SEISMIC DATA ACQUISITION SYSTEM (SDAS) COMPONENT EVALUATION

Richard P. Kromer, J. Mark Harris, and Toby O. Townsend

Sandia National Laboratories

Sponsored by National Nuclear Security Administration
Office of Nonproliferation Research and Engineering
Office of Defense Nuclear Nonproliferation

Contract No. DE-AC04-94AL85000

ABSTRACT

Sandia National Laboratories has tested and evaluated the Geotech DB24 Remote Digitizer and SAIC SAN2000B Authenticator/Formatter as components of the AFTAC Sensor Site Subsystem (SSS) of the Seismic Data Acquisition System (SDAS).

Geotech DB24 tests included response to static and dynamic input signals, data time-tag accuracy and seismic application performance. Configurations tested include:

DB24	3 Channel	40 Samples per second	Geotech KS54000 Broadband Seismometer Gain
DB24	3 Channel	4 Samples per second	Geotech KS54000 Long-Period Seismometer Gain
DB24	1 Channel	20 Samples per second	Geotech 23900 Seismometer Gain

A subset of component tests was performed on multiple Sensor Site Subsystems.

The SDAS equipment is proposed for some stations that may be part of the International Monitoring System (IMS). In these cases, IMS data surety requirements and guidelines must be met for station certification. SAIC SAN2000B data surety was tested to verify correct operation in the station environment and ensure data surety requirements are met. These tests included data authentication (CD-1.1 format), intrusion monitoring, remote command authentication, and remote key management operations.

This paper describes the evaluation of the SDAS digitizer, authenticator/formatter components and performance within the subsystem.

OBJECTIVES

Introduction

The Air Force Technical Applications Center (AFTAC) is tasked with monitoring compliance of existing and future nuclear test treaties. To perform this mission, AFTAC uses several different monitoring techniques to sense and monitor nuclear explosions, each designed to monitor a specific physical domain (e.g. space, atmosphere, underground, oceans, etc.). Together these monitoring systems, equipment and methods form the United States Atomic Energy Detection System (USAEDS). The Seismic Data Acquisition System (SDAS) is part of the USAEDS program. Some USAEDS seismic stations may be included in the International Monitoring System (IMS).

Sandia National Laboratories has tested and evaluated the Geotech DB24 Remote Digitizer and SAIC SAN2000B Authenticator/Formatter as components of the AFTAC Sensor Site Subsystem (SSS) of the SDAS.

Evaluations Performed

Sandia evaluated the overall technical performance of the Geotech DB24 remote digitizer component of the AFTAC SDAS. Distortions introduced by the high-resolution digitizers were measured. Sandia also evaluated the performance of the Geotech DB24 remote digitizer as a component installed in the SSS of the AFTAC SDAS. The additional distortions and noise introduced into the DB24 by the SSS were measured. The results of these evaluations can be compared to relevant AFTAC SDAS and IMS application requirements or specifications.

Sandia evaluated the data surety performance of the AFTAC SDAS for data authentication, command authentication, key management operations, and intrusion monitoring. These tests are intended to verify correct operation of the SAIC SAN2000B Authenticator/Formatter component and the Operation and Maintenance Subsystem (OMS) in an IMS station environment.

RESEARCH ACCOMPLISHED

Geotech DB24 Remote Digitizer

The DB24 borehole remote digitizer was built by Geotech Instruments, LLC, Dallas, TX. Geotech provided ‘dsutil’ data acquisition software for the DB24 digitizer. It operated on a PC Workstation under Windows 2000 and communicated with the DB24 through a direct-connect serial connection. Data were acquired in real-time in CSS 3.0 flat-file records. GPS was provided to the DB24 using a SAIC GPS/splitter.

Testing was performed at Sandia National Laboratories Facility for Acceptance, Calibration and Testing (FACT) Site (Figure 1).

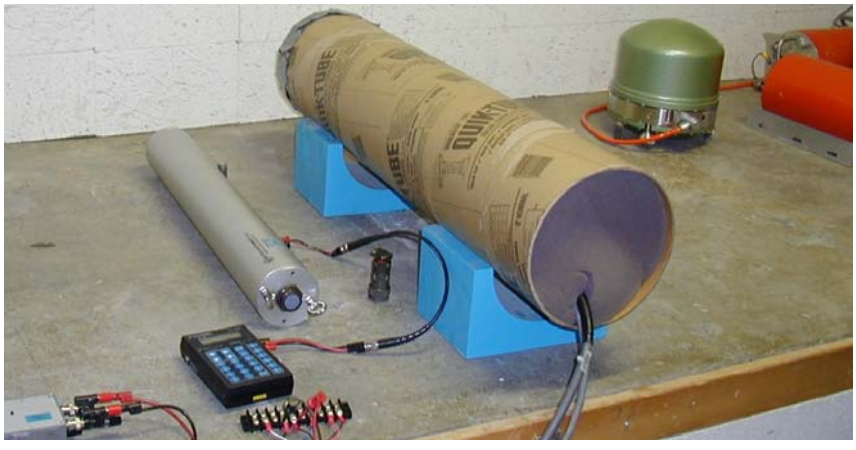

Figure 1. DB24 Testing at FACT Site

Three configurations of the DB24 were tested:

1. DB24, 3-Channel, 40 Samples per Second, Geotech KS54000 Broadband Seismometer Gain [1]
2. DB24, 3-Channel, 4 Samples per Second, Geotech KS54000 Long-Period Seismometer Gain [2]
3. DB24, 1-Channel, 20 Samples per second, Geotech 23900 Short-Period Seismometer Gain [3]

DB24 Digitizer Performance Tests and Results

The following tests were conducted on the DB24. This is a subset of tests as outlined in the Sandia Ground-based Monitoring R and E Technology Report [4].

Static Performance Tests

Input Terminated Noise (ITN) Test: Measure the Input Terminated Noise of the DB24.

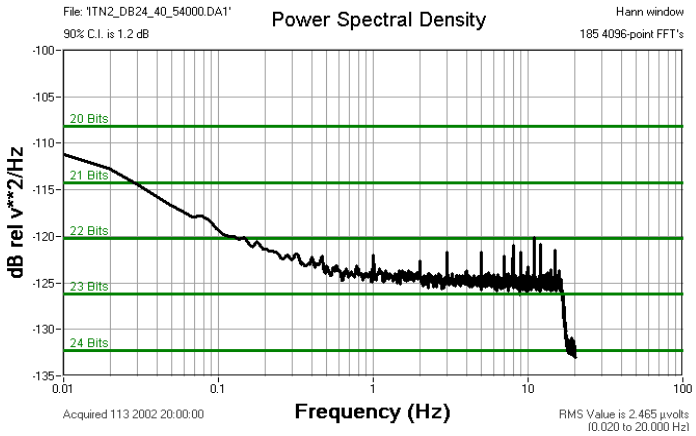

Figure 2. DB24 Channel 1 Input Terminated Noise with Integer Hz Peaks

ITN Test Results: Figure 2 indicates that the DB24 has < 0.7 count RMS noise and integer hertz spurious peaks. There is very little power in these peaks.

Maximum Potential Dynamic Range (MPDR) Test: Compute Maximum Potential Dynamic Range using data from the ITN Test.

Table 1. DB24 Channel 1-3 MPDR

Channel	RMS Noise µV 0.02 to 20 Hz	RMS Full-Scale Volts	MPDR
1	2.465	14.14	135.2 dB
2	2.474	14.14	135.1 dB
3	2.570	14.14	134.8 dB

MPDR Test Results: Table 1 indicates that the DB24 Maximum Potential Dynamic Range is greater than 134.8 dB.

Tonal Dynamic Performance Tests

Total Harmonic Distortion (THD) Test: Measure the linearity of the DB24 digitizers using Total Harmonic Distortion.

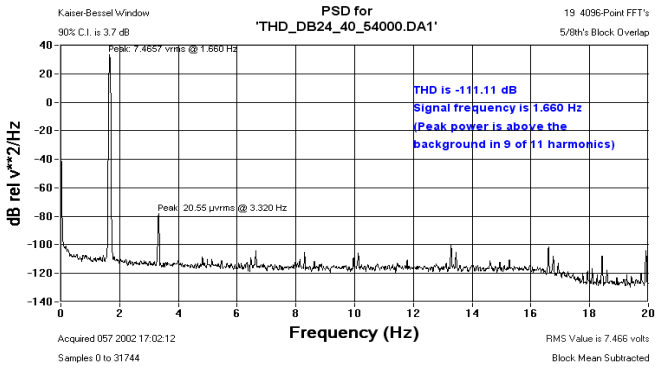

Figure 3. DB24 Channel 1 Total Harmonic Distortion

Table 2. DB24 Channel 1-3 THD

Channel	THD
1	111.11 dB
2	109.09 dB
3	109.88 dB

THD Test Results: Figure 3 and Table 3 indicate that the DB24 Total Harmonic Distortion is better than -109 dB.

Crosstalk (CTK) Test: Measure the amount of digitizer channel-to-channel crosstalk.

Table 3. DB24 Channel 1-3 Crosstalk

Channel	RMS Input	RMS Crosstalk	Crosstalk
1	4.96 V	0.51 µV	-139.8 dB
2	4.94 V	0.61 µV	-138.2 dB
3	4.92 V	0.47 µV	-140.4 dB

CTK Test Results: Table 4 indicates that the DB24 crosstalk is better than –138 dB.

Common Mode Rejection ratio (CMR) Test: Measure the ability of the digitizer to reject common-mode signals.

Table 4. DB24 Channel 1-3 Common Mode Rejection

Channel	Peak Input	Peak Common-mode	CMRR
1	10.0 V	0.512 mV	85.8 dB
2	10.0 V	0.937 mV	80.6 dB
3	10.0 V	0.197 mV	94.1 dB

CMR Test Results: Table 5 indicates that the DB24 CMR is better than –80 dB at 1 Hz.

Broadband Dynamic Performance Tests

Modified Noise Power Ratio (MNPR) Test: Determine DB24 performance using broadband signals.

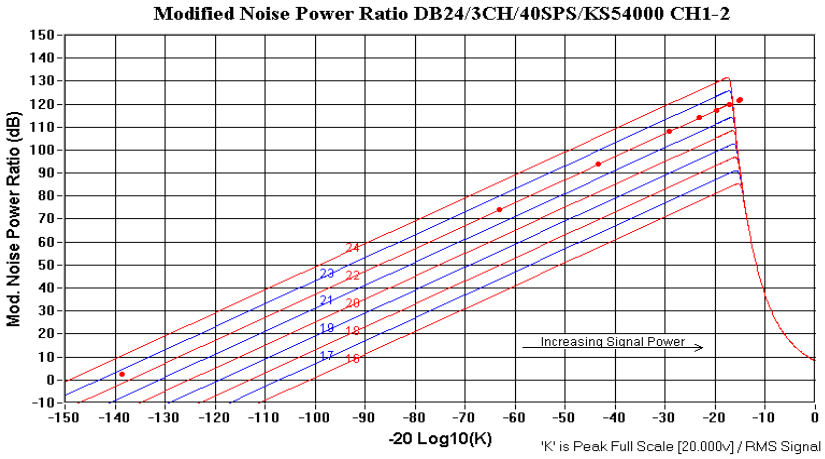

Figure 4. DB24 Channel 1-2 Modified Noise Power Ratio

MNPR Test Results: Figure 4 indicates that the DB24 has 22-bit performance using broadband signals.

Seismic Application Tests

Seismic System Noise (SSN) Test: Determine ability of the DB24 to resolve the expected seismic background using a KS54000 seismometer.

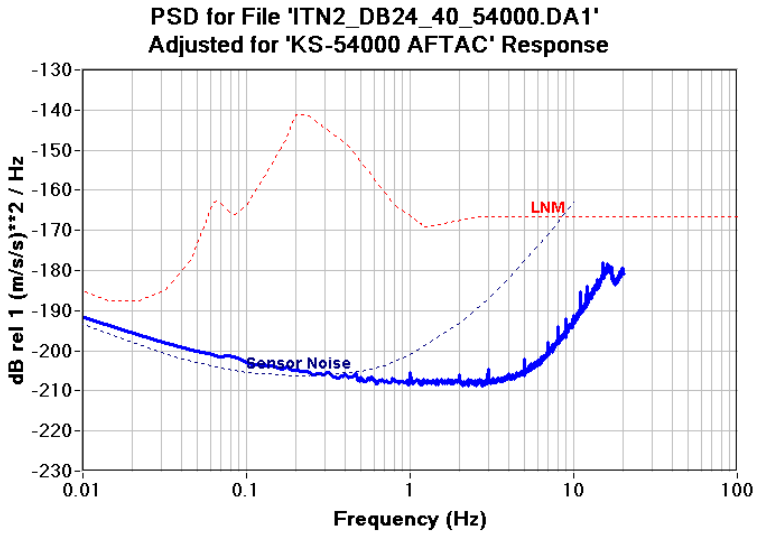

Figure 5. DB24 CH1 Seismic System Noise

SSN Test Result: Figure 5 indicates that the noise of the DB24 digitizer was at least 8 dB below the USGS New Low Earth Noise Model (NLNM) between 0.02 and 16 Hz when used with a Geotech KS54000 seismometer.

Sensor Site Subsystem - Geotech DB24 Remote Digitizer

SSS Testing was performed at the Pinedale Seismic Research Facility (PSRF) (Figure 6).

Figure 6. SSS Testing at PSRF

Three configurations of the DB24 were tested at PSRF:

1. DB24, 3-Channel, 40 Samples per Second, Geotech KS54000 Broadband Seismometer Gain [4]
2. DB24, 3-Channel, 4 Samples per Second, Geotech KS54000 Long-Period Seismometer Gain [4]
3. DB24, 1-Channel, 20 Samples per second, Geotech 23900 Short-Period Seismometer Gain [4]

Input Terminated Noise (ITN) Test: Measure SSS Input Terminated Noise on broadband DB24. Compare to FACT ITN Test.

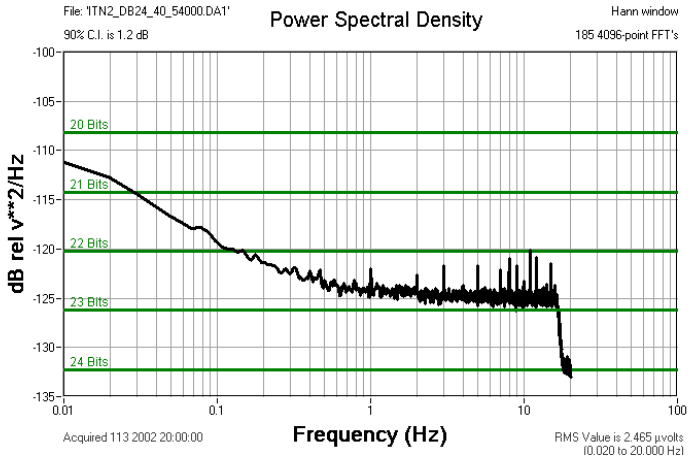

Figure 7. FACT Broadband DB24 Channel 1 Input Terminated Noise with Integer Hz Peaks

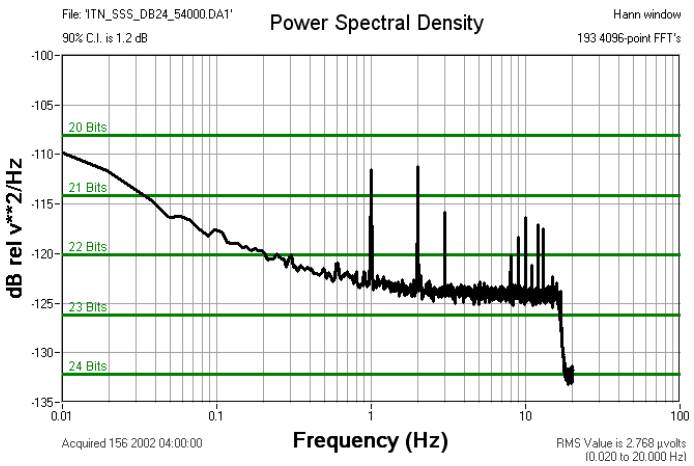

Figure 8. PSRF SSS Broadband DB24 Channel 1 Input Terminated Noise with Integer Hz Peaks

ITN Test Results: Figures 7-8 indicate that DB24 ITN testing at FACT showed < 0.7 count RMS noise with moderate integer hertz spurious peaks. SSS DB24 ITN testing at PSRF showed < 0.75 count RMS noise with increased integer hertz spurious peaks.

Input Terminated Noise (ITN) Test: Measure SSS Input Terminated Noise on short-period DB24. Compare to FACT Test.

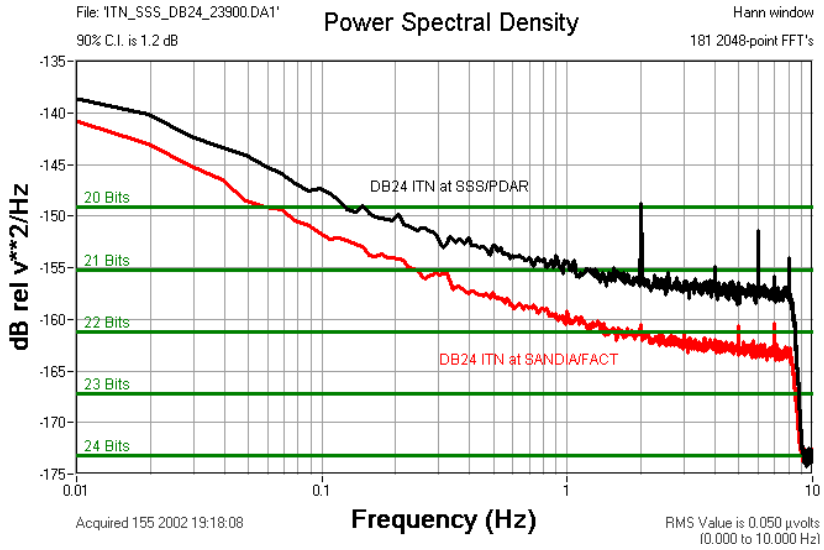

Figure 9. FACT and PSRF Short-period DB24 Channel 1 Input Terminated Noise

ITN Test Results: Figure 9 indicates that DB24 ITN testing at FACT showed < 0.95 count RMS noise with low integer hertz spurious peaks. SSS DB24 ITN testing at PSRF showed increased noise < 1.77 count RMS with increased integer hertz spurious peaks.

SDAS Data Surety

Data Surety Requirements

The PTS has developed requirements to ensure that data from IMS stations is reliable and authentic. These requirements cover data surety aspects of the station, including data authentication, command authentication, key management operations, and intrusion monitoring. Our tests are intended to verify correct operation of the SDAS equipment in an IMS station environment. IMS station data surety requirements, summarized from PTS documents [6], are listed here.

1. All IMS data must be signed at the sensor sites.
2. Data must be digitized and signed within a secure (tamper-detecting) environment.
3. Signature must be calculated within a dedicated, tamper-indicating hardware authentication device.
4. Data must be formatted for signing as specified by an approved protocol.
5. DSS (DSA with SHA-1) must be used with 1024-bit public key.
6. Signature device must generate DSA keys internally.
7. Signature device must provide public key components to user.
8. Signature device must not disclose private key directly to user or leak private key during operation.
9. Commands originating remote from the station must be signed by the originator and verified at the station.
10. A remote key change command must be supported for each authentication device; the authentication device must securely generate a new key pair and securely transmit the new public key.

The PTS strongly recommends that a PC Card device certified to FIPS 140-1 Level 2 be used for DSA operations and private key storage.

Test Configuration

The testing of the SDAS equipment described here was performed during May and June 2002. The following test environment was assembled at the Sandia National Laboratories FACT site (Figure 10, 11).

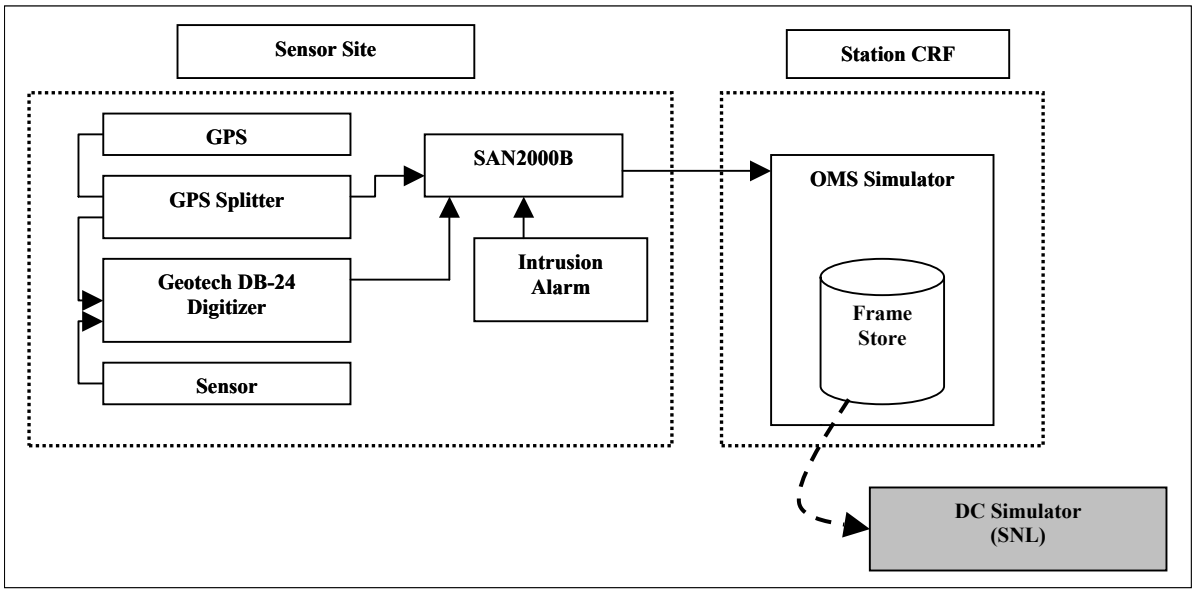

Figure 10. FACT Site Test Configuration

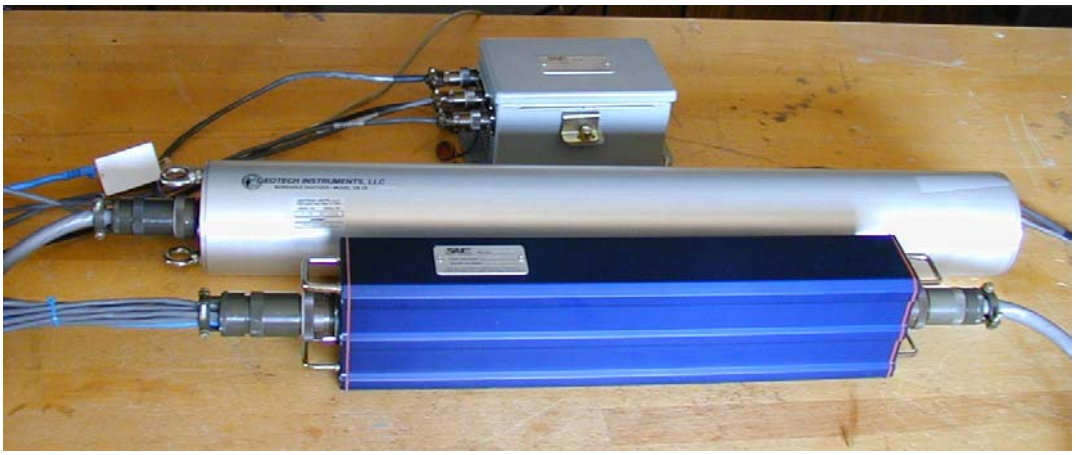

Figure 11. FACT Site Test Configuration

The DC Simulator is a computer at Sandia National Laboratories configured with software to parse the SAIC Frame Store files (the *saic_rip* program). It displays the CD-1.1 format data in a human-readable format, checks the validity of the format, and verifies authentication signatures using the *authd* program. The Station CRF is a Sun Ultra 60. Frame Store files were built on the Station CRF then manually transferred to the DC Simulator using FTP. The SAN2000B and Station CRF were connected on a 10BaseT LAN.

Data Surety Tests and Results

System Design Review Test: Determine that the SAN2000B and OMS, as part of the SDAS station environment, are designed to meet IMS surety guidelines; that system security, data authentication, and command authentication are incorporated in the equipment design and meet minimal criteria.

Test Results: The evaluation of the overall data surety of the station has not been completed. Additional system documentation is needed that describes which components sign, store, and exchange data, how commands are received, verified, and processed, how authentication keys are generated, signed, and distributed, and the physical security of the hardware components.

Data Authentication Test: Determine that the SAN2000B correctly calculates DSA signatures for sensor data in CD-1.1 format; that the station equipment transmits signed data that can be verified using the public key retrieved from the station.

Test Result: CD-1.1 data frames were successfully retrieved and parsed from the SAN2000B. The frames included the correct configuration, status information and were signed correctly. Data signatures were correctly verified using the public key retrieved from the SAN2000B. The SAN2000B has an internal Fortezza card for signature generation and public key protection. The Fortezza card is certified to FIPS 140-1 Level 2, and meets IMS guidelines for security of authentication operations. It has not yet been verified that the Fortezza card is used securely within the SAN2000B.

Intrusion Monitoring Test: Determine that intrusion detection hardware is monitored correctly by the SAN2000B; that the SAN2000B sets the appropriate intrusion flags in the signed data; that the data transmitted from the station has these flags set correctly.

Test Results: The SAN2000B correctly monitored opening of its own enclosure. External intrusion monitoring (vault/wellhead open alarm) could not be tested at the FACT Site with the hardware supplied to date. Procedures are in development to allow access to the external intrusion alarm inputs.

Remote Key Change Command Test: Determine that the key change operation works correctly on the SAN2000B and OMS.

Test Results: It was determined that the SAN2000B will generate a new key pair on command, then start to use the new key on a second command. This was tested by entering commands directly to the SAN, which uses test-mode software in the SAN. A software bug was discovered and has been reported to be fixed. It was also discovered that the key change operation is performed differently when requested from operator software on the OMS workstation. This additional OMS software is needed to test the key change operation in the station environment.

Remote Command Authentication Test: Determine that all commands issued remote from the station are signed at the remote location and verified at the station.

Test Results: SDAS command authentication has not yet been evaluated. Additional software and documentation is needed to test this function.

CONCLUSIONS AND RECOMMENDATIONS

DB24 Digitizer Performance Tests

The DB24 digitizer performed at the 21 to 22 bit performance levels depending on seismometer gain and sample rate. The moderate amount of integer Hertz noise was identified at low levels that will not be seen above the seismic background. It is recommended that the source of these spurious peaks be determined and removed if possible.

The DB24 amplifier configuration for 23900 seismometer application may be insufficient for quiet sites. It is recommended that a DB24 amplifier be developed for quiet site applications.

Data Surety Tests

At the time of this writing, several data surety tests have not been completed. Data authentication performance is acceptable, but command authentication, key management operations, system security, and intrusion monitoring require further evaluation. Additional hardware, software, and documentation are needed to complete the evaluation. We expect to receive these items soon and complete testing of the data surety of the SDAS by October 2002.

REFERENCES

Evaluation of the Geotech DB24 Remote Digitizer for AFTAC SDAS Application: DB24/3CH/40SPS/KS54000 Configuration, Ground-based Monitoring R and E Technology Report, June 17, 2002.

Evaluation of the Geotech DB24 Remote Digitizer for AFTAC SDAS Application: DB24/3CH/4SPS/KS54000 Configuration, Ground-based Monitoring R and E Technology Report, June 17, 2002.

Evaluation of the Geotech DB24 Remote Digitizer for AFTAC SDAS Application: DB24/1CH/20SPS/23900 Configuration, Ground-based Monitoring R and E Technology Report, June 17, 2002.

Test Plan for the Evaluation of Digitizing Waveform Recorder Subsystems for Ground-based Geophysical Monitoring, Ground-based Monitoring R and E Technology Report, February 26, 2002.

Evaluation of the Geotech DB24 Remote Digitizer for AFTAC SDAS Application: Multiple SSS DB24 Elements Configuration, Ground-based Monitoring R and E Technology Report, June 25, 2002.

Implementation Plan for IMS Authentication, CTBT/PTS/INF.100/Rev.1, 4 February 1999.