SRI International

20 June 1980

Quarterly Reports 1 & 2

PHASE I: HARDWARE CONSTRUCTION AND SYSTEM EVALUATION

Prepared by

E. C. May
G. S. Hubbard (consultant)

SRI International

333 Ravenswood Ave. • Menlo Park, California 94025
(415) 326-6200 • Cable: SRI INTL MPK • TWX: 910-373-1246

ABSTRACT

We have constructed a computer-based random number generator and analyzer system. Two sources of true random input were used (a β-decay source and an electronic noise diode), and special attention was devoted to insuring their independence from environmental influences. Extensive testing has shown that the system performs according to expectations, and a data sample of approximately 10^6 bits from each source meets all appropriate criteria for accepted definitions of randomness.

CONTENTS

ILLUSTRATIONS

TABLES

Approved For Release 2000/08/07 : CIA-RDP96-00788R001300180001-9

EXECUTIVE SUMMARY

General

The purpose of this program is to develop a reliable computer-based random number generator (RNG) system with graphics display capabilities. The system is designed to reduce to acceptable levels, or to eliminate entirely, external interference with the random source elements.

In order to achieve the objective of this program, we have developed a computer-based random number generator. Special efforts have been made in two specific areas: First, extensive testing of the true random sources was carried out to study their response to environmental factors. Second, a variety of statistical tests have been applied to the complete system in order to ensure that the output is truly random under experimental conditions.

We have assumed that the computer and peripheral electronic equipment will operate in conformance with manufacturer's specifications and therefore will not require additional testing.

System Description

Figure 1 shows the overall system design.

Random Sources

The random source elements consist of a commercially available noise diode, a radioactive source with an appropriate radiation detector, and a pseudorandom shift register.

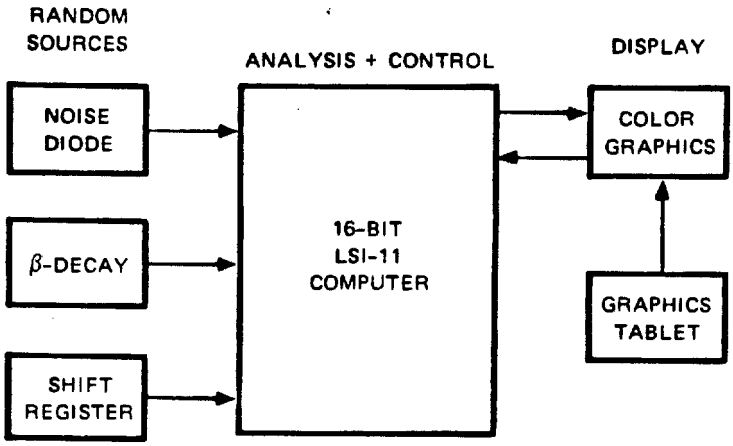

FIGURE 1 BLOCK DIAGRAM OF COMPUTER-BASED RNG SYSTEM

A Texas Instruments MD-20 planar silicon noise diode was chosen for its large noise output (~500 $\mu V/\sqrt{Hz}$) and its well-described functional characteristics.[1,2*]

^{147}Promethium was selected as a radioactive source because it is nearly a 100% β-emitter with no competing decay modes. Detection of the electron continuum is accomplished using a well-understood and reliable ORTEC silicon surface-barrier detector.

To act as a control noise source a standard pseudorandom shift register was constructed. The binary output of such a device has the property that although the sequence meets a number of criteria for randomness, the sequence is deterministic, once the starting seed for the register is given.

Figure 2 shows the process by which a random number is generated from the noise diode source. Random-amplitude 1-MHz sawtooth voltage pulses from the diode (Caption 1, Figure 2) are filtered by a bandpass filter (2).

---

*References are listed at the end of this report.

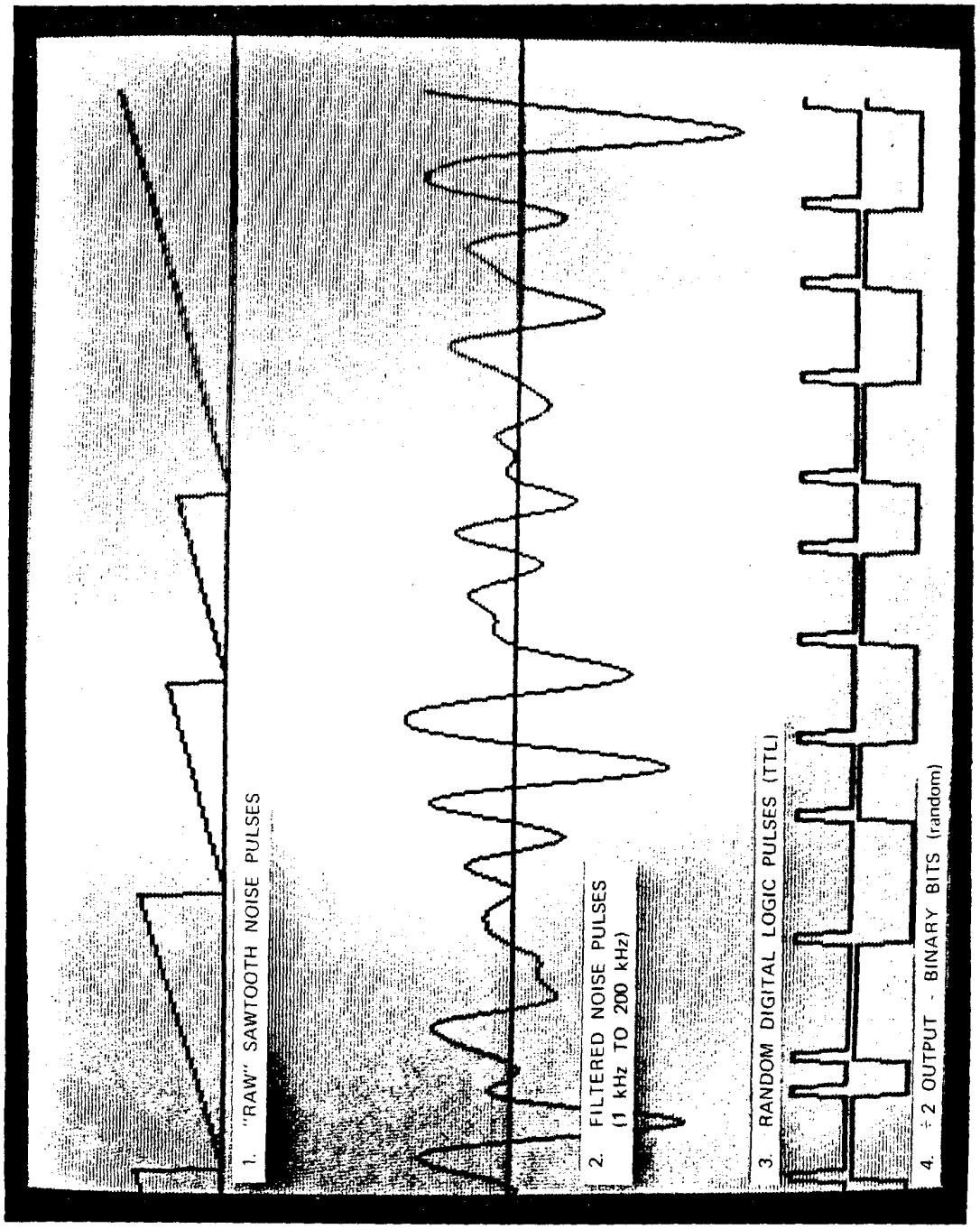

FIGURE 2 PULSE PROCESSING SEQUENCE

At each positive-going zero crossing of the filtered signal a TTL pulse is generated, giving a random digital signal (3). Finally, a divide-by-two circuit changes state at the rising edge of each TTL pulse, yielding a binary bit stream (4) with probability of being in the logical 1 state of 1/2. This bit stream is sampled and shifted into an 8-bit shift register at a 1-kHz rate, so that a random 8-bit number may be selected at intervals greater than 8 ms. A completely analogous process occurs with the β-decay source. The major distinctions are that electrons of random energy arrive at a detector where they are converted into electrical signals of random voltage. A low-level discriminator generates a TTL pulse whenever the voltage rises above a certain point. From this point, the signal processing is the same as described above.

Analysis and Control

The analysis and control portion of the system consists of an LSI-11 microcomputer. The LSI-11 is programmed to sample one of the noise sources at a specified rate to obtain its random bits. A sequence of such samples is tested by the LSI-11 for an excess or deficiency of 1's on a continuous basis, using a sequential analysis statistical technique.[3,4] Sequential analysis is extremely efficient for determining whether or not the output of the binary random generator contains a distribution of 0's and 1's as expected. The principal advantage of the sequential sampling technique as compared with other methods is that, on the average, fewer bits per final decision are required (roughly 50% fewer) for an equivalent degree of statistical reliability.

Display

The computer-driven graphics display system consists of two independent 19-inch color video monitors, a Grinnell display controller, and a Summagraphics 20-by-20-inch graphics tablet. Using these components, data from

sequential sampling statistics, pulse height analysis, or any other output may be displayed.

System Testing

Noise diodes for use in this system were extensively tested for response to changes in temperature (-40 to +40°C), leakage current (40 μA to 200 μA), and other environmental factors such as a 6000-gauss dc magnetic field and low-intensity radioactive sources (^{241}Am, ^{60}Co, ^{147}Pm). We found that over the range examined for each factor the spectral noise density was flat within ±1 dB for the bandpass of the filter (1 kHz to 200 kHz). Furthermore, the filtered noise followed a gaussian distribution under all conditions tested as long as the leakage current was 80 to 120 μA.

The random emission of electrons from the β-decay of ^{147}Pm is independent of known external influences. The element that is sensitive--the surface barrier detector--was tested for changes in leakage current as a function of temperature. At the maximum temperature tested (~40°C) it was found that the noise contribution due to the increased leakage current could be completely eliminated with an appropriate low-level discriminator.

We assume that the TTL logic circuitry and devices composing the shift register conform to the low fail rate found in the manufacturer's specifications, thus eliminating the need for further testing.

We have also assumed that the other system elements (LSI-11, Grinnell controller etc.) will continue to operate as specified by the vendor so that extensive environmental testing of these components is unnecessary.

System Isolation and Interference Protection

To prevent spurious signals due to known external influences from being incorporated into the random source output, numerous precautions have been taken. Each random source is encased in a sealed 0.125-inch-thick

soft iron box with radio frequency shielding, providing protection against mechanical, magnetic, or RF intrusion. Power is supplied by batteries to eliminate ac line transients and 60-Hz noise. All data output to the LSI-11 is via optical links to ensure complete electrical isolation. In addition, the temperature of the noise diode is continuously monitored.

Fail-safe circuits have been included in both random sources so that the units will automatically shut off and must be manually reset under the following circumstances:

- The battery supply drops below a critical point.
- The electron detector leakage current rises above an acceptable level.
- The diode current deviates from a narrowly defined-current window.

Results

A variety of fixed-length statistical tests have been applied to 500,000 sample control runs of random numbers generated by the system described above. No unexpected deviations from chance expectation were observed in these control runs, indicating that the system performs in accordance with design. The numerical results are tabulated in Section III.

I SYSTEM DESCRIPTION

A. Sources

1. Noise Diode

Commercially available random noise diodes typically have an output of < 10 $\mu V/\sqrt{Hz}$. An exception is the Texas Instruments MD-20 noise diode, which produces a noise voltage on the order of 500 $\mu V/\sqrt{Hz}$. This large noise voltage is achieved by a device design in which internal field emission initiates avalanche breakdown bursts resulting in ~1 MHz random amplitude sawtooth pulses. This diode is incorporated into a random number generator as shown in Figure 3.

Sawtooth pulses from the diode are fed into a 6-pole bandpass Butterworth filter with rolloff points at 1 kHz and 200 kHz, respectively. Filtered output goes to (1) an optical transmitter where the analog data are sent to the LSI-11, and (2) a zero-crossing detector. The zero-crossing circuit generates TTL logic pulses, creating the digital Poisson distributed output. This binary string is also transmitted to the LSI-11 via an optical channel. A platinum resistor has been bonded to the noise diode to provide temperature sensing. The resistor's temperature coefficient is extremely well characterized (T_c = 0.385 $\Omega/^{\circ}C$) and quite stable. Using a voltage-to-frequency converter, the temperature data are transmitted to the LSI-11 via a third optical link.

Power is supplied from rechargable Ni - Cd batteries. In its current configuration the unit can operate for approximately 5.5 hours before the supply voltage drops below the cutoff point. Recharge time is 10 to 15 hours. Current sensing circuitry will shut off in the system if the diode operating point falls below 95 μA or rises above 105 μA.

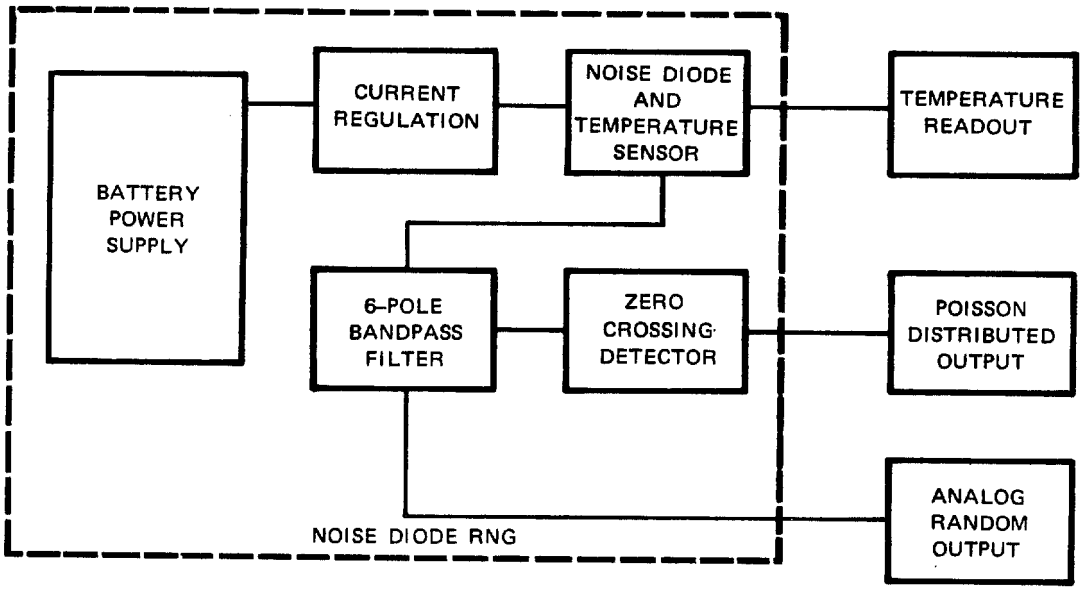

FIGURE 3 A TEXAS INSTRUMENTS MD-20 NOISE DIODE IS SHOWN WITH ITS ASSOCIATED ELECTRONICS. Each output is via optical signal coupling.

2. β-Decay

A ^{147}Pm* source of initially 5 μCi (half-life 2.7 y) emits electrons that are detected by a partially depleted silicon surface barrier radiation detector. The output of this detector is the source of random numbers, as shown in Figure 4. Using a charge-sensitive pre-amplifier, the detector signal is converted into pulses that are further shaped and amplified. A low-level discriminator passes only those events greater than 25 keV, eliminating contributions from electronic noise. The output of the amplifier/voltage discriminator is sent to (1) an optically

*^{147}Pm undergoes β-decay with a ground state branching ratio of 99.994%. The maximum and average energy electrons emitted are 225 and 60.5 keV, respectively.

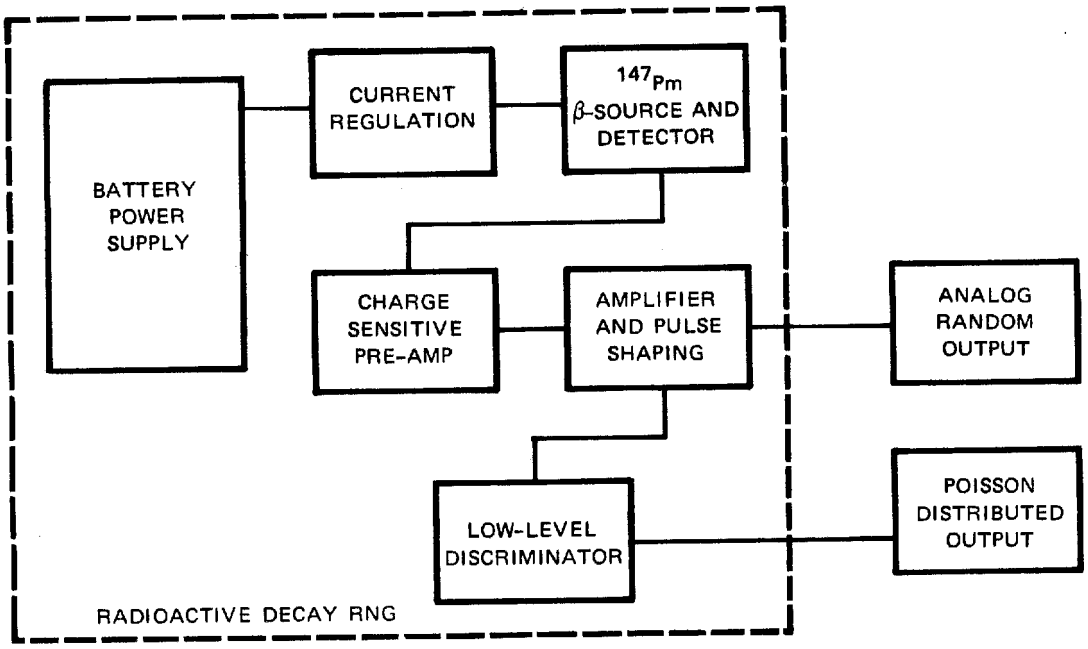

FIGURE 4 β-DECAY FROM A ^{147}Pm SOURCE IS DETECTED BY A SURFACE-BARRIER RADIATION DETECTOR TO PROVIDE A RANDOM SIGNAL. All output is via optical signal coupling.

coupled output for analog pulse height analysis, and (2) a TTL pulse generator. Each event greater than 25 keV creates a logic pulse. The output is a random binary string, Poisson distributed in time, just as in the noise diode RNG. These binary pulses are also sent to the computer by an optical channel.

Power is supplied in the same way as for the noise diode RNG. If the detector leakage current rises above 2 μA, the system shuts down.

3. Hardware Pseudorandom Shift Register

A third source of random input is that which is generated from a pseudorandom shift register. The sequences derived from such devices are well understood,[5] and the randomness properties can be specified exactly. For example, if a maximum-length binary sequence is chosen,

there will be one less excess number of binary 1's than the expected number, which is 1/2 the sequence length. Also, the length of the runs follows a decreasing geometric progression, in that the probability of finding a run of length n + 1 is half that of finding a run of length n. Lastly, the autocorrelation function of the complete sequence is only two-valued, for the zero-lag and nonzero-lag cases respectively.

To serve as a form of control, we have chosen an 8-bit register with the generating polynomial given by

$$X^6 + X^3 + X^2 + 1 \quad .$$

Starting from the initial value of 255, 255 pseudorandom numbers are generated in the order shown in Table 1.

This pseudorandom generator resides on the general interface board and can be initialized and examined under software control.

B. Analysis and Control

1. Digital Equipment Corporation (DEC) LSI-11 Microcomputer

The LSI-11 microcomputer is a standard item manufactured by DEC. It is chiefly characterized by its internal bus structure and ease of operation from both the hardware and software perspective. Because of these latter two points, LSI-11 systems have gained a wide acceptance within the scientific community.

The system consists of a number of pc boards, each with a specific function, that plug into a standard backplane. Table 2 is a list, by manufacturer, of the various subcomponents of the system. Figure 5 shows the position of the boards in the backplane, and Table 3 gives the assigned address for each I/O device.

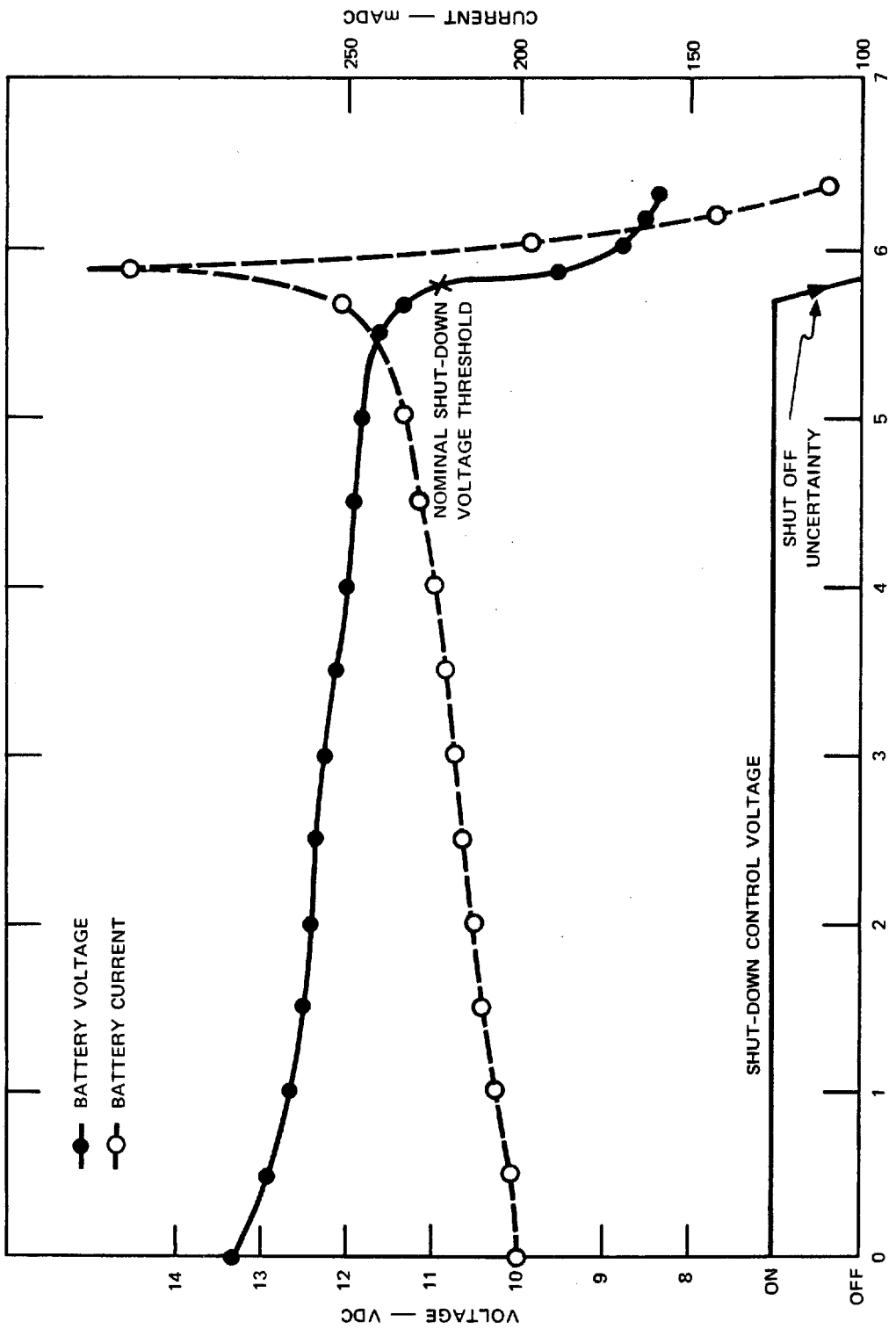

FIGURE 11 BATTERY VOLTAGE AND CURRENT AS A FUNCTION OF TIME

by rechargable Ni-Cd batteries to eliminate transients in ac supply, ground loops, and/or 60-Hz noise. The usable system time on a single charge is shown in Figure 11. After approximately 5.5 hours the voltage drops, causing the current to rise because the supply regulator is set for constant power output. At an 11-volt threshold the system shuts off automatically, requiring a manual reset before operation can continue. Additional electrical isolation is provided by the use of optical links from the RNG to the computer. All data are transmitted in this manner.

Magnetic and mechanical isolation comes from the 0.125-inch soft-iron housing in which all the RNG components are contained. It is well known that such material provides for attenuation of external magnetic fields.

An RF shield has also been installed to reduce the likelihood of penetration by high-frequency electromagnetic disturbances.

Temperature monitoring of the device is carried out via a platinum resistor. These devices are considered to be secondary temperature standards and therefore traceable to N.B.S. standards. The temperature coefficient of very pure platinum wire is extremely well known and the manufacturers specifications show very good stability. The resistance of the device is converted into a frequency that is in turn transmitted to the computer for decoding via a third optical link. Figure 12 shows that the RNG enclosure has sufficient self-heating to raise the diode to approximately 28°C over a period of 6 hours. The gaussian/white noise character of the diode output is unaffected by such a small change.

Since we have determined that optimum diode performance occurs at 100 μA leakage current, a failsafe circuit has been installed that shuts off the RNG if the device current falls below 95 μA or rises above 105 μA.

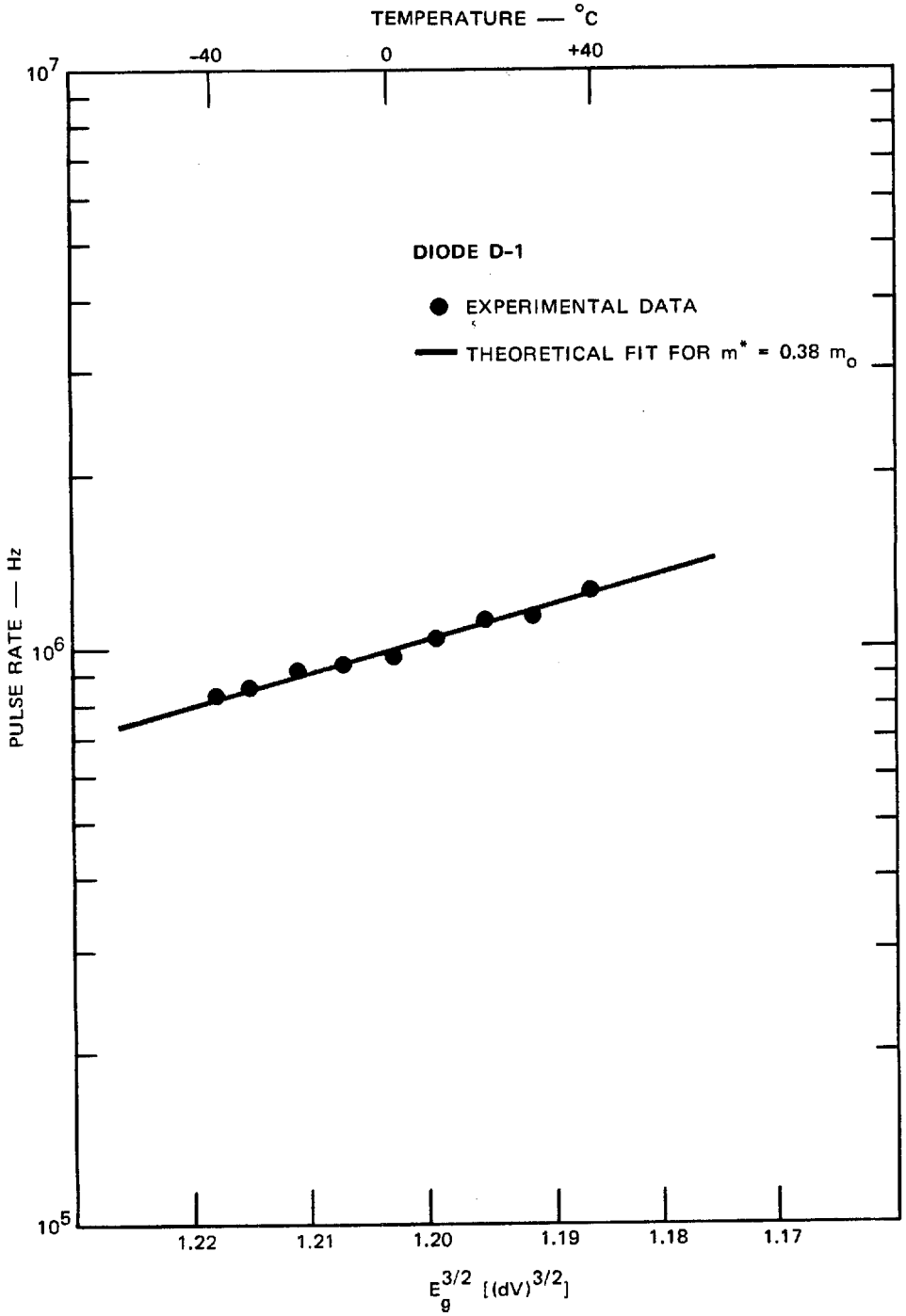

FIGURE 10 LOG OF THE PULSE RATE AS MEASURED BY FREQUENCY ANALYSIS PLOTTED AS A FUNCTION OF BAND GAP

probability for the carrier that initiates a noise pulse.[7] In turn, the temperature dependence of the pulse rate is dominated by the variation of the energy bandgap E_g with temperature:

$$N \propto T$$

where

$$T = \exp - \frac{4\sqrt{2m^*}\, E_g^{3/2}}{3q\hbar\mathcal{E}}$$

m^* = Effective mass of tunneling carrier

q = Electronic charge

$\hbar$ = Planck's constant

$\mathcal{E}$ = Electric field

E_g = Bandgap of silicon.

While this theory was never extended to high-rate (10^6 s^{-1}) diodes such as the MD-20, Figure 10 demonstrates that agreement of the principal features of the theory with experiment is still good. The pulse rate N (obtained from frequency spectra) was plotted semilogrithmically as a function of $E_g^{3/2}$. From the linear dependence of log N on $E_g^{3/2}$ it is clear that the variation in pulse rate with temperature is due to the change in E_g with temperature.

From the published data on the MD-20, the electric field in the breakdown volume can be calculated. Assuming all other parameters to be well known, the best fit to the data in Figure 10 is obtained with an effective mass = 0.38 ± 0.01 m_o, which is of the same order as the accepted values for effective masses in silicon.

2. System Isolation and Monitoring

To provide for system integrity under various environmental conditions, a number of isolation steps have been taken. Power is supplied

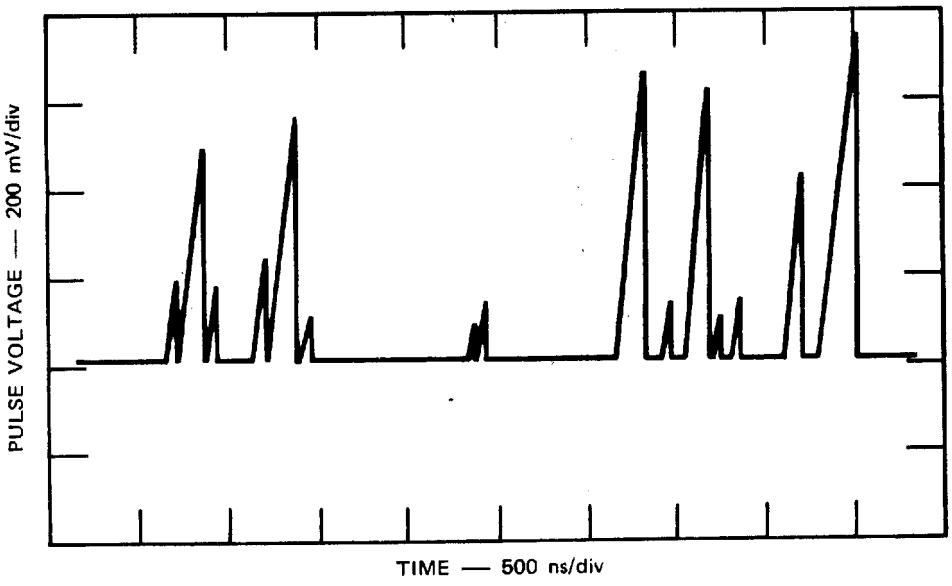

FIGURE 9 REPRESENTATION OF SINGLE-SWEEP PULSE TRAIN FROM NOISE DIODE AT A CURRENT OF 150 μA

We have experimentally measured the response of unfiltered noise pulses to variations in reverse current, and have determined the mean "dead time" occurring randomly between sawtooth pulses to be:

$$\tau = 0.01 \times 10^{-9} \exp[1/1.567 \times 10^{-5}]$$

where I is in amperes, and τ is in seconds. The device response to other environmental conditions was measured by: (1) Subjecting the diode to an applied magnetic field of 6000 gauss with the junction both perpendicular and parallel to the field; and (2) irradiating the device with low-intensity ^{60}Co γ-rays (1.33 MeV), ^{241}Am α-particles (5.49 MeV), and ^{147}Pm β-radiation (255 keV max). As expected from the small junction area and device packaging, none of these variations in physical environment caused any change in either the pulse height or frequency spectrum.

In the theoretical model for the behavior of low-pulse-rate devices, the pulse rate N depends most strongly on T, the tunneling

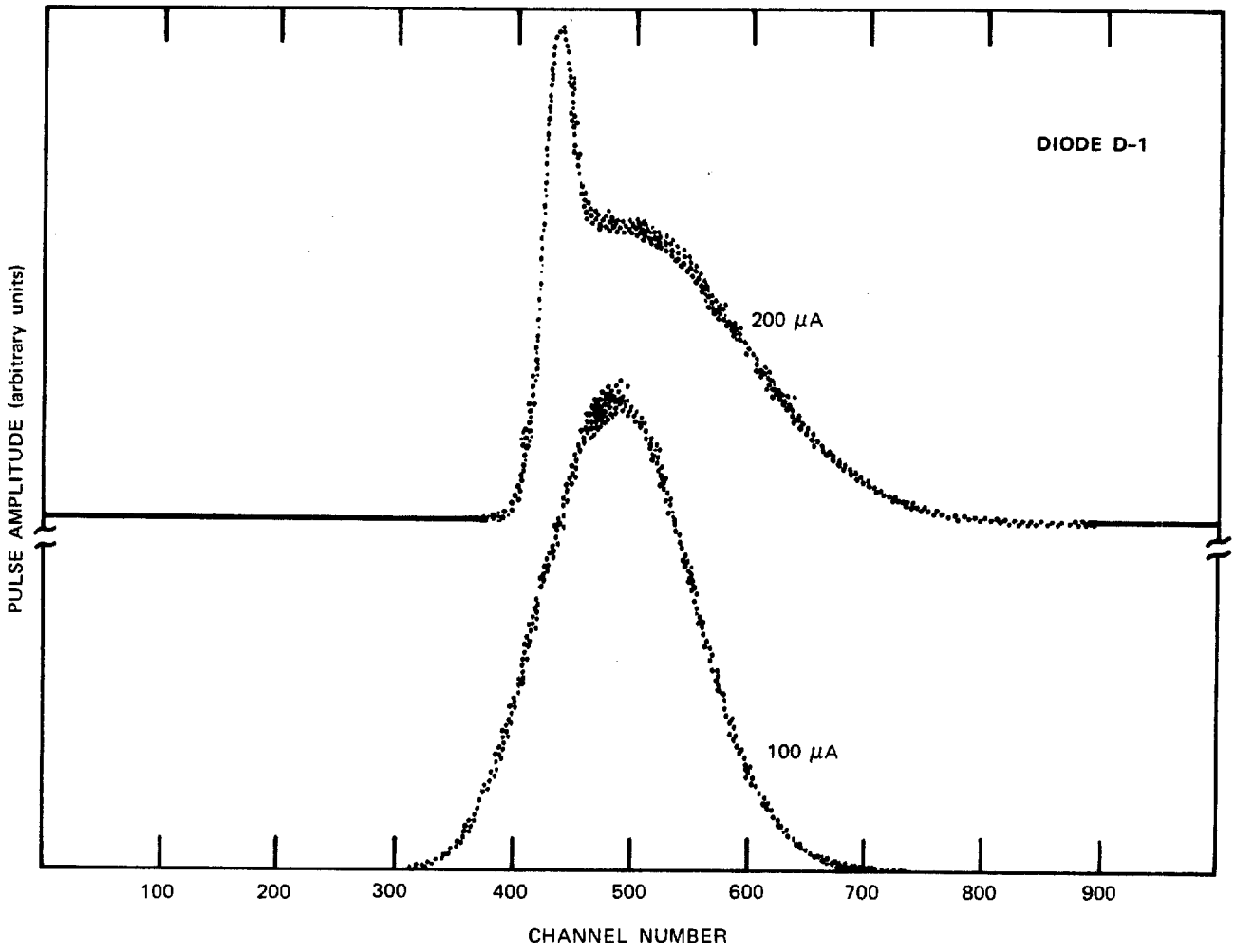

FIGURE 8 PULSE HEIGHT ANALYSIS OF DIODE D-1 AT TWO LEAKAGE CURRENT VALUES

production processes. The narrow peak on the left results from continuous carrier avalanche while the broad feature is produced by the large sawtooth noise pulses.

This picture is supported by analysis of the sawtooth pulses. At a reverse leakage of 100 μA, continuous pulse trains are observed with a fast oscilloscope. As shown in Figure 9 considerable "dead time" in the pulse train appears at a current of 150 μA. As the current increases, there is a greatly enhanced probability that the device will stay "on" in the avalanche mode after a pulse.

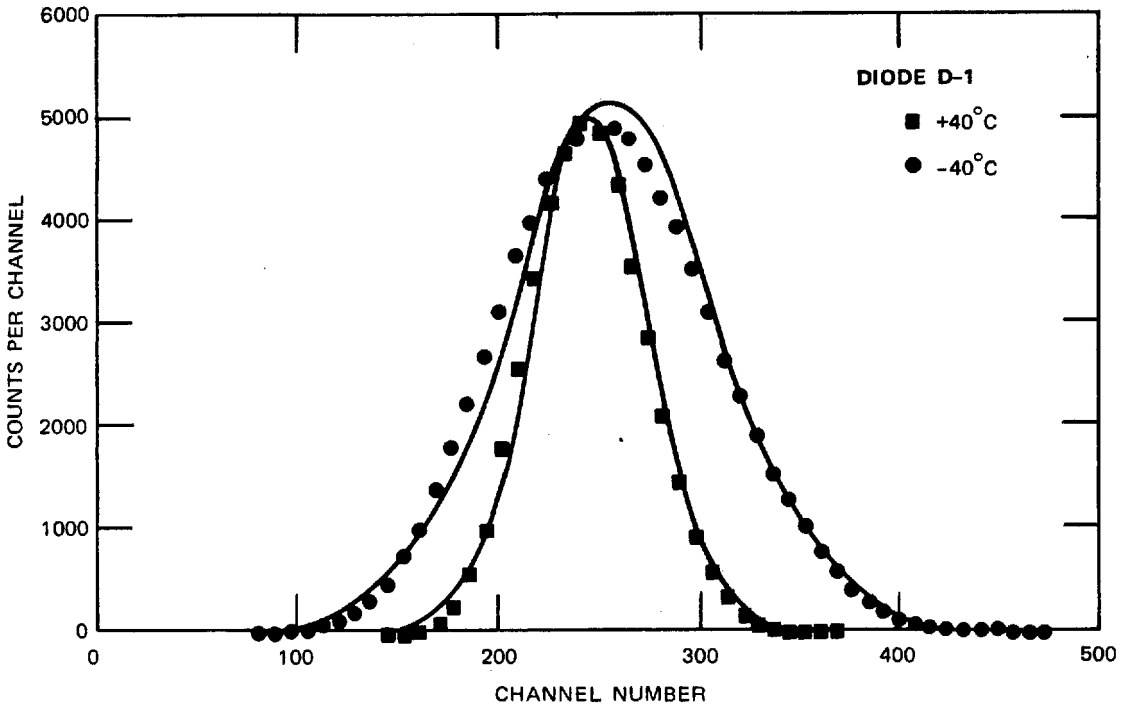

FIGURE 7 PULSE HEIGHT DISTRIBUTION OF FILTERED DIODE NOISE FROM -40 TO +40°C

Over the same temperature range, the spectral density of filtered output from the diode was found to be white noise within ±1 dB. The unfiltered frequency spectrum (to 2 MHz) showed a shift in the fundamental pulse rate peak as a function of temperature. This is to be expected from the dependence of pulse rate on bandgap energy.

Published performance data on the MD-20 shows only that the spectral noise density is relatively constant from a reverse current of 60 to 120 μA and drops off at higher currents. Figure 8 shows two pulse height spectra, at 100 μA and 200 μA. While the spectrum taken at 100 μA can be easily fit with a gaussian distribution, it is clear that at 200 μA the spectrum is extremely asymmetric. Since the behavior of this device at very high currents (~1 mA) is like that of a purely avalanche diode--i.e., small noise voltage and wideband white noise--we believe the asymmetric response shown at a reverse current of 200 μA is due to competing noise

II SUBSYSTEM TESTING

A. Noise Diode RNG

1. Device Tests

Six Texas Instruments planar silicon noise diodes (type MD-20) were tested. Data collection was accomplished through pulse height analysis, frequency spectrum analysis and fast signal analysis of individual pulse trains. By varying such factors as temperature, reverse current, magnetic field, etc., the dependence of diode output on each variable was established. The unfiltered diode output was found to be random amplitude sawtooth pulses with a rising slope of 3.1×10^6 V/s for a load capacitance of $\approx$10 pF and reverse current of 100 μA. The mean rate of these pulses was determined to be a function of temperature consistent with the change of bandgap energy. In addition, "dead spaces" were found to appear randomly between pulses. The duration of these dead times depends strongly on the reverse current.

While maintaining a constant reverse current of 100 μA, as measured by an electrometer, the temperature of the diode was varied from -40 to +40°C. Over this temperature range, the pulse height and frequency spectra of several diodes were measured. The variation in spectral noise density measured by plotting the integral of each pulse height spectrum as a function of temperature was within a few percent of the specified value of -3.2 $\mu V/\sqrt{Hz}$ °C. The integral of each peak was also compared with the area obtained by integrating a gaussian curve that was fitted to each set of data points. These areas were found to agree to within 1%; indicating that from -40 to +40°C, the noise pulses maintain a gaussian amplitude distribution. Figure 7 displays the pulse height data and computer fit.

resolution in both the x and y direction is 200 points/inch over a 20-by-20-inch surface. Points may be entered in a stream of up to 200 points per second or may be entered individually.

4) D^2 Test

The D^2 test consists of comparing the theoretical distribution of a random line in 2-space with an empirical distribution obtained from the random number generator being tested. This test seeks to determine if there is a clustering of numbers in 2-space.

5) Conditional Bit Test

The conditional bit test is performed to check independence of bits within each number produced by a random number generator. Given a 1 in a single bit position, what is the probability that any other bit is also a 1. For true bit-by-bit independence this should be one-half.

C. Display

1. Grinnell Graphics Display System

The Grinnell Graphics Display System consists of 256 × 512 bytes of read/write high-speed memory, two sets of three 8-bit DACs, and two 8 × 24 bit color look-up tables. Depending upon the configuration determined by software commands over a DMA channel from the LSI-11, a single image with high color resolution (8-bits of color/pixel) may be displayed on either or both of two color monitors, or two 4-bit color resolution images may be displayed independently. Because the color of a given pixel is determined by the values in a color look-up table, it is possible to simulate animation by software manipulating the color of a complex predrawn image.

2. Summagraphics Tablet

Graphic information in the form of an x-y coordinate point is presented as input to the LSI-11 over a 16-bit parallel interface. The

c. Fixed-Length Statistical Tests

1) Frequency Test

The frequency test analyzes the number of times a particular digit and the number of transitions between pairs of digits are observed in a random sequence. For the test of the various sources considered here, a 15-bit fraction ($0 \leq$ fraction < 1) is derived from the source in question. That fraction is used to calculate an integer between 1 and 10 inclusive. A single-row matrix is used to accumulate the transition occurrences where matrix element (I, J) represents the number of times digit I followed digit J. Standard chi-square techniques are used to determine if there is no preference either among single digits or among paced sequences.[6]

2) Gap Test

Given a digit between 0 and 9 derived as above, the gap test measures the number of digits that occur in the sequence between successive appearances of the specified digit. The accumulated number of digits in each gap are compared to the expected geometric distribution by a chi-square test. This procedure is followed for all digits 0 through 9 in the given sequence.

3) Yule Test

The Yule test measures the distribution of the sum of 5 consecutive decimal digits for the random number generator in question and compares the resultant distribution with the expected (near normal) one by a chi-square test. This test is particularly sensitive to excessively nonuniform distribution of the digits between 0 and 9 in the sequence.

Utilization of the above statistical procedure permits analysis of the binary noise sequence for excess 1's or 0's by the most efficient technique currently possible.

To show this, consider the expected number of samples required in a fixed-length sequence to meet the Type I and Type II error specifications, α and β:

$$n_{fix} = \frac{\left[Z_\alpha \sqrt{p_o(1 - p_o)} - Z_\beta \sqrt{p_1(1 - p_1)}\right]^2}{(p_1 - p_o)^2}$$

where Z_α is the z-score, assuming a normal distribution, corresponding to the α criteria (for $\alpha = 0.05$, $z_\alpha = 1.65$). Likewise, for $\beta = 0.05$, $Z_\beta = -1.65$. For $p_o = 0.5$ and $p_1 = 0.6$, $n_{fix} = 267$.

The average number of trials required to reach a p_1 decision and a p_o decision, respectively, is given by

$$\bar{n}_1 = \frac{\beta \log\left(\frac{\beta}{1 - \alpha}\right) + (1 - \beta) \log\left(\frac{1 - \beta}{\alpha}\right)}{p_1 \log\left(\frac{p_1}{p_o}\right) + (1 - p_1) \log\left(\frac{1 - p_1}{1 - p_o}\right)}$$

$$\bar{n}_o = \frac{(1 - \alpha) \log\left(\frac{\beta}{1 - \alpha}\right) + \alpha \log\left(\frac{1 - \beta}{\alpha}\right)}{p_o \log\left(\frac{p_1}{p_o}\right) + (1 - p_o) \log\left(\frac{1 - p_1}{1 - p_o}\right)}$$

Using the above values for p_o, p_1, α, and β, $\bar{n}_1 = 132$. Thus, sequential analysis requires approximately one-half the number of samples required by the fixed sample situation for this case. The general proof is given in Reference 3.

(3) If the sum of 1's lies in Region I, do Step 1.

(4) If the sum lies in Region II, stop the run, concluding that the binary sequence is derived from the undistorted p_o distribution.

(5) If the sum lies in Region III, stop the run, concluding that the binary sequence is derived from the distorted p_1 distribution.

The equations for the upper and lower limit lines shown in Figure 6 are, respectively:

$$y_1 = d_1 + Sn$$

$$y_o = -d_o + Sn$$

where

$$d_1 = \frac{\log \frac{1 - \beta}{\alpha}}{\log\left[\frac{p_1}{p_o}\frac{1 - p_o}{1 - p_1}\right]}$$

$$d_o = \frac{\log \frac{1 - \alpha}{\beta}}{\log\left[\frac{p_1}{p_o}\frac{1 - p_o}{1 - p_1}\right]}$$

$$S = \frac{\log \frac{1 - p_o}{1 - p_1}}{\log\left[\frac{p_1}{p_o}\frac{1 - p_o}{1 - p_1}\right]}$$

in which S is the slope, n is the number of samples, and d_1 and d_o are the y-axis intercepts.

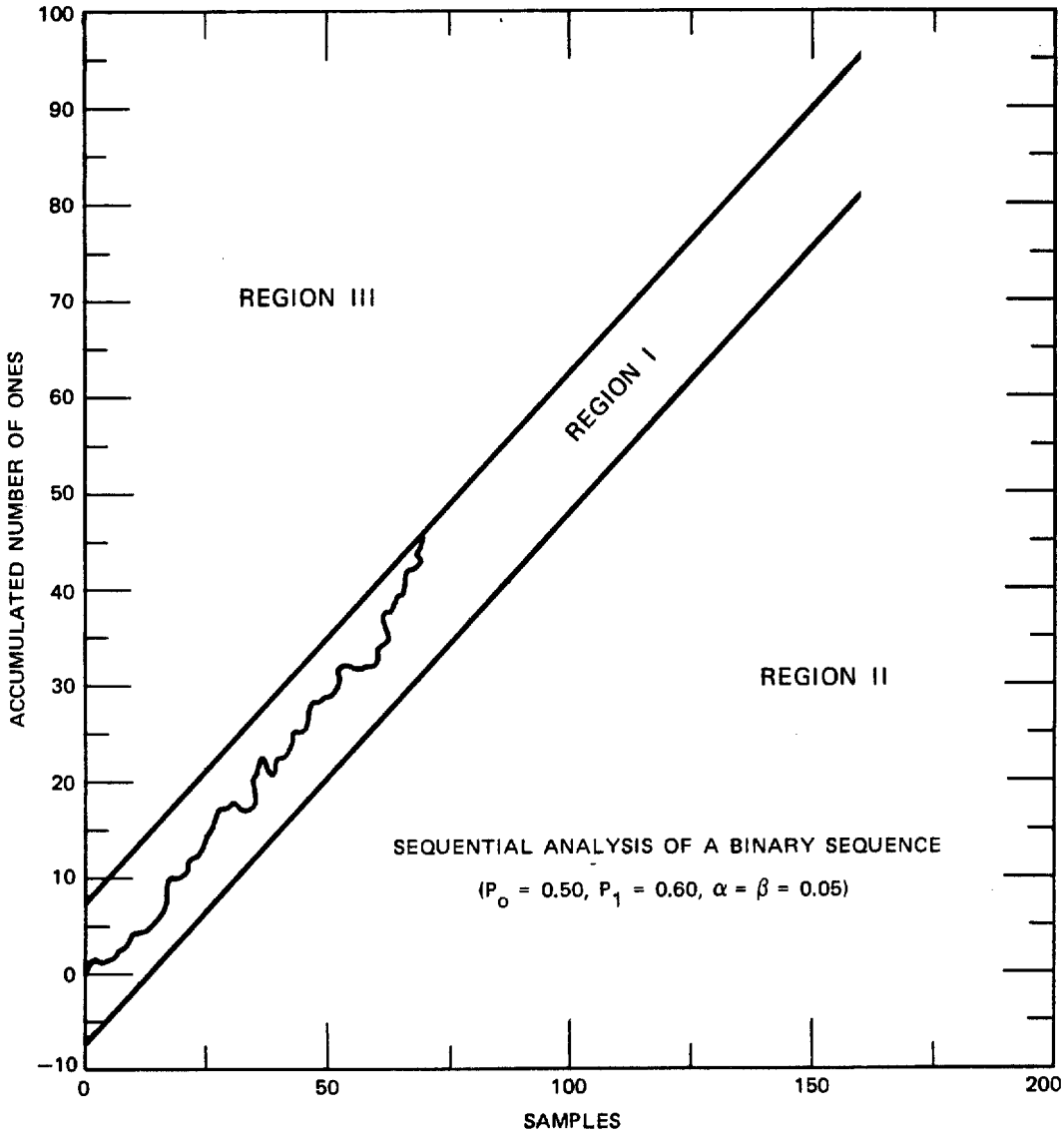

FIGURE 6 EXAMPLE OF SEQUENTIAL SAMPLING PLOT

following the sampling of each bit: continue sampling before making a decision (Region I in Figure 6); label the sequence as distorted (Region III) or undistorted (Region II).

Thus, sampling steps can be defined for the nth sample:

(1) Sample the binary sequence

(2) Sum the number of 1's to date.

higher-level languages such as FORTRAN and MACRO, and provides a framework for an extensive real-time interactive system. Versions of RT-11 monitors have been in operation for nearly ten years, so that this software system is especially trouble-free.

b. Sequential Analysis

The sequential analysis technique[3,4] is an extremely efficient technique for determining whether the output of a binary random generator contains a distribution of 0's and 1's as expected, or is distorted. The principal advantage of the sequential sampling technique as compared with other methods is that, on the average, fewer bits per final decision are required (roughly 50%) for an equivalent degree of reliability.

Before we are able to detect if the random output of a binary generator has been distorted, we must a priori define criteria as to how much distortion we require, and what statistical risks we are willing to accept for making an incorrect decision. To meet these criteria, sequential analysis requires the specification of four parameters to determine from which of two binomial distributions under consideration (distorted or undistorted) a data sample belongs. The four parameters are: p_o, the fraction of 1's expected in an undistorted distribution (e.g., 50%); p_1, the fraction of 1's assigned a priori to define a distorted distribution (e.g., 60%); α, the a priori assigned acceptable probability for concluding that the random source is perturbed (p_1 distribution) when in fact it is not (Type I error); and β, the a priori assigned acceptable probability for concluding that the random source is unperturbed (p_o distribution) when in fact it is (Type II error). With the parameters thus specified, the sequential sampling procedure provides for construction of a decision graph as shown in Figure 6. The decision graph gives a procedure for making one of three possible decisions

Table 3

ADDRESS ASSIGNMENTS

Device	Address	Function	Interupt Vector
Special interface	172420	Command/data	130
	172422	Clock input	
	172424	Temperature	
Graphics tablet	167770	Command/register	304
	167774	Data buffer	
DRV 11-B (Grinnell)	172410	Word count	124
	172412	Buffer address	
	172414	Command	
ADC	172440	Command	146
		Data buffer	

Functionally the system consists of a 16-bit CPU, 32K words of random access memory, and one dual floppy disk drive capable of double-density recording. Special purpose I/O interface cards allow for serial communication to a CRT terminal, 16-bit parallel communication to any parallel device, and direct memory access to and from an external device. An eight-channel fully differential analog-to-digital converter allows the monitoring of external analog signals. Finally, the system has a foundation module on which a specific interface is constructed for control of the various random sources. Appendix B contains the functional description (at the component level) of this interface.

2. Software

a. RT-11 V03B Monitor

The software environment of the LSI-11 system is under control of DEC's RT-11 V03B monitor. This monitor allows for the use of

Table 2

SUBCOMPONENT MANUFACTURERS

LSI-11 Subcomponent	Function	Manufacturer
KD11-HA	CPU board	MDB Systems
MLSI-SMU	System monitor	MDB Systems
DRV-11C	16-bit digital I/O	MDB Systems
MSV-09	MOS memory, 28K	MDB Systems
DT-1761	16 channel ADC	MDB Systems
DRV-11J	4 port serial I/O	Digital Equipment Corporation
DRV-11B	DMA interface	International Data Systems
DSD-440	Floppy disk	Data Systems Design
TCU-50	Calendar	Digital Pathways

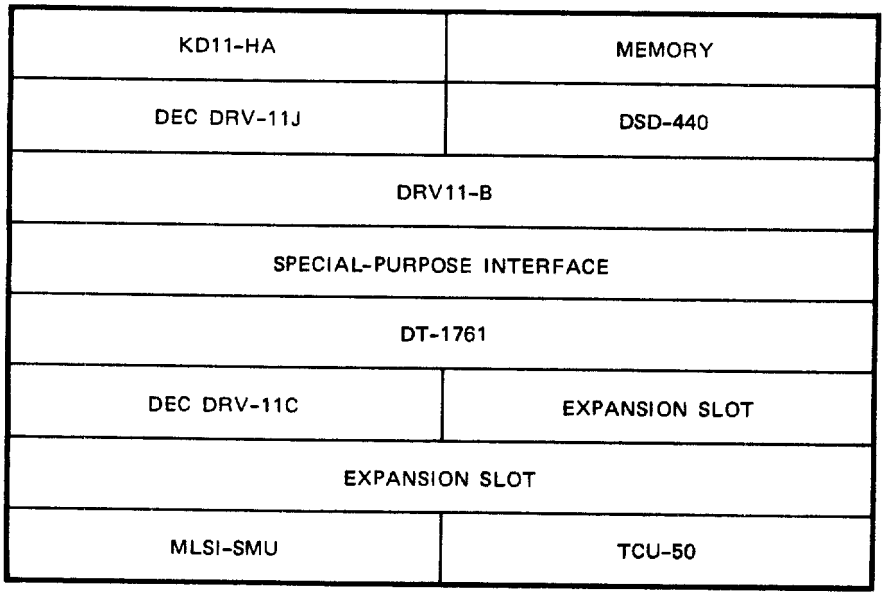

FIGURE 5 SLOT DIAGRAM--FRONT VIEW

Table 1

PSEUDORANDOM SEQUENCE FROM 8-BIT SHIFT REGISTER

Sequence Number J	J	J+1	J+2	J+3	J+4	J+5	J+6	J+7	J+8	J+9
1	236	93	64	141	57	240	165	18	132	251
11	13	35	131	69	89	161	243	250	56	197
21	67	210	19	177	29	205	180	201	85	183
31	150	127	246	46	160	198	28	248	82	9
41	194	253	134	145	193	162	172	208	121	125
51	156	226	33	233	137	216	142	102	218	228
61	170	91	203	63	123	23	80	99	14	124
71	169	4	225	126	195	200	96	81	86	232
81	188	62	78	241	144	244	68	108	71	51
91	109	114	213	173	229	159	189	11	168	49
101	7	190	84	130	112	191	97	100	176	40
111	43	116	94	31	167	120	72	122	34	182
121	163	153	54	185	234	214	242	207	222	5
131	212	152	3	95	42	65	184	223	48	50
141	88	148	21	58	175	143	83	60	36	61
151	17	219	209	76	155	92	117	107	249	103
161	239	2	106	204	129	47	149	32	220	111
171	24	25	44	202	10	157	215	199	41	30
181	146	158	136	237	104	166	77	174	186	181
191	252	179	119	1	53	230	192	151	74	16
201	238	55	140	12	22	101	133	206	235	227
211	20	15	73	79	196	118	52	211	38	87
221	221	90	254	217	187	128	26	115	224	75
231	37	8	247	27	70	6	139	178	66	231
241	245	113	138	135	164	39	98	59	154	105
251	147	171	110	45	255					

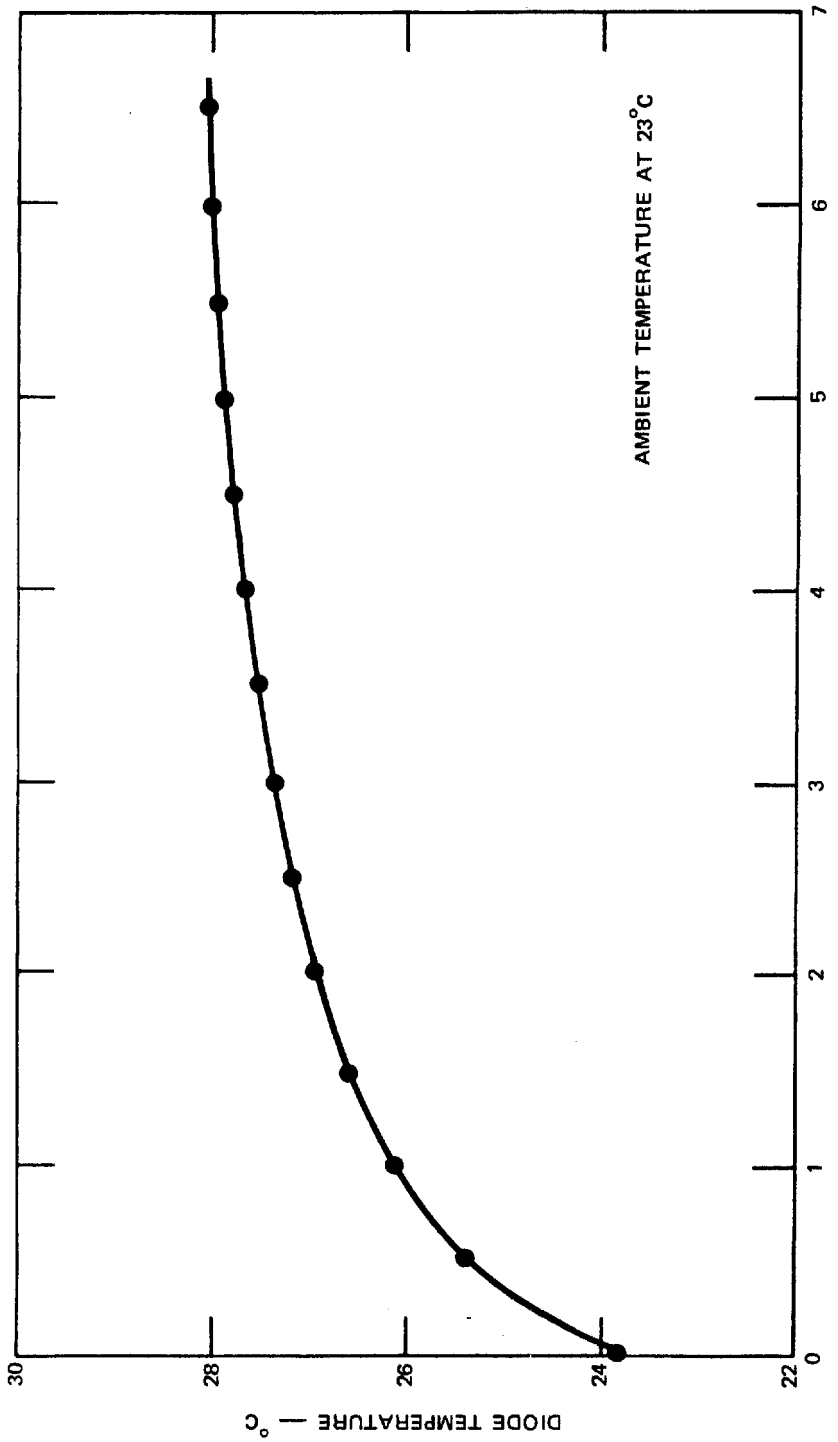

FIGURE 12 DIODE TEMPERATURE vs TIME

B. β-Decay RNG

1. Device Tests

Since the ^{147}Pm source undergoes random β-decay independent of external influences such as temperature, electric field, magnetic field, etc., we restricted our testing to the radiation detector. It should be mentioned that, in general, measured decay rate is a function of both source half-life and source-detector geometry. In our configuration we have minimized the latter effect by arranging a nearly 2π (steradians) source-detector geometry.

Commercially available silicon surface barrier detectors are quite well characterized for noise leakage and resolution at room temperature. Since leakage current is a function of temperature and can contribute noise to the overall system, we tested the device performance over the temperature range 20°C to 43°C. Figure 13 shows this dependence. We have set a cutoff point on dc leakage current at ~2 μA. For this value we can calculate a noise figure given by

$$V = 2.35 \sqrt{\frac{\epsilon^2 I e^2 \tau}{4q}}$$

where

V = Noise voltage (full-width-half-maximum, in eV)

ϵ = eV/pair (3.5 for Si)

I = Leakage current (amperes) 2×10^{-6}

e = Base e

τ = Amplifier peaking time (seconds) 0.25×10^{-6}

q = 1.602×10^{-19} coulombs

V_{noise} (FWHM) = 19.7 keV for 2-μA leakage.

Since the low-level discriminator is set at 25 keV, this noise contribution would not be observed.

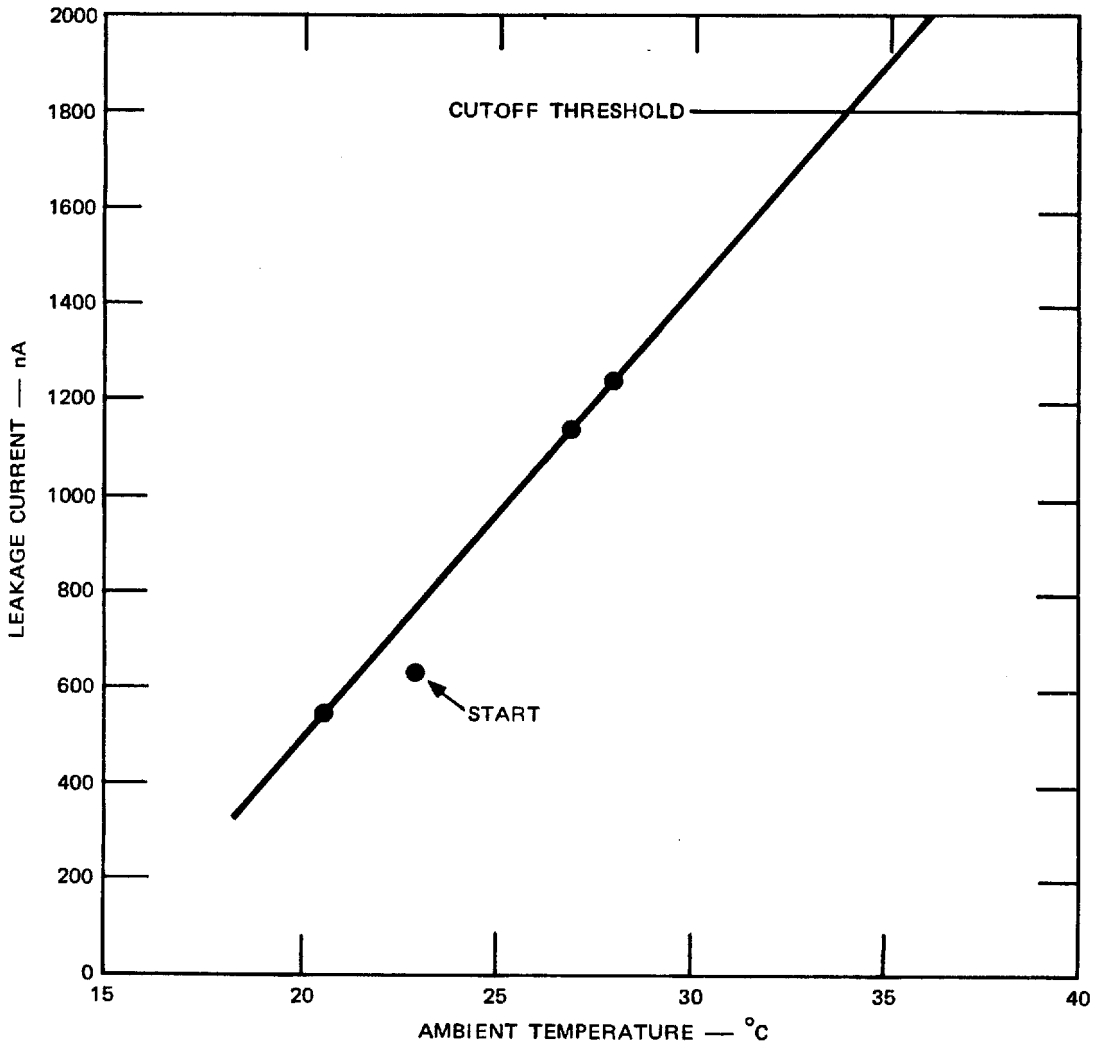

FIGURE 13 DETECTOR LEAKAGE CURRENT AS A FUNCTION OF TEMPERATURE

It is possible that a detector such as this can undergo breakdown, resulting in carrier avalanche noise similar to the MD-20 diode. Should this occur, the output will consist of the superposition of two fundamental random processes (i.e., electronic noise and β-decay).

2. System Isolation and Monitoring

As with the noise diode module, protection against magnetic and mechanical interference has been provided by a 0.125-inch soft iron box.

Similarly, there is an RF shield, a battery power supply, and optical links for data transmission.

Fail-safe provisions on the power supply are the same as for the noise diode unit. In addition there is an automatic shutoff should the device leakage current rise above 2 μA. Quite often breakdown phenomena of the type mentioned earlier are accompanied by a steep rise in the leakage current. The fail-safe point provides protection in case of temperature increase as well as device breakdown.

C. Computer Pseudorandom Generator

Extensive work[6] has been done to develop various computer algorithms that meet a variety of statistical requirements for pseudorandom sequences. One of the best and most studied is a form of Tousworth feedback shift register generator. In this type of number generation, various bits from a shift register are summed modulo 2 and presented to the shift register input. The length of the shift register and those bits used for feedback determine the properties of the resulting sequence.

Using an algorithm by Kendall[6] we have adopted a 31 bit register with bits 31 and 13 used as feedback. Reference 6 compares a number of different generators using an extensive series of statistical tests. The particular shift register generator we have selected is considered to be among the best.

III SYSTEM ANALYSIS

Using the random source hardware developed for this project and the standard fixed length statistical tests briefly described in Section I-B, a number of control runs were collected and analyzed. Five hundred thousand samples in two groups of 250,000 each were taken from each random source and then tested with four separate procedures. The results are listed in Table 4.

In addition, the entire system was tested for 1,000 runs for each source in the final configuration, which utilizes sequential analysis in conjunction with the random sources. The results are tabulated in groups of 100 in Table 5.

Table 4

RESULTS OF STATISTICAL TESTS
OF THE RANDOM NUMBER GENERATORS

Generator	Test	Digit	Bit	Chi-Square
Pseudorandom	Digit frequency (0-9)			9.7 (9)
	Transition frequency (all possible pairs)			80.5 (99)
	Gap	0		12.2 (21)
		1		18.0
		2		17.5
		3		24.6
		4		17.5
		5		17.7
		6		24.1
		7		23.1
		8		23.3
		9		22.7
	Yule			100.4 (45)*
	Distance			22.6 (19)
	Conditional bit		0	110.0 (127)
			1	108.0
			2	108.9
			3	109.8
			4	95.7
			5	115.6
			6	98.2
			7	102.0
	Digit frequency (0-9)			6.8 (9)
	Transition frequency (all possible pairs)			85.9 (99)
	Gap	0		16.2 (21)
		1		14.6
		2		10.2

*Significant results for $p \leq 0.05$.

NOTE: Numbers in parentheses are degrees of freedom.

Table 4 (continued)

Generator	Test	Digit	Bit	Chi-Square
Pseudorandom (cont'd)	Gap (cont'd)	3		29.5
		4		19.1
		5		23.8
		6		20.5
		7		17.4
		8		13.0
		9		17.5
	Yule			30.4 (45)
	Distance			29.8 (19)
	Conditional bit		0	126.7 (172)
			1	142.6
			2	138.4
			3	148.3
			4	125.9
			5	110.9
			6	129.7
			7	140.0
Beta Decay	Digit frequency (0-9)			3.3 (9)
	Transition frequency (all possible pairs)			85.7 (99)
	Gap	0		13.8 (21)
		1		17.6
		2		18.4
		3		19.1
		4		23.4
		5		37.7*
		6		21.1
		7		13.9
		8		21.6
		9		18.2
	Yule			33.8 (45)
	Distance			17.8 (19)

*Significant results for $p \leq 0.05$.

NOTE: Numbers in parentheses are degrees of freedom.

Table 4 (continued)

Generator	Test	Digit	Bit	Chi-Square
Beta Decay (cont'd)	Conditional bit		0	116.6 (127)
			1	114.6
			2	105.4
			3	110.9
			4	127.6
			5	94.2
			6	106.5
			7	122.3
	Digit frequency (0-9)			7.0 (9)
	Transition frequency (all possible pairs)			109.2 (99)
	Gap	0		18.8 (21)
		1		31.5
		2		15.5
		3		22.3
		4		19.5
		5		22.1
		6		15.4
		7		20.8
		8		31.3
		9		20.4
	Yule			41.5 (45)
	Distance			18.3 (19)
	Conditional bit		0	124.4 (127)
			1	118.1
			2	116.7
			3	126.1
			4	110.5
			5	123.2
			6	105.3
			7	133.4

*Significant results for $p \leq 0.05$.

NOTE: Numbers in parentheses are degrees of freedom.

Table 4 (continued)

Generator	Test	Digit	Bit	Chi-Square
Noise Diode	Digit frequency (0-9)			8.1 (9)
	Transition frequency (all possible pairs)			100.6 (99)
	Gap	0		21.0 (21)
		1		19.7
		2		25.3
		3		21.2
		4		27.5
		5		10.2
		6		24.2
		7		9.5
		8		31.4
		9		12.8
	Yule			32.8 (45)
	Distance			24.0 (19)
	Conditional bit		0	132.2 (127)
			1	153.6*
			2	135.0
			3	121.3
			4	135.5
			5	132.1
			6	143.9
			7	136.6
	Digit frequency (0-9)			10.0 (9)
	Transition frequency (all possible pairs)			85.3 (99)
	Gap	0		23.9 (21)
		1		18.0
		2		18.6
		3		17.7
		4		20.9
		5		12.5

*Significant results for $p \leq 0.05$.

NOTE: Numbers in parentheses are degrees of freedom.

Table 4 (concluded)

Generator	Test	Digit	Bit	Chi-Square
Noide Diode (cont'd)	Gap (cont'd)	6		10.3
		7		16.4
		8		23.2
		9		25.0
	Yule			42.7 (45)
	Distance			16.9 (19)
	Conditional bit		0	142.7 (127)
			1	128.3
			2	109.6
			3	121.4
			4	125.8
			5	155.6*
			6	127.2
			7	127.8

*Significant results for $p \leq 0.05$.

NOTE: Numbers in parentheses are degrees of freedom.

Table 5

SEQUENTIAL ANALYSIS OF RANDOM SOURCES
IN SETS OF 100 TRIALS

Set Number	β-Decay	Diode	Pseudorandom
1	9	13	8
2	8	9	10
3	11	10	11
4	2*	9	8
5	14	10	13
6	9	15	9
7	12	10	13
8	10	7	14
9	10	14	7
10	6	9	13

*Significant with $p < .001$.

NOTE: Table entries are the number of trials out of 100 that met the sequential analytic decision criterias. The expected value is 10.

IV CONCLUSIONS

We have shown by extensive environmental testing and Monte Carlo techniques that the LSI-11 based random number generator and analyzer meets all appropriate criteria for accepted definitions of randomness. Specifically, approximately 10^6 bits were analyzed in exactly the same conditions that will be utilized during the experimental phase of this program.

These tests showed no unexpected deviations from the appropriate chance distributions.

Environmental and electrical isolations of the sources and manual reset fail-safe circuitry assures reliable operation.

Appendix A

TECHNICAL CONSTRUCTION DETAILS OF RANDOM SOURCES

Appendix A

TECHNICAL CONSTRUCTION DETAILS OF RANDOM SOURCES

1. Introduction

The need for, and the requirements to be met by, a noise generator system have been established and described elsewhere. In quick review, the performance specifications and goals call for a stable generation source of white noise that is protected from external physical influence or its susceptibility to those effects is known in advance. That noise then needs to be formatted in a specific way and transmitted to a remote processing unit, again with minimal disturbance by the external environment. The ultimate goal is a statistically stable random signal that can be measured over long periods of time with no variation with environmental changes.

Two sources for the random signal were chosen. First, a special avalanche breakdown mode (zener) diode was selected that produces a very predictable series of quasi-impulses essentially random over a reasonable time range and amplitude range. Although external circuit component values affect the spectral density function, and the applied reverse bias voltage affects the avalanche breakdown levels, those conditions can be controlled closely and hence their effects reduced to an acceptable level. Temperature also affects noise statistics but again in a very predictable and stable fashion, so a measure of diode temperature is necessary during the operational usage. The second source of random noise is obtained from a radioactive material of known radiation intensity and statistics. For all practical purposes it emits only low energy electrons (225 keV max), so a silicon surface barrier detector can be used to generate an electrical signal

proportional to the energy of the incoming radiation. Except for the detector, the phenomenon is nearly independent of the local environment.

Packaging of the sources and sensors along with the associated electronic circuitry provides a first level of protection from external influences such as heat, light, vibration, and electromagnetic radiation. To minimize the possibility of external electrical influence, the source of power for the units is provided by internal chemical batteries. To avoid coupling of extraneous electrical signals from either the remote processing unit or nearby equipment, the data link from the noise source unit is provided entirely by use of fiber optic cables. The unit case is fabricated from mild steel that provides shielding from both magnetic and electric fields.

2. Noise Diode Source

The heart of this unit is the avalanche zener diode. It produces a noise-like voltage when reverse biased with a constant current dc source of about 100 μA. The average zener breakdown occurs at about 12 V and the noise voltage spikes ramp continue for a few volts about that level.

a. Bias Circuit

For simplicity and practical realization, the diode bias current is provided by a 67.5-Vdc battery and a series dropping resistor to a shunt 30-V zener diode for voltage regulation, and then on through another resistor of the appropriate value to the noise diode. A large bypass capacitor is used across the regulator zener diode to keep incidental noise from reaching the noise diode. Since this is really not a constant current source, the diode current, and hence its operating condition, can change. It has been found that the noise statistic varies significantly if the bias current changes more than about plus or minus 5%, and so it was necessary to include a capability to monitor that bias current.

b. Bias Current Monitor

An operational amplifier was employed as a transconductance amplifier to convert the bias current to a voltage measure and to keep the diode at a virtual ground. The feedback resistor was chosen to be 50 kΩ, which then provides a -5 Vdc output. An inverting amplifier with unit gain generates a +5 Vdc output that is used for comparison against a limit window of 4.75 to 5.25 Vdc. If the bias current varies more than ±5% of nominal, then the comparator test circuit output can be used for warning or control.

c. Noise Preamplifier

The output of the noise diode is a voltage ranging from about 12 V upward in sawtooth fashion to 14 to 15 V and with an extremely fast fall time back to 12 V. The diode chip capacitance and the stray capacitance of the wire leads establish the minimum, which is about 2 or 3 pF. The charging resistance is essentially the bias supply resistor value of 180 kΩ and hence it is necessary to use an amplifier with a very low input capacitance and a quite high input resistance if the noise voltage waveform, and hence its spectral response, is not to be influenced greatly. This is achieved by use of a National LM310N unity gain buffer amplifier which has a specified input capacitance of only 1.5 pF, an input resistance of 10^{10} ohms, and a slew-rate of at least 30 V/μs, which maintains the desired system bandwidth.

d. Noise Bandpass Filter

Although the noise diode power frequency spectrum continues to at least 5 MHz, only that portion from 1 kHz to 200 kHz is desired for use by the processing unit. Thus, a cascade of a high-pass and a low-pass active filter is used. Both filters contain three poles so as to provide

18 dB per octave rolloff, and the design is a Butterworth for smooth amplitude and phase response. Again, the National LM308A voltage follower is employed for the active filter elements.

e. Noise Output

Two outputs to the processor unit are provided. The first is the bandpass filter output time waveform in analog form, and the second is a zero-crossing digital pulse train.

1) Analog Output

The analog output is provided by use of a video bandwidth fiber-optic data link. Because the peak voltage from the bandpass filter is less than 100 mV, a post-amplifier is necessary as well as a current booster to drive the light emitting diode circuitry. A National LF357N FET operational amplifier and a LH0002CH current booster amplifier are configured as an X10 gain noninverting signal amplifier with adequate bandwidth and linearity to faithfully reproduce the noise signal. A Meret, Inc., analog optic transmitter composed of a current linearizer and the LED then converts the analog noise signal to an optical replica for transmission over a fiber optic cable.

2) Digital Output

The zero-crossing digital representation of the noise is provided by first a standard analog voltage comparator (a National LM2903N) followed by a CMOS one-shot multivibrator chip (Motorola MC14528BP), which establishes the minimum pulsewidth at 5 μs, and then a single transistor (2N2222) to drive the Meret, Inc. digital optic transmitter LED. Thus, each time the noise voltage from the fiber passes through zero in the

positive-going direction, a 5 μs optical pulse is applied to the digital fiber optic cable.

f. Test and Shutdown

Since the noise unit is powered by internal batteries of limited power capability, it is necessary to monitor the state of the battery and shut down the optic links if that voltage drops below a level that is known to cause erroneous operation. A simple analog voltage comparator (LM2903N) is used to sense when the battery voltage drops below that level, and the output of the comparator is used to inhibit the one-shot multivibrator in the digital optic data link. Thus, the operator at the data processing center can detect a low-battery condition if the digital link ceases to transmit but the analog continues to function. Similarily, if the noise diode bias current varies outside the ±5% of nominal window, the comparator output is used to shut down the digital optic data link. Either of these "fail" signals will toggle a simple latch circuit (CA4011B), which then shuts off the digital optic data link. The latch is reset each time the unit is powered down and then turned on again. There is about a 10-s time delay to allow for the unit to reach normal operation before the latch is released.

g. Temperature Monitor

Since the noise diode output is temperature-sensitive, a measure of the diode holder temperature is made and passed out to the data processor via a low-speed fiber optic data link. A platinum resistance thermometer element is imbedded in the diode holder, and a precision resistance bridge circuit feeds the temperature difference voltage to a precision instrumentation amplifier (BB3630AM), where it is scaled to 100 mV per degree Celsius. A voltage-to-frequency-converter (BB-VCC42) then converts the

signal to 100 Hz per degree Celcius. This digital frequency pulse stream is then applied to a digital optic transmitter (BB3713T) that converts the pulse train to an optic replica for transmission over a fiber optic cable. The accuracy of the system is 0.5°C from 10 to 60°C.

h. Power Distribution

Several different voltages are needed for the circuit elements. First, the noise diode is operated from +30 Vdc, which is not shared by any other circuitry to avoid interaction effects. The noise amplifiers and active filters are supplied with a +10 Vdc while the peripheral amplifiers are provided with ±12 Vdc. The digital optic transmitter LED uses +5 Vdc, while the analog optic transmitter LED and current linearizer use +12 Vdc. A special +10 Vdc source is used by the temperature-sensor bridge circuit. Finally, the direct battery voltage at a nominal 14 Vdc is used for the low battery test circuit. All of these voltage lines are adequately bypassed using large value tantalum capacitors with decoupling ceramic capacitors located at each integrated circuit.

i. Circuit Layout

All of the circuitry is located on a single printed circuit board that was especially designed for analog hand-wire layout and assembly. Large-area ground-plane is provided so as to minimize coupling effects from either adjacent or remote circuitry. Component lead-length is kept to a minimum and interconnective wires are run point-to-point along the ground plane. Parallel bundling of wires is avoided. Power supply voltages are attached at one end of the PCB with direct bypassing. Signal flow layout is approximately linear down the board to the opposite end where the optic transmitters (high current loads) are located. All discrete components and integrated circuits are located on one side of the PCB, while

the majority of the interconnective wiring is on the opposite side. PCB mechanical support is provided by four standoff posts, one at each corner electrically tied to the PCB ground plane.

j. Noise Diode Mechanical Mount

The noise diode and the thermometer are thermally coupled with a low temperature solder inside a small cylinder of stainless steel. The electrical leads were first painted with an insulating varnish and then held in place with epoxy resin. This type of mount provides a firm mechanical support and a good thermal link between the diode case and the thermometer element. The holder is then attached to the PCB using a metal clamp and screw, with the whole structure acting as a grounded electric shield. The diode and thermometer electrical leads exit from the ends of the holder cylinder.

3. Electron Noise Source

This unit derives its random noise from a radioactive material that emits electrons of a random energy below 225 keV at random time intervals. These electrons are detected by use of a large-area silicon diode that is reverse-biased at 100 Vdc to establish the proper charge collection volume.

a. Bias Circuitry

The radiation detector diode operates best for this application when reverse biased at about 100 Vdc from a voltage source impedance as high as practical. At that bias voltage, the detector has a small but significant leakage current of about 300 nA, which therefore requires that the source resistance be less than about 10 MΩ so as not to cause a significant bias voltage drop. At 300 nA and 10 MΩ, the drop is only 3 V, which is acceptable. Thus, the bias circuit is a +100 Vdc supply, a 1 MΩ

series resistor, and a shunt 0.1 μF capacitor for filtering purposes followed by the 10 MΩ detector load resistor and then the detector itself.

b. Leakage Current Monitor

Since the detector leakage current is a sensitive measure of device integrity and can contribute noise to the electron signal, this current is measured and used to shut down the system if leakage exceeds a predetermined limit. As was done in the noise diode source, a transconductance amplifier (LF 355 N) is used in the common or ground lead of the detector. It maintains the anode at a virtual ground along with large capacitance shunting as well as providing an output voltage proportional to leakage current. The feedback resistor value was selected as 3 MΩ, which scales the current to -3 V per μA. A unity-gain inverting amplifier (LM 741 V) then applies the voltage to a comparator (LM 2903 N) that has a threshold of +6 Vdc. Thus, a shutdown command is generated if the leakage current exceeds 2 μA--a level where the noise contribution to the electron signal is still below the discriminator threshold.

c. Noise Preamplifier

This type of noise is best processed by use of a charge-sensitive amplifier followed by a double differentiation to extract only the very fast diode discharges when an electron passes through it and to ignore the slow "tail" recharge. This is performed by use of a commercial hybrid unit (AMPTEK A-203). At the output of this device there exists a series of random height "impulses" that occur at random times, each impulse corresponding to a single electron that passed through the diode.

d. Post Amplifiers

The output of the charge-sensitive amplifier is quite small in amplitude, and so it is necessary to amplify it further before it can be

used. This amplification is provided by a chain of three IC amplifiers. First, a single low-level, wide-bandwidth operational amplifier (NE531V) increases the signal by 10 from about 10 mV up to about 100 mV. This is followed by a two-state high-level, wide-bandwidth amplifier composed of an op amp (LF357N) and a current amplifier (LM0002CH) which provides another times-10 gain. At that point, the noise pulses are about 1 V in amplitude and can be processed for transmission.

e. Data Transmission

Two forms of the noise signal are generated and transmitted to the remote processor unit. The first is an analog replica of the noise while the second is a digital pulse replica from a threshold level discriminator.

1) Analog Output

The entire analog voltage waveform from the post amplifier is used without bandlimiting to drive the MERET analog optic transmitter LED via the current linearizer. Since the optic link has a bandwidth of at least 5 MHz, essentially all of the analog noise signal spectrum is transmitted without significant degradation.

2) Digital Output

The same analog signal is then applied to a threshold-level discriminator (AMPTEK A-206) for conversion to pulse form. The amplitude threshold is set for a lower-level pulse energy output of 25 keV, and the resulting signal is then applied to the digital optic transmitter LED through a standard IC TTL Gate (SN74LS00). The discriminator also includes a minimum-width one-shot multivibrator that sets the digital pulsewidth to 5 μs.

f. Test and Shutdown

Three operating parameters are monitored and, if out of limit, are used to shut down the digital optic data link. The first is the main system dc power in the form of the battery voltage. A minimum voltage of 12 Vdc is the threshold for the nominal 14-V battery voltage and corresponds to the condition where about 95% of the available energy is consumed. When the 12-V threshold is reached, a comparator (LM2903N) senses it and shuts down the optic data link via the TTL AND Gate. The second parameter is the power supply voltage used for the bias supply for the electron detector diode. When that voltage falls to +110 Vdc from its initial value of +135 Vdc, another comparator senses that condition and shuts off the data link. Finally, when the electron detector diode leakage current exceeds 2 μA, a third comparator senses that condition and also shuts down the data link. Thus, any normal failure condition will be sensed and used to shut down the digital data link as a warning to the processor. Any one of the three failure signals will toggle a simple latch circuit (CA4011B), which in turn shuts off the digital optic data link. The latch is reset whenever the unit turned off and then turned on again. There is about a 10-s time delay to allow for the unit to reach normal operation before the latch is released.

g. Power Distribution

The various power supply voltages required by the circuitry are brought into the circuit board, bypassed using large-value tantalum capacitors, and then distributed to the circuit points. Additional capacitive bypassing and decoupling are provided at each critical circuit point and integrated circuit. Sensitive portions of the circuit are supplied with isolated power voltages such as the detector diode, and the signal amplifier chain. The high-power amplifiers and the optic transmitter LEDs are powered separately to avoid feedback to the low-level sections.

h. Circuit Layout

Layout of the electron noise source PCB is essentially the same as that used for the noise diode source (see Section 2-h).

i. Electron Source and Detector Mechanical Mount

The radiation source is a commercial unit in the form of a thin metal disk about 1 inch in diameter and 0.1 inch thick. The electron detector diode is also a commercial package in the form of a 1-inch-diameter cylinder about 0.7 inch long with a BNC type of connector on the end opposite the diode sensitive surface. These two units are held together with the radiation source next to the diode surface by use of a specially made plastic holder. The holder is then mounted to the circuit PCB such that a standard BNC barrel connector and a bulkhead connector tie the detector to the PCB both electrically and mechanically. The radiation source can be removed easily through a top cover that is held on by a metal spring clip. When the units are in place, they form an electrically conductive shell that also provides closure to visible light. This is necessary because the radiation detector is quite sensitive to photons as well as electrons.

4. Power System

Since both the noise diode and the electron noise sources require essentially the same dc power supply voltages, a common power source and regulator circuit were developed. The major difference is in the need of a higher voltage for the electron detector than that needed for the noise diode. Power consumption is higher for the noise diode source since it includes the temperature monitor and data transmitter and a few more ICs that are not needed for the electron noise source. The main power source is a 12-Vdc NICAD rechargeable battery, while the bias supply is a set of carbon-zinc dry-cell batteries.

a. Batteries

Most of the power is provided by two 6-V NICAD battery packs series-connected to provide 12 Vdc. The desired operating period per day was two 3-hour runs and the total current drain on the battery is 210 mA for the noise diode and about 160 mA for the electron noise source. This requires that the battery have at least a 1.3 ampere-hour capacity when discharged at 210 mA for 6 hours. The batteries chosen (Eveready N91) have a 1.5 ampere-hour capacity and hence can just meet the requirements if they are fully charged. Charging of this type of battery is achieved after 14 hours at 150 mA and hence can be ready each day after an overnight charging. The batteries are sealed units and so present no hazard to either equipment or personnel.

The bias voltage for each noise source is provided by independent carbon-zinc dry cells. Since the current drain is quite small, these types of batteries provide hundreds of hours of operation before cell voltage drops below the useful level. The noise diode requires 30 Vdc at 100 μA, which is provided by a single 45-V battery (Eveready #415). The 45-V battery voltage is dropped and regulated to 30 Vdc by use of a series resistor and a shunt zener diode followed by a L-C low-pass filter. The electron detector diode requires 100 Vdc at about 1 μA, which is provided by two 67.5-V batteries connected in series for a total of 135 Vdc. This is dropped and regulated to +100 V using a series resistor and a shunt zener diode also followed by a L-C low-pass filter.

b. DC Voltage Regulators

Several dc voltages are needed by the electronic circuitry, integrated circuits, and optic transmitters. Much of the current is required at +12 Vdc, and so the 14-V battery voltage is reduced to +12 V by use of a special series-pass regulator circuit. This circuit has the

distinct characteristic of regulating to within 0.3 V of the battery voltage, a feature not normally available in IC regulators. Thus, the battery voltage can fall to 12.3 V before any of the circuit power voltages fall below 12.0 V.

Two +10 Vdc supplies are needed, one by the low-level sensitive signal amplifiers, and one by the temperature sensor bridge circuit. These are provided by use of standard IC regulators (LM340LAH-10). A single +5 V power supply is required by both TTL logic ICs and the digital optic transmitter LEDs. This is provided by use of another IC regulator (LM340LAH-5). The negative 12 V needed by various amplifiers is generated in a small hybrid switching dc-dc converter (W5R-12).

All of these power supply regulators are followed by L-C low-pass filters using either powdered iron core or ferrite pot cores for high inductance at the static dc current. Large-value tantalum capacitors provide the low shunt impedance to ground. Smaller RF types of feed-through capacitors are employed to help reduce any RF pickup that may exist in the power system.

c. Interconnection

A double-pole, double-throw switch either connects the main battery and the dry cells to the circuitry or disconnects them and connects the NICAD battery to a battery charger jack. A 1/4-A fuse protects the battery against inadvertent internal short circuit.

5. Packaging

Both the noise diode and the electron noise sources are mounted in enclosures of identical dimensions. The noise diode unit has an extra aperture for the temperature optic transmitter cable connection. The internal layout of each is the same except for the minor positioning of

the carbon-zinc dry cell batteries, one for the noise diode unit and two for the electron noise unit.

The enclosure is fabricated from mild steel so as to provide both electric and magnetic shielding for the contained circuitry. All seams are welded and the cover has an overlapping flange. Six screws attach the cover and a special RF gasket seals the enclosure along the mating surfaces. Internally, there is a steel partition separating the power supply compartment from the electronics compartment so as to minimize any interaction between the two. The power supply wires pass through the partition via RF type feedthrough capacitors.

The batteries are held in place by conformal foam rubber and stryofoam plastic. The power supply regulator circuitry is mounted on a Vector composition board, which is then attached to the partition using stand-off posts and machine screws. The on-off power switch, the fuse holder, and the battery charger receptacle are mounted on the side wall of the enclosure.

The noise source circuit board is mounted in the other part of the enclosure on stand-off posts and machine screws. The three optic transmitters are attached to the circuit PCB and the alignment is such that the fiber-optic cable connectors protrude through openings in the end wall of the enclosure. Although this configuration does not provide the best of RF shielding, it was chosen as a reasonable alternative to ease the problem of electrical connection. A set of short, insulated wires connect the PCB to the partition feedthrough capacitors for the various dc voltages. By simply removing the cover and the four mounting screws, the circuit PCB may be lifted out while still connected electrically for diagnostic testing and repair.

6. Data Receiver Unit

The analog and digital signals that are generated in the two noise units are transmitted to the processor unit by use of fiber-optic cables. The noise units contain the optic transmitters, so a special receiver must be provided to reconstitute the electrical signals. This function is achieved in a single package incorporating all of the matching optic receivers, power supplies, and signal line drivers.

a. Analog Receivers

These units are special linear optic receivers with wide bandwidth (5 MHz) and good dynamic range. They reconstitute the analog signal as transmitted from the noise units and provide it at a level of about 1 V peak-to-peak. Since the output level and impedance are not compatible with the requirements of the processor analog-to-digital converter (ADC), a signal amplifier and line driver are provided. This is a single wide-band op-amp that provides a voltage gain of X5 and an output impedance of about 100 ohms. Thus, the signal is available at a level of about 5 V peak-to-peak at a low source impedance. Several feet of 50-ohm cable can be driven without significant bandwidth or level loss.

b. Digital Receivers

These units are also special optic receivers matched to the transmitter characteristics and can handle standard TTL bit streams of at a pulse rate of several megahertz. No special post amplifiers are needed except for a simple TTL buffer to isolate the receiver to inadvertent external high voltages.

c. Auxilary Analog Comparators

Two special analog comparator units with adjustable threshold voltages are included. These can accept input signals of as much as plus and minus 12 V peak excursions and with bandwidths of several megahertz. The comparator threshold is adjustable over a ±4 V range by means of a front panel 1-turn potentiometer. The output of the comparator triggers a one-shot multivibrator that produces a TTL output pulse with a width of about 0.1 μs. Hysteresis (100 mV) is provided in the comparator input circuitry to suppress noise-induced oscillations.

d. Power Supply

The optic receivers and the auxilary amplifiers, comparators, and one-shots require ±12 Vdc and +5 Vdc reasonably regulated and filtered. A simple, special-purpose triple supply using commercial IC regulators powered from a 115 Vac full-wave rectified transformer is provided. It is constructed on an aluminum shelf that also serves as the regulator heat sink.

e. Packaging

A standard 7.5-inch-high-by-19-inch-rack panel supports the optic receiver modules, the peripheral circuitry, and the power supply shelf. Since the optic receiver modules have BNC output connectors, a simple clamp and connector arrangement hold them to the front of the panel so that the fiber-optic cable can be attached easily. The cables hang vertically down for minimum strain, since they are somewhat fragile.

The final outputs of the five optic receivers are provided via bulkhead BNC connectors at the top of the panel directly in line with each optic module. Thus, connection to the processor interface is by

short coaxial cable. The two auxilary comparator circuits are also connected via front panel BNC connectors and the threshold controls are in line with them for ease of identification and use. The unit's power switch and pilot light are also on the front panel, but the fuse is located on the power supply tray in the back.

The peripheral circuitry is mounted on a long, narrow strip of vector perf-board and attached to the back of the panel near the top so that the input and output connections to the panel BNC connectors are direct. The power supply tray is attached to the rear of the panel at one end. The ac line cord is hard-wired to the power supply tray and exits at the rear.

The unit is mounted in a standard 19-inch rack directly below the processor interface and connects to it with short coaxial cable. The fiber optic cables are attached and routed to the noise units as needed.

Appendix B

TECHNICAL DETAILS OF SPECIAL INTERFACE BOARD

Appendix B

TECHNICAL DETAILS OF SPECIAL INTERFACE BOARD

1. Introduction

The special interface board contains several major functional components:

- Command output
- Real-time clock
- Input data to LSI-11
- Output data from LSI-11
- β-decay channel
- Noise diode channel
- Pseudorandom shift register
- Counters.

The DRVII-P board from Digital Equipment Corporation contains a prewired section for address decoding and interrupt handling. The description of these sections as well as PIN assignments may be found in the Digital Components Group DRVII-P Module Users' Manual. All pin references on the schematic prints may be found in this manual. We have followed a chip placement procedure that differs slightly from the one shown in the manual. Columns are labeled on the component side of the board. With the bus contacts facing you we label the chip positions A through L starting on the left. Noticing that the hole positions are numbered on the board 0 through 64, a chip may be positioned by specifying its column letter and the hole position for chip pin number 1.

2. Functional Description

a. Command Output

The special interface board functional commands are completely contained in a single byte (74LS374). All outputs from the LSI-11 are strobed per the DLVII-P protocol through a NOR decoding gate (74LS02). The function of each of the command bits is shown in Table B-1.

b. Real Time Clock

The time base for the real time block is derived from a standard crystal-controlled oscillator that is divided by 10^6 in three stages with 74LS390 dividers. Depending upon the tick-select bit in the command byte, either a 10-kHz or an 0.1-Hz clock is gated into a 16-bit countdown counter (4-74LS193 counters). These counters may be preset from a 16-bit register that is under software control (described below). Two 74LS74 dc flip-flops ensure:

- That the clock enable pulse starts the timing countdown.
- That at the end of countdown, the clock is reset to initial conditions and restarted.

A 74LS123 one-shot is used to produce an interrput signal (called real-time block pulse) that enables the DRVII-P interrupt protocol and is presented to the outside world through 74LS04 inverter/drivers.

Depending upon the clock select bit, either the above process is enabled or the real-time block pulse is derived from an external source through a 74LS04.

c. Data Input to LSI-11

The DRV11-P allows for up to four different addresses to be decoded from the Q-bus, and thus four different 16-bit registers have

Table B-1

DEFINITION OF COMMAND-BYTE BITS

Number	Name	Function
Ø	Go	Start clock when asserted; stop clock when not asserted
1	Tick select	Clock tick is 0.1 s when asserted; clock tick is 100 μs when not asserted
2	Clock select	Internal clock is disabled and external clock input is accepted when asserted
3	Diode data enable	Random byte from diode when asserted
4	Decay data enable	Random byte from β-decay when asserted
5	Pseudorandom data enable	Random byte from shift register when asserted
6	Interrupt enable	Enable interrupt from real-time clock when asserted
7	Not used	

been provided for data input to the LSI-11. The two bytes of word Ø contain the diode noise random data byte (LOB) and β-decay random data byte (HOB); Word 1 contains the input count rate for each source, respectively (LOB is the number of diode pulses per 10^{-3} s, and the HOB is the number of electrons per 10^{-2} s); Word 2 contains the diode temperature information and pseudorandom course data byte in the HOB and LOB, respectively, and Word 3 is unused. To convert the 8-bit temperature data to degrees centigrade, use the following relationship:

$$T = \text{data byte}/1280.0 \quad .$$

The data in a given word are strobed on to the Q-bus via the DRV11-P protocol and the 74LS32 decode OR gate. Data are clocked into the output

registers either by the selected data source bit in the command byte or from the strobes derived from the appropriate scalers.

d. Output from the LSI-11

Two output words may be latched into 74LS374 registers from the LSI-11 Q-bus. The LOB of Word Ø is the command byte described above. The HOB of this word is an 8-bit seed number for the pseudorandom shift register. Word 1 is a 16-bit integer representing the number of ticks that must elapse before the real-time clock causes an interrupt. The strobe logic from the 74LS02 NOR gate is determined by the DRVII-P protocol.

e. β-Decay Channel/Noise Diode Channel

Both random source channels are handled identically. A logic pulse from the optical receiver is presented to a 74LS123 one-shot with a reset time of approximately 50 ns. It is also presented to a second 74LS123 one-shot gated by a symmetric 1-kHz clock. This one-shot provides a 50-ns "dead zone" centered about either transition of a divide-by-two 74LS74. This ensures that when the 8-bit shift register (74LS164) is strobed by the 1-kHz clock, the register will not shift during a divide-by-two transition. This added logic feature eliminates a small bias in favor of a binary one state due to differential rise and fall times of TTL logic. The output of the shift register is 8 bits of random data toggling at 1 kHz. These data are presented to the appropriate input of the 74LS374 latches. Data from these latches are strobed onto the bus at the leading edge of the RTCP derived from the real-time clock time out.

f. Pseudorandom Shift Register

According to the Kendall algorithm[6] a pseudorandom 8-bit shift register may be constructed by feeding back the Mod 2 summation of a

number of output stages. Each number is generated by shifting the register $2^n - 1$ times, where n is the number of bits in the register. (Here, n = 8).

A 74LS93 counter is used to accumulate 8 clock pulses and a 74LS74 dc flip-flop is used to gate the oscillator to form the register shift pulse. When RTCP is asserted, 8 pulses are sent to the 8-bit shift register formed by two shift registers (7495). One 74LS86 performs the Mod 2 addition. The same signal that strobes the seed data from the Q-bus also latches the seed into the shift register parallel inputs. (The strobe is delayed by three 74LS04 inverters to allow stable operation.) Thus, one 8-bit pseudorandom number is generated with each RTCP.

g. Counters

The special interface board contains three 8-bit counters (74LS393) to count the diode, β-decay, and temperature data, respectively. Each counter is gated on for a different counting time, depending on the basic count rate of the source involved. Two 74LS04 inverters are used with each counter to allow time for the data to be strobed to the data output latches (74LS374) before the counter is cleared for the next cycle.

REFERENCES

1. R. H. Haitz, "Controlled Noise Generation with Avalanche Diodes I. Low Pulse Rate Design," IEEE Trans. on Electron Devices, Vol. 12 (April 1965).

2. R. H. Haitz, "Controlled Noise Generation with Avalanche Diodes II. High Pulse Rate Design," IEEE Trans. on Electron Devices, Vol. 13 (March 1966).

3. A. Wald, Sequential Analysis (Dover Publications, Inc., New York, N.Y., 1973).

4. M. Fisz, Probability Theory and Mathematical Statistics, pp. 584-611 (John Wiley & Sons, Inc., New York, N.Y., 1973).

5. S. W. Golomb, Shift Register Sequences (Holden-Day, Inc., San Francisco, CA, 1967).

6. T. G. Lewis, Distribution Sampling for Computer Simulation (Lexington Books, Lexington, MA, 1975).

7. R. H. Haitz, "Mechanisms Contributing to the Noise Pulse Rate of Avalanche Diodes," J. Appl. Phys., Vol. 36, No. 10, pp. 3123-3131 (1965).