DIGITAL COMMUNICATIONS FOR TELEPROTECTION

By:

Kenneth J. Fodero
Director Of Product Planning

RFL Electronics Inc.
Boonton, New Jersey

ABSTRACT

Until recently, communication and relay engineers have had two basic choices for teleprotection: powerline carrier (PLC) and audio tones over analog, microwave, or leased telephone circuits. With the wide acceptance of fiber optics and digital microwave, high-speed digital circuits are now available for use on transfer trip circuits that have traditionally been powerline carrier or audio tone. PLC is a natural for the utility industry, which is somewhat in control of the medium. However, with the available spectrum being reduced (either by frequency congestion or government agencies reallocating large chunks for use by others), it is becoming more and more difficult to apply.

Audio tones over leased circuits was a decent alternative to powerline carrier prior to the break-up of AT&T. Now, with many different companies controlling the Nation's telephone lines, there is a possibility that service reliability may be adversely affected. Even so-called dedicated lines can be handled by more than one carrier. Audio tones over utility-owned analog microwave is still a viable medium, and probably will be for years to come.

SOURCE: Reference Data For Engineers, Howard W. Sams & Co, Indianapolis, Indiana. Sixth Edition, Second Printing, 1977.

INTRODUCTION

The introduction of digital fiber optic and digital microwave systems makes it possible to offer true digital communications channels. Digital communication has been done in the past by digital/analog conversion circuits; these require the use of modems and are hard to make dependable at higher bit rates. The new technology now makes a new communications medium available for use with protective relays. Two advantages quickly realized from the new medium are higher operating speed and higher security (if implemented correctly). The use of bit rates of 56 Kb/s (56,000 bits/second) and higher makes it possible to add back the dependability which is typical of an analog system. This is accomplished by sending each command several times during a short time frame.

Along with digital communications devices came new methods of rating channel integrity. Where signal-to-noise (S/N) ratios were once used, now measurements of bit error rates (BER) appear. A typical BER used by the utility industry is $1x10^{-9}$. This means that out of 100,000,000 bits sent, one was received in error. This type of BER is typical for fiber optic systems. T1 carrier systems which are used over wire lines more typically average $1x10^{-8}$ BER, and digital microwave systems average about $1x10^{-9}$.

The currently-available basic digital channels are labeled by their maximum baud rate. Some of the most commonly-used rates are as follows:

9.6 Kb/s
19.2 Kb/s
56 Kb/s
64 Kb/s (DS0)
1.544 Mb/s (DS1, T1)
6.312 Mb/s (DS2, T2)
44.736 Mb/s (DS3, T3)

The rates listed above are, for purposes of this paper, considered to be high-speed, so 1200 and 2400 baud are intentionally left off.

Typically, there are twenty-four DS0 channels in a T1 channel, four DS1 channels in a T2 channel, and twenty-eight DS1 channels in a T3 channel.

The most commonly available line rates are T1 and its associated DS0 channels. If the equipment is intended for use over T1 carriers of all vendors, then it is wise to use a 56-Kb/s line rate, as the full 64 Kb/s is not always available for use.

Likewise, if the equipment is operating at a T1 rate and is intended for use over the public network or higher order multiplexers, the data format of the signal must be compatible.

If these systems are to be operated on their own internally-generated fiber optic systems, the data format is not a problem, because systems of this type do not require compatibility with other systems.

DIGITAL SYSTEMS FOR TRANSFER TRIP

In the past few years, more and more digital systems for transfer trip applications have become available in the United States. As with most new types of equipment, industry acceptance is slow and cautious.

Digital systems designed for transfer trip need to operate under worst-case conditions. The conventional method of rating transfer trip system performance is in terms of "security" and "dependability":

Security

A measure of the communications system's ability not to trip falsely under adverse signal conditions.

Dependability

A measure of the communications system's ability to receive and output trip commands during adverse signal conditions.

Methods for testing and documenting the security and dependability of audio tone transfer trip systems are well documented in the industry. However with digital systems this is not the case at the present time, but appropriate methods will be developed as more digital systems are installed.

Another critical design criteria for digital transfer trip equipment is its survivability in the substation environment. While in most utilities the microwave and fiber optic backbone systems are usually isolated from the relaying equipment, this is not the case for digital transfer trip equipment.

The communications equipment must conform to the same dielectric characteristics as the protective relays with which it operates. In almost all installations, the communications equipment will be located in the same rack as the relays, or very close to them. The dc input voltage source is split about 50/50 between station battery and comm battery, so the associated power supplies need to be substation hardened. Two IEEE/ANSI standards which should apply to all relay system interfaces as well as the dc input are C.37.90-1978 (Surge Withstand Capabilities) and C.37.90.1-1989 (Fast Transient). Circuits associated with data interfaces, telephone lines, and general voice communications probably are not required to meet these stringent isolation requirements, since current practice is to keep such wiring separate from control cables.

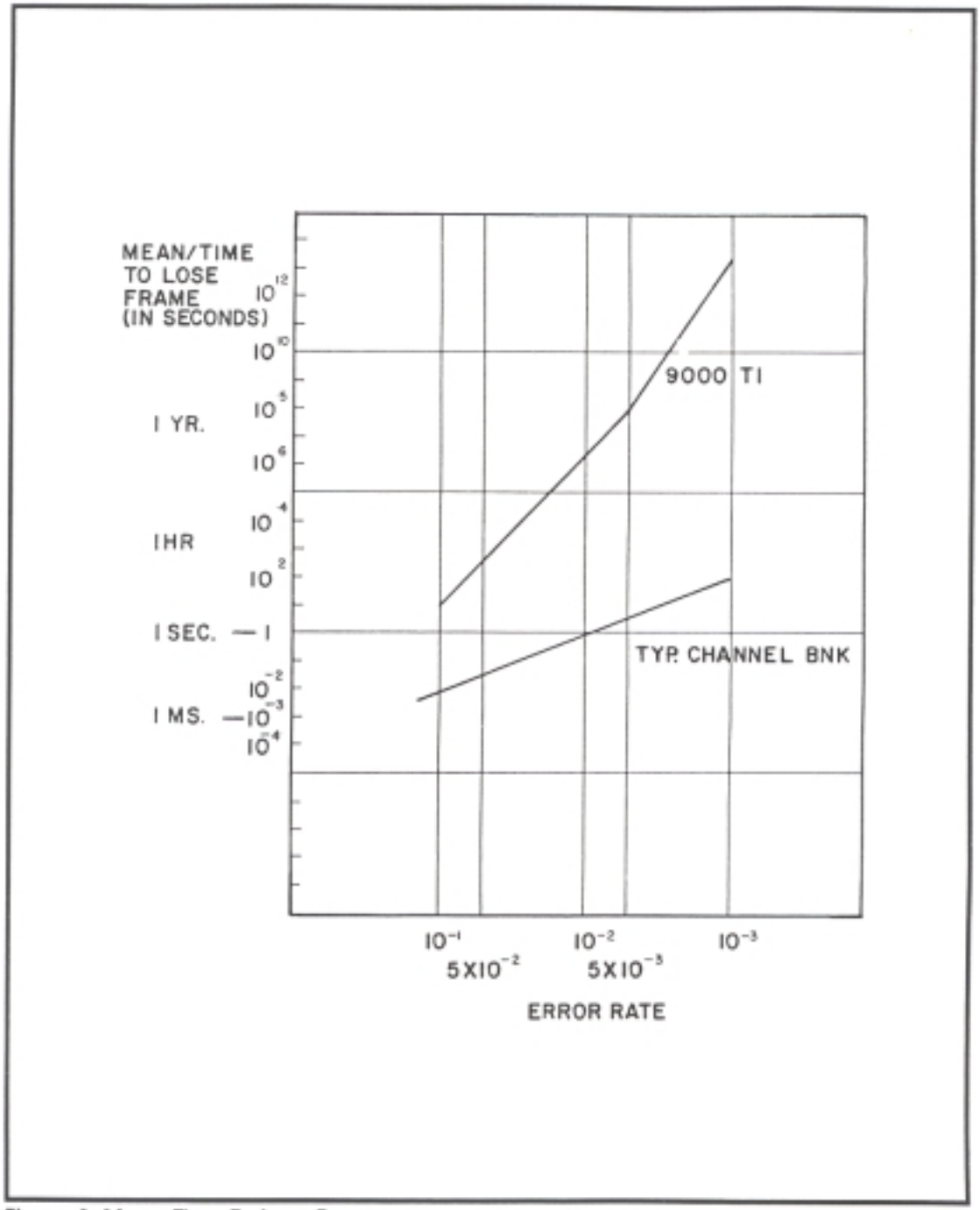

Figure 1. Mean Time To Lose Frame

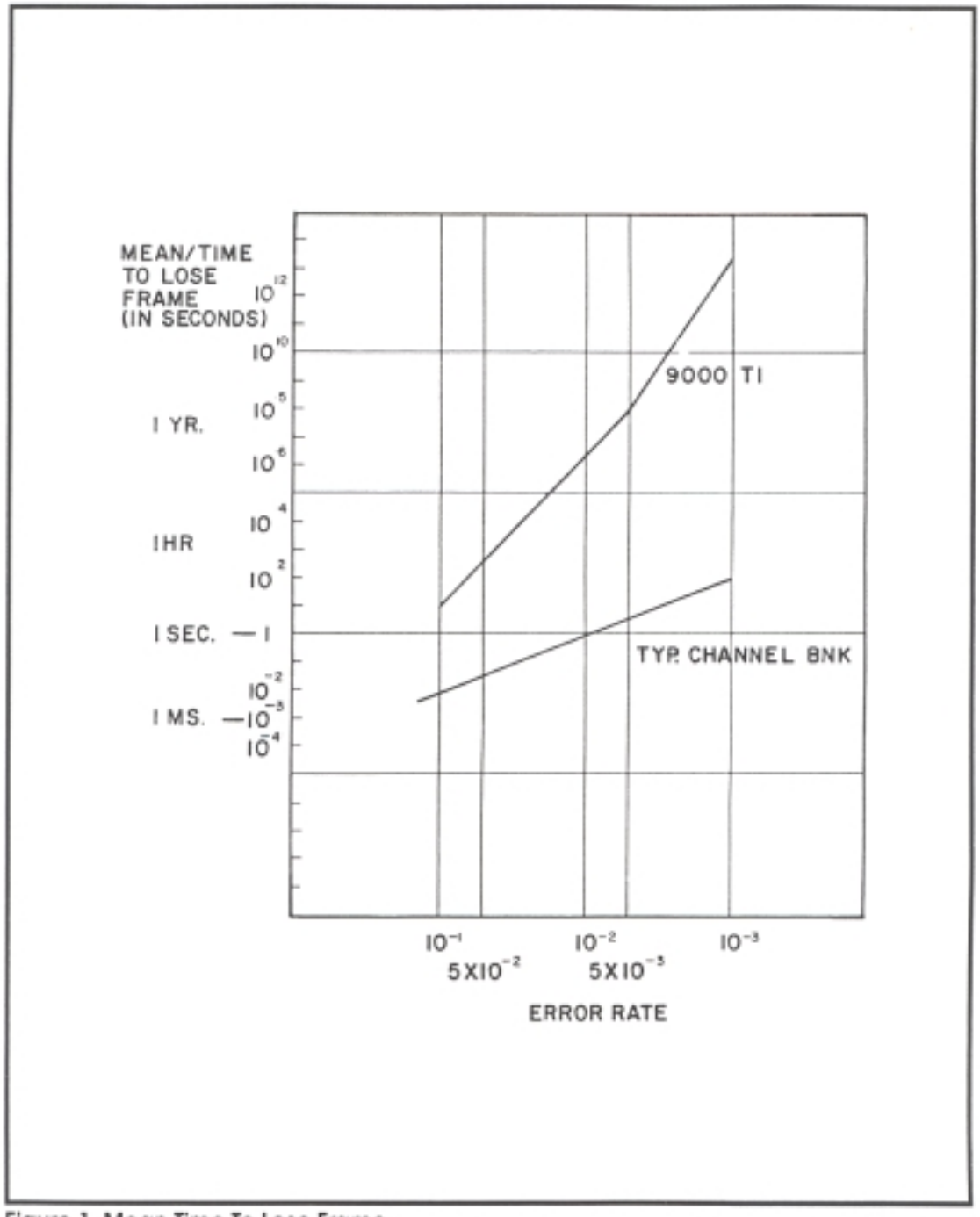

Figure 1. Mean Time To Lose Frame

In figure 1, the X axis is the time to lose frame in seconds and the Y axis is the bit error rate. Since bit errors do not occur every one millionth bit, for this plot a gaussian distribution of bit errors is calculated against the algorithm used by the multiplexer to determine loss of frame. Although there is little that can be done to overcome the typically long times required to reframe, it is possible to ensure that a system will stay in frame long enough to insure proper system operation.

One question which may be asked is: "If framed systems have such long reframe times, why use them?" The answer is simple: In order to be completely compatible with common carriers or higher-order multiplexers, this type of data configuration must be used. Since the T1 multiplexer was primarily designed for the telephone industry and this type of message structure suits their needs, there was no need for changing this technique.

SECURITY

For systems primarily designed for transfer trip applications (such as the RFL Model 9700), it is important to be able to rate them in terms of security and dependability. As an explanation, with tone systems the standards for testing security are such that the noise which is introduced into the tone lines is pulsed at a rate that allows the unit under test to be restored to its normal operating state between noise bursts.

With digital systems, a similar method of testing should be used. In our case, we are using a CRC word in the message to detect bit errors in the received message. The polynomial used in the Model 9700 is very secure with its most vulnerable state at four corrupted bits per message. With four corrupted bits, there are 22 out of 1001 combinations which could trick the CRC detection into accepting these occurrences as valid. The Model 9700 also has variable security settings, so for this test we used the most dependable setting, which is also the least secure. The Model 9700 also contains eight independent trip functions in each message, so all eight were monitored for false operations. The criteria to determine false operation was any output of 267 microseconds or longer.

In figure 2, security is plotted using two methods for the Y axis: hours to false trip, and false trips per corrupted message. The X axis is the bit error rate. It is important to note that although the curve is plotted to a BER of 10^{-1}, the channel squelch software shuts down the output circuits at about 10^{-4} BER.

The formula used to calculate the security of the system is based on the following assumptions:

1. For a given 14-bit message, four bits must be corrupted before there is any possibility of false data being sent to the outputs.

2. There are 1001 different four-bit corruption combinations possible, so for any single valid message, corrupting four bits yields a 22-out-of-1001 chance of being accepted.

Using these assumptions, the following formula is derived:

$$P_K = (N!/K!(N-K)!) \times P^K \times (1-P)^{N-K} \times (22/1001) \times (4/14) \times (1/2)$$

Where

P	= Bit error rate (BER)
N	= Number of bits in a message
K	= Number of corrupted bits in a message before it will be accepted
22/1001	= Number of chances that a corrupted message will be accepted as valid
4/14	= Chance that a corrupted bit will fall in a given channel
1/2	= Chance of setting the bit to a one or a zero
P_K	= Probability of a corrupted message passing a false trip on a given channel

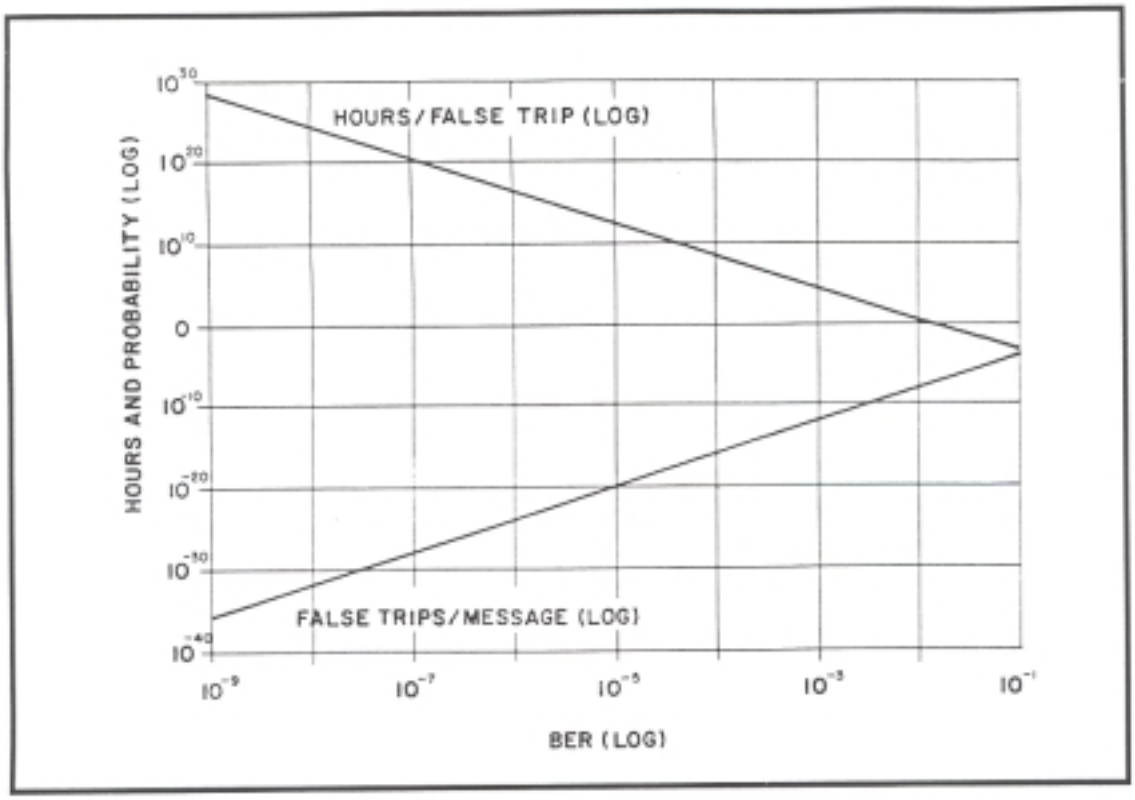

Figure 2. Security curve, RFL Model 9700 Digital Protection Channel

To convert data to false trips/hour, use the following formula:

False Trips/Hour = (False Trips/Message) x (Messages/Hour)

DEPENDABILITY

In audio tone systems, testing methods for dependability are well defined. In this type of testing, noise is gated on while simultaneously keying the unit under test to its trip state. The ability of the unit to detect the trip command in the presence of noise is plotted to illustrate its dependability.

For digital systems the test is very similar, except in this case noise is replaced with bit errors. In our Model 9700, the CRC detection circuit is set up so that one bit error is enough to discount the message in which the bit error was detected. Figure 3 depicts the dependability curve for the Model 9700. It is important to note that although the curve is plotted to a BER of 10^{-1}, the unit will not operate below 10^{-4} BER, due to the method used to determine a healthy channel. In figure 3, the Y axis is the probability of correctly outputting a trip, with 1 being equal to 100 percent; the X axis is the bit error rate.

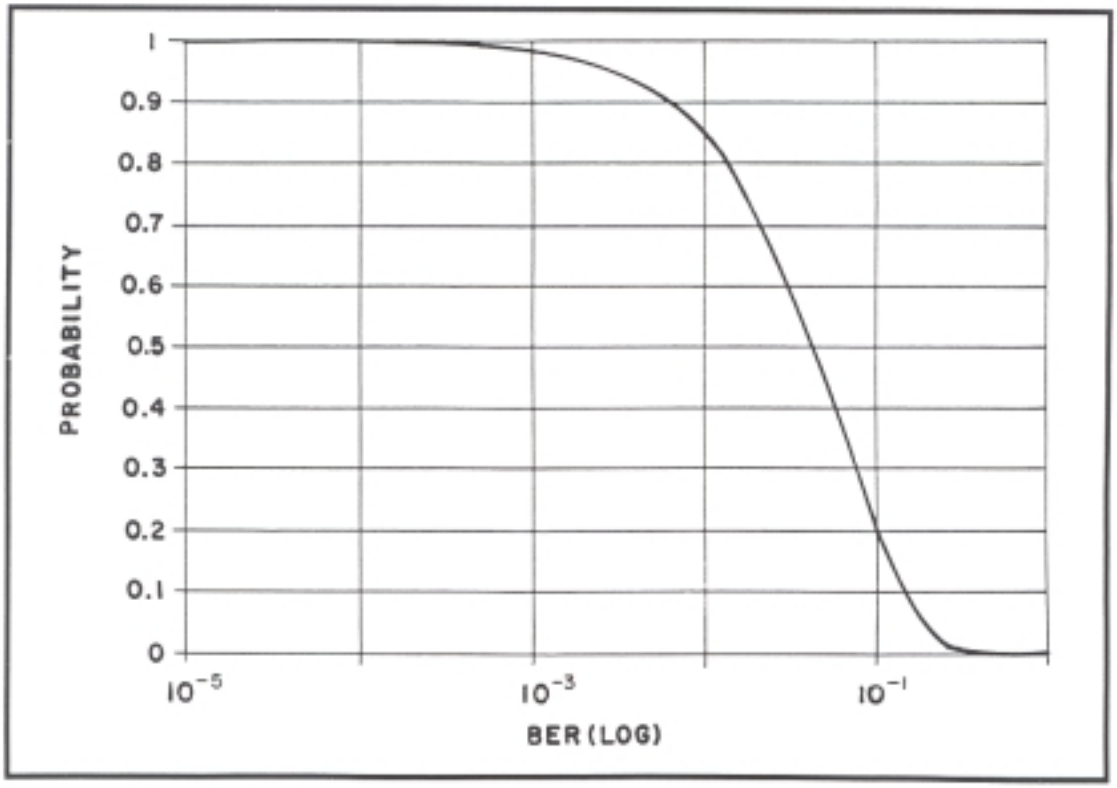

Figure 3. Dependability curve, RFL Model 9700 Digital Protection Channel

The calculations are based on the following assumptions:

1. For a given 14-bit message, the CRC test will prevent the data from being sent to the outputs if a bit is corrupted.

2. The calculation are made for the most-dependable channel setting. The data in one valid message will be directly outputted.

3. For the Model 9700, a trip is defined as an input lasting at least 100 microseconds. The internal trip buffer will extend the pulse to 2.3 milliseconds.

4. If three bad messages in ten are received, a software squelch is activated. Once it is activated, six good messages in a row must be received to reset the system (take it out of a hard block). Therefore, if one valid message is received in a string of three, a trip is received.

Calculating the probability of corrupting zero bits out of a string of fifteen is a "Binomial Distribution". The BER is taken into account in this expression.

Formula 1:

$$P_{k1} = \{(N!/K!(N-K)!) * P^K * (1-P)^{N-K}\} \quad 0 \leq K \leq N$$

Where

P	= Bit error rate (BER)
N	= Number of bits in a message
K	= Number of corrupted bits in a message before being accepted
P_{k1}	= Probability of a message passing a trip on a given channel

If there are no corrupted bits (K = 0), then $(N!/K!(N-K)!) = 1$

and $P^K = 1$

so therefore $P_{K1} = (1-P)^N$

Formula 2:

$$P_{k2} = 1-\{1-(1-P_{k1})\}^n$$

Where

P_{k2}	= Probability of a signal passing a trip on a given channel.
P_{k1}	= Message dependability
N	= Number of messages in a signal

Although the Model 9700 does not operate below a BER of 10^{-4}, this region is a very important part of the dependability curve. Obviously, these curves are derived by calculation; it would be difficult to run a security test for thirty years. In order to prove the validity of the calculated curves, we disabled the CRC error detection in the system and ran the security and dependability tests. The formulas used take into account error combinations that are most likely to get past the CRC detection circuit, so performing these tests in this manner is viable. By doing this, we are able to plot the lower portion of the curves, adding confidence in the formulas; that is, if the calculated and tested data agrees.

The next type of curve which we generated is a plot of the fiber optic receiver sensitivity (fig. 4). In this curve, we plot the input signal strength in dB-average on the X axis and the bit error rate which is produced by the receiver on the Y axis. When rating receiver sensitivity, it is important that this number be tied to a bit error rate. For our systems, we have chosen to use a BER of 10^{6} to rate our modules; this is due to the fact that our systems operate very well at this BER. Although we could have stopped plotting at 10^{6}, we felt that this information would be very helpful in troubleshooting installed systems, should the fiber system deteriorate over time.

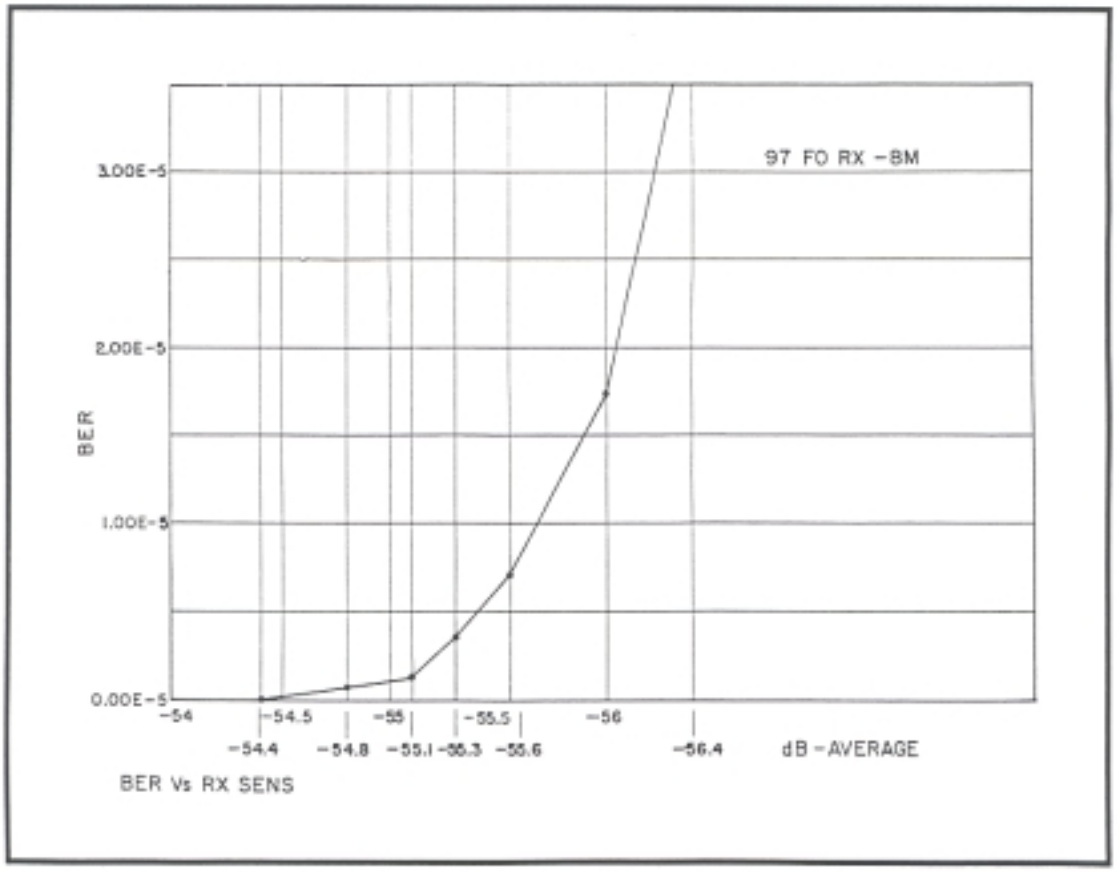

Figure 4. Fiber optic receiver sensitivity, RFL Model 9700 Digital Protection System

OTHER CONSIDERATIONS

CRC error detection was originally designed to check large data messages. In our case, we send a CRC check with every message. Each message which contains the eight transfer trip functions and the CRC bits is 267 microseconds long. This allows many messages to be sent during a trip condition, taking full advantage of the number of messages being received in a short period. If a CRC error is detected in a message, that message is discarded and no attempt is made to use the CRC information for error correction, which is another common use of CRC detection schemes.

In protection schemes, there comes a time during disturbed channel conditions in which the communications system should go into a hard squelch. Our system runs a shift register which clocks in the CRC checks for the last ten messages. If an error is detected in three of the ten messages, the system will go into a hard squelch. In order to restore the channel, six correct CRC checks in a row must be detected.

Although the CRC error detection scheme works very well, it is not enough by itself. There are a few other considerations which need to be made. If the transmitter were to suffer from component failures, it is not inconceivable that it could send trip signals in error, which means that the proper CRC code would be calculated for the bad message. In our system, all data is compared against the input status prior to being sent. Should this check fail to compare, a message which is deliberately corrupted and easily detected as an error is sent.

Systems which operate synchronously also require some type of sync-check detection scheme.

Even with all of the extra measures taken to ensure that the communications system is secure and reliable, it is still necessary to use additional logic. The additional logic is required to make this communication system fully compatible with the relaying schemes in which it is intended to work. One example would be logic for unblocking relay schemes, where on loss of channel the system would respond by opening a trip window and force a trip for about 150 ms.

CONCLUSION

When using a transfer trip system with a digital communications medium, digital transfer trip equipment is a viable alternative. The equipment used must be designed to operate in accordance with all of the considerations required for transfer trip applications. There are also many advantages to using digital systems, including increased system availability and performance. This makes digital systems an intelligent choice for these applications.

RFL Electronics Inc.

353 Powerville Road, Boonton Township, New Jersey 07005, USA
Phone: (201) 334-3100 Fax: (201) 334-3863