polar/TIDE and Polar/PSI operational and data issues lies with the TIDE/PSI principal 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 Polar near real time (NRT) data stream is critical during instrument commanding exercises involving the high voltage power supplies. Commanding of this type takes place approximately 4 times per year. In addition, saved NRT files or quicklook data files are important for monitoring quickly changing conditions at the spacecraft due to extreme geophysical conditions or when monitoring TIDE's frequent changes to various operational limits. This additional level of monitoring is required for several days duration approximately 10 times per year. LZ data files are important for the routine daily monitoring of instrument health.

Generating routine command sequences: TIDE instrument team software exists for generating the project required, instrument specific, commanding sequences (RQL files) and for analyzing orbital parameters for the optimal timing of commands. RQL command files for routine (daily) instrument commanding are typically generated by the TIDE instrument administrator, Peggy Sloan, and verified by the TIDE instrument scientist, Paul Craven, on a weekly basis. Significant oversight to the commanding process is provided by the TIDE MSFC lead co-investigator, Michael Chandler.

Generating unique and/or prompt command sequences: When instrument commanding lies outside the routine path described above, real-time command request lists (RTC files) are typically generated by the TIDE instrument administrator, Peggy Sloan, with backup given by the TIDE instrument scientist, Paul Craven, and the TIDE MSFC lead co-investigator, Michael Chandler.

Transfer of commanding sequences to mission operations personnel: RQL and RTC files, once generated, can be transferred to the Polar operations team by a variety of means. Routine transfer is by email from the TIDE command account on griffin.msfc.nasa.gov to the spofcmd account on spof01.gsfc.nasa.gov. Commanding has also been accomplished by fax and telephone directly with flight operations personnel although these methods are not considered to be error-free and therefore used only when necessary.

Maintenance of support equipment: Development, support and maintenance of TIDE/PSI supporting hardware and software is the responsibility of the TIDE co-investigator, Barbara Giles, and the TIDE lead programmer, Peggy Sloan.

Summary of Other Non-Critical, But Important, Functions:

The TIDE/PSI team is also responsible for the supply of LZ data files, associated calibration and anslysis files, analysis software, processed data files, and graphic files to the various TIDE and Polar science teams. The team is also responsible for archiving the appropriate data products to the NSSDC. TIDE/PSI data analysis and distribution software resides on several Unix machines. The primary site is at MSFC/NSSTC (http://satyr.msfc.nasa.gov) and includes a Sun Ultra 30 as the primary data processing machine (griffin.msfc.nasa.gov), a Sun Ultra 30 as the web server (satyr.msfc.nasa.gov), a 500-count CDRom jukebox supported by a Sun Sparc10 as the TIDE LZ and summary plot archive (delphi.msfc.nasa.gov), and a backup Sun Sparc 10 workstation for commanding functions (cyclops.msfc.nasa.gov). A mirror site is maintained at GSFC (http://tide.gsfc.nasa.gov) and consists of

a Sun Ultra 60 and RAID system for all software and data service functions (goewin.gsfc.nasa.gov). The GSFC hardware is shared with the LENA instrument on IMAGE.

TIDE/PSI Backup and Recovery Policies:

The TIDE/PSI 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 MSFC and GSFC IT security policies. The responsible MSFC system administrator is Jeanette Johnson. The responsible GSFC system administrator is Jennifer Ash-Poole.

All information content on the MSFC and GSFC servers and workstations supporting TIDE/PSI are backed up on a weekly schedule. At MSFC the most current tape backups are stored by the system administrator in an NSSTC office area separate from the computer systems (where?). Older backup sets rotate to an office area in a separate building (room 375/building 4481/MSFC). Full backups of all but the archived, static data are performed monthly with incremental backups performed weekly. The MSFC archived data reside on CDRoms for which the team has multiple copies to serve as backups. At GSFC, all information content on the GSFC server supporting TIDE is backed up on a weekly schedule. 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 to an off-site location (where? still need to fill this in). Full backups are performed weekly rotating through 4 sets of tapes. 3-month, 6-month, 9-month, and yearly sets of tapes are stored for retrieval of old information if necessary. The MSFC backup tapes are 8mm. The GSFC backup tapes are DLT and are readable with the Unix ufsrestore command. At least quartly, a restore is performed from the backup tapes to verify backup integrity.

In addition, a CDRom, updated yearly, with ASCII files of all TIDE/PSI data analysis, data service and instrument commanding software resides with the Polar project scientist at GSFC.

Passwords for key machines and accounts are held by at least two people. Root passwords for MSFC-based servers and workstations are known to both the MSFC TIDE/PSI system administrator, Jeanette Johnson, and by NSSTC system administrator Bob Dean. Root passwords for GSFC-based servers and workstations are known to both the GSFC TIDE/PSI system administrator, Jeannette Ash-Poole, and by Judith Johnson. Passwords to the software and analysis accounts at both MSFC and GSFC are held by Peggy Sloan and Dick West.

For critical instrument monitoring and commanding functions: Software to receive the TIDE/PSI NRT data stream and to create commanding sequences resides and is active on two separate servers (griffin and cyclops) at MSFC's NSSTC and can be used on either machine at will. The software also resides on the TIDE/PSI server at GSFC but is used only to verify its functionality in case of future need. Because all monitoring and commanding software resides on both machines, backup and recovery for these functions can be easily and almost immediately accomplished.

For data service functions: Almost complete data service redundancy is provided, on an immediate basis, by mirroring of data and software between the GSFC and MSFC sites. Because all data and data servicing software resides on both machines, backup and recovery for data serving functions should be easily accomplished. Several automated data download/production processes would need minor software modifications if production processing needed to be switched from MSFC to GSFC at a cost of

approximately 1 man-week of our experienced senior programmer's time or 6 man-weeks of an unfamiliar programmer's time.

Documentation: TIDE software, data processing and commanding software is documented in the following electronic manuals:

TIDE Software/Data Location Summary
TIDE Commanding User's Guide
TIDE Production Software User's Guide
TIDE Web Site Summary

These manuals are available through the TIDE web servers (http://tide.gsfc.nasa.gov or http://satyr.msfc.nasa.gov), are maintained by the TIDE lead programmer, Peggy Sloan, and are included within the normal backup procedures.

TIDE/PSI 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 TIDE/PSI, with regard to these levels of threat, are as follows:

7. Credible threat

Mirroring of software functions between machines at MSFC and between MSFC and GSFC provide for immediate recovery for all mission critical functions and almost immediate recovery for the less critical data processing functions. The instrument commanding sequences can be remotely generated through the MSFC or GSFC servers and submitted to the GSFC FOT. The GSFC FOT have often provided multiple methods, or routes, for command submission. It is also possible, though not optimal, to command the instrument from within the GSFC mission operation center if experienced personnel can be transported there.

Most science data processing and data access procedures are automatically performed by the MSFC 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 MSFC system administrators and the lead programmer.

6. Data loss/corruption

same as above

5. Loss of one or more critical systems

If required, recovery of software, data, and/or data processing hardware at MSFC or GSFC can be provided through the use of backup tapes and newly procured servers. Remote downloads from the mirror site, or backup tapes stored off-site, would be used if access to the center stored tapes was not possible.

System and TIDE software backup procedures should be adequate such that TIDE ground system machines could be restored or duplicated within 1 day to 2 weeks time depending on the extent the machines are affected and the availability of experienced personnel, hardware, and space resources. New

servers and a 8mm tape drive for a replacement MSFC facility could be acquired for approximately $100k.

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 instrument scientist has unique and primary knowledge of instrument behavior and safe commanding procedures that the instrument administrator and other co-investigators do not. However, in the case of loss of experienced personnel at MSFC, instrument commanding can be competently assumed by the TIDE/PSI co-investigator at SWRI, Craig Pollock, or by the instrument principal investigator at GSFC, Thomas Moore. Data serving and programming responsibility would be assumed by GSFC. An unplanned interruption of instrument commanding may require safing the instrument for as much as one month's time. Such a move would also require additional funding at backup institution equal to that currently supporting the MSFC personnel (approx. 2 man-year). The nearly complete software mirroring between MSFC and GSFC mean that data service would be impacted only to the degree that functions would need initiation as noted above.

b. Little or no loss of life

same as above

Contact Information:

Thomas Moore/GSFC/(301) 286-5236
Barbara Giles/GSFC/(301) 286-0447
Peggy Sloan/MSFC/(256)961-7681
Michael Chandler/MSFC/(256) 961-7645
Paul Craven/MSFC/(256)961-7639
Dick West/MSFC/(256)961-7657
Jeanette Johnson/MSFC/(256)961-7650
Jennifer Ash-Poole/GSFC/(301)286-9650
Craig Pollock/SWRI/(210) 522-3978
Judith Johnson/GSFC/(301) 286-4888

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.