Power line communication systems for industrial control applications

Thesis

'Power Line Communication Systems for Industrial Control Applications'

by

Kerry John Morris

BA(Hons), MBCS

A Thesis submitted to the

OPEN UNIVERSITY

Faculty of Technology

Discipline of Electronics

For the degree of

DOCTOR of PHILOSOPHY

December 2001

'Power Line Communication Systems for Industrial Control Applications'

by

Kerry John Morris

BA(Hons), MBCS

A Thesis submitted to the

OPEN UNIVERSITY

Faculty of Technology

Discipline of Electronics

For the degree of

DOCTOR of PHILOSOPHY

December 2001

Acknowledgements

The author thanks his employer, Elcontrol Limited, for financially sponsoring the period of this research.

Special thanks are also due to the author's supervisor, Dr John E Newbury, B.Sc, Ph.D, F.B.I.P.S, M.Inst.P, F.R.A.S. of the Open University, for his patient help and guidance.

And last, but not least, thanks to my wife Janice, and children, Owen and Gillian, for their patience, support and understanding.

Memorandum

All work and ideas recorded in this dissertation are original unless otherwise acknowledged in the text or by reference. The work has not been submitted in support of an application for another degree in this university, nor for any degree or diploma at any other institution.

Table of Contents

EX12

THE OPEN UNIVERSITY

RESEARCH SCHOOL

Library Authorisation Form

Please return this form to the Research School with the two bound copies of your thesis to be deposited with the University Library. All candidates should complete parts one and two of the form. Part three only applies to PhD candidates.

Part One: Candidates Details

Name: KERRY JOHN MORRIS PI: M 1793983

Degree: PhD

Thesis title: POWER LINE COMMUNICATION SYSTEMS FOR INDUSTRIAL CONTROL APPLICATIONS

Part Two: Open University Library Authorisation

I confirm that I am willing for my thesis to be made available to readers by the Open University Library, and that it may be photocopied, subject to the discretion of the Librarian.

Signed: ..... Date: 28/01/2002

Part Three: British Library Authorisation [PhD candidates only]

If you want a copy of your PhD thesis to be available on loan to the British Library Thesis Service as and when it is requested, you must sign a British Library Doctoral Thesis Agreement Form. Please return it to the Research School with this form. The British Library will publicise the details of your thesis and may request a copy on loan from the University Library. Information on the presentation of the thesis is given in the Agreement Form.

Please note the British Library have requested that theses should be printed on one side only to enable them to produce a clear microfilm. The Open University Library sends the fully bound copy of theses to the British Library.

The University has agreed that your participation in the British Library Thesis Service should be voluntary. Please tick either (a) or (b) to indicate your intentions.

☒ I am willing for the Open University to loan the British Library a copy of my thesis.
A signed Agreement Form is attached

☐ I do not wish the Open University to loan the British Library a copy of my thesis.

Signed: ..... Date: 28/01/2002

Abstract

For almost as long as the electricity distribution industry itself has existed, so also has the idea of utilising the transmission grid, be it over a wide area or on a local basis, for the transmission of 'intelligence'. This might be in the form of voice transmissions, or for the purposes of monitoring or controlling electrical devices attached to the network.

This thesis specifically concerns itself with the potential applications of power-line-carrier (PLC) communications technology within the field of industrial plant/equipment control, as it is within this field that the author works.

We look at the entire subject area of industrial control, starting from a historical viewpoint, and consider the special needs and requirements that a proposed PLC solution must offer for this application, especially based on the noise conditions likely to be experienced on a 'real' power line.

A proposal is made for a 'Power Bus', intended for use within certain areas of industrial control, and decisions are made based on the projected link response times for such applications.

The experimental phase of the research is practical in nature and consists of a raft of tests and evaluations of the performance of power line modem technologies, under controlled and repeatable noise conditions. To complement these results, further tests are carried out under 'real world' conditions, within an actual factory environment.

Based on the results of all of these tests, the suitability of a PLC solution for this type of industrial control application is considered.

The Thesis concludes with a look at recent developments in, as well as the future of, Power Line Communication techniques.

Summary

The work contained within this Thesis commences with a discussion of the historical perspectives of the subject area - the origins of electricity generation and the electrical distribution industry, before moving on to consider the modern Electricity Distribution Network.

We next look at some early developments in power line communications, then at uses of PLC in the electrical distribution industry, including techniques such as Cyclocontrol, Ripple Control, and TWACS.

We conclude Chapter 1 with a look at the development of meter reading techniques, and the de-regulation of the utilities industry which has prompted the need for real-time automatic meter reading technologies, such as those utilising PLC. Finally, the context is outlined for the rest of the Thesis and the experimental work.

Chapter 2 considers the development of industrial and home automation, beginning with a look at the history of industrial automation and a description of the increasing adoption of modern technologies as we move towards the present day. The evolutionary path of relay-based controllers, to electronic control, to programmable logic controllers, to industrial computers is described.

Home and building automation is introduced, before we describe some of the transmission media applicable to such applications. Chapter 2 concludes with a discussion of some current home and building automation systems.

In Chapter 3 we look at the history of computer networking, up to the present day, and discuss typical networking systems and topologies. We then look at the OSI model for general networking systems, before considering how this model might be simplified in an industrial networking context. Chapter 3 concludes with a look at the well-known high-level industrial networks, MAP and TOP.

In Chapter 4, we introduce the idea of lower-level industrial networking, local control networks, and the emerging Fieldbus concept. Several current Fieldbus systems are described, and the Chapter concludes with a look at moves towards Fieldbus interoperability.

In Chapter 5 the characteristics of the power line from a communications viewpoint are discussed. We begin with a discussion of the many and varied sources of signal degradation and noise to be found on the power line, then discuss the relevant aspects of the EMC testing standards that are applicable. We conclude Chapter 5 with a look at filtering techniques that have the potential to simplify the task of power line communication.

In Chapter 6, we look at some power line communication techniques, before considering the family of standards that are evolving to cover the subject area.

The need for protocols is discussed, and we describe the different techniques for transmission error detection and correction. After considering the structure of a 'typical' data packet, we look at the data rates required for industrial control, and then introduce the 'Power Bus' concept, and its potential applications.

Chapter 7 describes the experimental work in detail, the nature of the tests carried out, the development of the specialised 'BERT' test equipment, detailed information regarding the two specific power line modems used, and the subsequent processing of the experimental data.

In Chapter 8, the experimental results are described, analysed, and conclusions are drawn.

Chapter 9 considers the future directions in which the research effort could be pursued, and proposes further lines of experimentation, and developments to the BERT equipment. To conclude the chapter, we have an overview of the advantages and disadvantages of more recent developments in PLC - high speed systems operating at high frequencies, before finally looking at the emerging concept of a 'Web Connected Appliance'.

CEPT	*European Conference of Postal and Telecommunications Administrations*
CISPR	*'Comite International Special des Perterbations Radioelectriques' (International Special Committee on Radio Interference)*
CPU	*Central Processing Unit*
CSMA	*Carrier Sense Multiple Access*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
CSMA/CD	*Carrier Sense Multiple Access with Collision Detect*
CSV	*Comma Separated Values*
DC	*Direct Current*
DCS	*Distributed Control System*
DLC	*Distribution Line Carrier*
DLL	*Data Link Layer*
DPSK	*Differential Phase Shift Keying*
DS-SS	*Direct Sequence Spread Spectrum*
EDT	*Electronic Data Transfer*
EIA	*Electrical Industries Association*
EMC	*Electromagnetic Compatibility.*
EMS	*Energy Management System*
EN	*European Norm*
ESD	*Electrostatic Discharge*
EUT	*Equipment Under Test*
FH-SS	*Frequency Hopping Spread Spectrum*
FIP	*Factory Information Bus*
FM	*Frequency Modulation*
FSK	*Frequency Shift Keying*
FTB	*Fast Transient Burst*

FTP	*File Transfer Protocol*
HART	*Highway Addressable Remote Transducer*
HBES	*Home and Building Electronic Systems*
HDLC	*High-level Data Link Control*
HF	*High Frequency*
HLL	*High Level Language*
HTTP	*Hypertext Transfer Protocol*
HV	*High Voltage*
HVAC	*Heating, Ventilating, Air-Conditioning*
IC	*Integrated Circuit*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronic Engineers*
IF	*Intermediate Frequency*
I/O	*Input / Output*
IP	*Internet Protocol*
IR	*Infra-Red*
IS	*Intrinsically Safe*
ISA	*Instrumentation Society of America*
ISDN	*Integrated Services Digital Network*
ISM	*Industrial, Scientific and Medical*
ISO	*International Standards Organisation*
ISR	*Interrupt Service Routine*
IT	*Information Technology*
LAN	*Local Area Network*
LF	*Low Frequency*
LLC	*Logical Link Control*

LON	*Local Operating Network*
LSB	*Least Significant Byte*
LV	*Low Voltage*
MAC	*Medium Access Control*
MAP	*Manufacturing Automation Protocol*
MF	*Medium Frequency*
MODEM	*Modulator/Demodulator*
MSB	*Most Significant Byte*
MV	*Medium Voltage*
NRZ	*Non-Return to Zero*
NRZI	*Non-Return to Zero Inverted*
OFDM	*Orthogonal Frequency Division Multiplex*
OOK	*On-Off Keying*
OSI	*Open Systems Interconnection*
PC	*Personal Computer*
PCB	*Printed Circuit Board*
PLC	*Power Line Carrier*
PLC	*Programmable Logic Controller*
PLL	*Phase-Locked Loop*
PM	*Phase Modulation*
PNA	*Phone-line Networking Alliance*
POTS	*Plain Old Telephone System*
PSK	*Phase-shift keying*
RF	*Radio Frequency*
RISC	*Reduced Instruction Set Computer*
RMR	*Remote Meter Reading*

RMS	*Root Mean Squared*
RSGB	*Radio Society of Great Britain*
Rx	*Receive, Receiver*
S-FSK	*Spread Frequency Shift Keying*
SMTP	*Simple Message Transfer Protocol*
SSB	*Single Side-band*
STP	*Shielded Twisted Pair*
TC	*Technical Committee*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TOP	*Technical and Office Protocol*
TP	*Twisted Pair*
TWACS	*Two Way Automatic Communication System*
Tx	*Transmit, Transmitter*
UART	*Universal Asynchronous Receiver / Transmitter*
UTP	*Unshielded Twisted Pair*
WAN	*Wide Area Network*
WWW	*World Wide Web*

Other Terminology in Power Line Communications

Term	Definition
Power Line Carrier:	A generic term for the technology encompassing data communications using the power line as the medium.
Mainsborne Signalling:	Two-way data transmission on the power line medium, over the part of the circuit on the secondary side of the distribution transformer.
Distribution Line Carrier:	Two-way data transmission over the electricity distribution network from, and including, the customers' premises up to the Grid Supply Point.
Transmission Line Carrier:	Two-way data transmission over the electricity transmission network.
Domestic Bus:	Network within domestic premises for the transmission of data and control signals between intelligent devices and appliances.
Telecontrol:	Literally, remote control.
Telemetry:	Literally, remote metering.
Automation:	The concept of making certain tasks automatic.

Chapter 1 : Introduction

To begin this Thesis, we will look at some of the historical background surrounding the subject area of this research – Power Line Communications.

There have been attempts to utilise the power line for telecontrol functions for almost as long as there has been an electricity industry. We will mention these early efforts later, but first let us consider the phenomenon on which it all relies - electricity, and the technologies which evolved to make practical use of the phenomenon – those of electrical generation and distribution.

1.1 A Historical Perspective and Early Electrical Discoveries

Without knowing exactly what it was, the effects of electricity (for example, lightning) have been observed by man for thousands of years. The word electricity itself comes from the Latin term *electricus*, meaning to 'produce from amber by friction'. This is a reference to early experiments by the Greeks, whereby static electricity was generated, and its effects observed, using the technique of rubbing amber rods with cloth.

After these very early discoveries, we must wait until the 18th Century before any significant further progress in electrical research is made. Here are some milestones leading to the harnessing of electricity in the service of man:

- **1729** Gray discovers that electricity can be conducted.
- **1745** Von Kleist invents the 'Leyden Jar', an early form of electrical capacitor, capable of holding an electrical charge.

- **1747** on Franklin starts work with static charges and postulates the existence of an *electrical fluid* that might be composed of particles. In 1750 he discovers that lightning is the same as an electrical discharge, and proposes lightning rods that would draw this charge away from homes, making them safer and less prone to fires.

- **1799** Volta proves the principle of the electric cell and battery - the first continuous and controlled source of electricity.

- **1820** Oersted and Ampere independently discover the relationship between electricity and magnetism by observing that electrical currents effected the needle on a compass.

- **1827** Henry discovers the concept of electrical inductance and builds one of the first electric motors.

- **1827** Ohm discovers the law relating potential, current, and circuit resistance.

- **1831** Faraday discovers electromagnetic induction - the principle upon which electrical generators rely.

1.2 The Beginnings of the Electrical Distribution Industry

After Faraday had discovered the principle of electromagnetic induction, it soon became feasible to construct practical and powerful electrical generators. By the mid-19th century, the potential of electricity as a source of power and illumination had begun to be recognized, and early, small-scale electricity generation facilities had appeared. The concept of a *public* electricity utility did not appear until some twenty years later, prompted by other developments such as the incandescent lamp.

In 1878 St George Lane-Fox in the UK and Edison in the USA proposed systems to supply electrical energy for lighting to customers, and in 1882 the first power-stations began operation in both London and New York. In these early years, there was a proliferation of independent electricity suppliers, often resulting in technical incompatibilities between their generating systems.

A major question was whether to use direct current (DC) or alternating current (AC) transmission. Low-voltage DC systems were inefficient, since substantial amounts of power were lost in the cabling. Alternating current, by contrast, could be easily transformed to higher voltages for transmission, resulting in far less power loss and permitting the electricity to be sent over long distances with relative ease.

The first practical AC transmission system was designed by a German engineer, von Miller, and it began operation in 1891. DC supply and transmission systems persisted well into the 20th Century, but were eventually ousted by AC for general consumer use. The economies of scale brought about by high-voltage AC transmission would eventually lead to low-cost electricity supplies in most industrialized countries.

In the UK, the Central Electricity Board was created in 1925, to act as a coordinating and controlling body for the supply of electricity, and in 1927 work was begun on the national grid network that adapts electricity supply to suit demand. The grid consists of a common, shared, network of transmission lines connecting all electricity producers and consumers, allowing peak loads in one area to be met by electricity generated in another. All the power stations on the grid share the load. The grid system will be discussed further in the next section, when we consider the structure of the modern electricity distribution network.

1.3 The Modern Electricity Distribution Network

The whole basis of the distribution network is optimising the efficiency of electricity supply and transfer. We have already mentioned the fact that the adoption of AC transmission was a key factor in the development of efficient electricity transmission, since it permitted electricity to be transmitted over long distances with minimal losses.

Ohms' law tells us that for a given resistance of transmission line, the loss is proportional to the current flowing ($P = I^2 \times R$). Therefore, for a given amount of power being transmitted ($P = V \times I$), the higher the voltage, the lower the current, and the lower the transmission losses. Against these benefits must be weighed the increased difficulty (and costs) of transmission at higher voltages, and the hazards of taking such voltages into populated areas. Therefore, in practice, a stepped system is implemented, where voltages are stepped up for wide-scale distribution, then stepped down (progressively) to the final voltage levels used by consumers.

In the UK (see Figure 1), the output voltage from Power Stations lies in the range 11 kV - 33 kV. For distribution nationally, over the 'Supergrid', this is stepped up to 275 kV or 400 kV, or, for more local distribution, to 132 kV. Likewise, power from the 'Supergrid' is stepped down to 132 kV, then to 33 kV, with a further drop, to 11 kV, as we move towards the final end user. Large users may take this voltage (33 kV or 11 kV) directly, into their own substations, or, more generally, the voltage is stepped down at local sub-stations to the familiar 230 V (phase to neutral), or 415 V (phase to phase), for final distribution to users. Note also, that in some industrial applications a further voltage standard of 110 V is encountered. This is usually derived locally from one of the standard LV supplies using transformers.

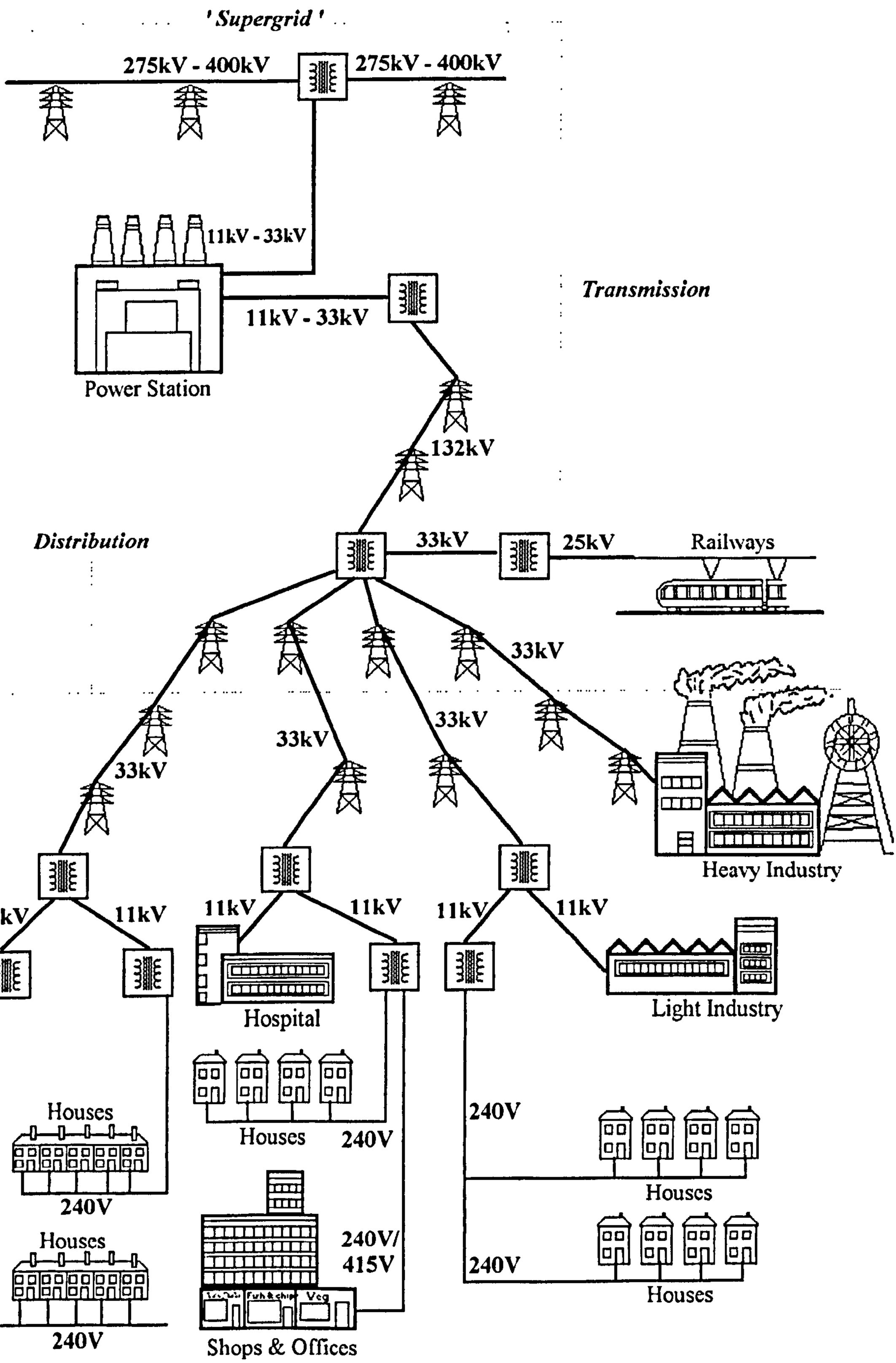


Figure 1: The Electricity Distribution Network

Having described the structure of the power distribution network, We will next consider early developments in PLC, and also some of the uses to which it is put in the present day by the electrical utility companies.

1.4 Early Developments in Power Line Communications

It is interesting to consider the fact that, within less than twenty years of the first electricity supply network being created, Swiss inventors Routin and Brown had submitted a patent (in 1896) proposing utilising a form of power line communication as a means of controlling street lighting [1].

After this early start, the next milestone in the PLC field occurred once national grid systems had started to be introduced. By the 1930s, telephone signals were routinely being transmitted along the HV power distribution network between sub-stations, providing communications facilities for the electricity companies [2]. The technique was even proposed as a means of providing a commercial telephone service in rural areas in the USA [3]. These techniques utilised a modulated HF carrier frequency to carry the speech signal, and indeed, similar techniques are still used today by electricity companies for in-house communications purposes.

On a more local level, i.e. over the low and medium voltage distribution network, PLC techniques have been utilised by utility companies for various purposes. These include remote switching (for example, to activate equipment running on an 'off-peak' electricity tariff), load shedding (turning off certain equipment when the network loading is excessive), and automatic meter reading. These applications will be discussed in greater detail in subsequent sections.

At the level of the consumer (i.e. over the 230/415 V network) perhaps the commonest early use of PLC was to provide voice intercom facilities within the home, without the need to run additional wiring. These tended to utilise a frequency modulated (FM) high frequency carrier, or perhaps several discrete carrier frequencies, giving the option of channelisation, i.e. allowing several simultaneous conversations, or for more than one system to co-exist on the same power circuit.

It is notable that the transmission of speech over the power lines represents a fairly noise-tolerant technique, since it is essentially 'person-to-person'. The human brain is capable of 'decoding' and understanding the 'intelligence' in such a signal, even in the presence of high noise levels. Such advantages do not apply when we wish to use the power line for sending digital signals that will be acted upon automatically, without any human intervention.

1.4.1 PLC in the Electricity Distribution Network

We have already mentioned some applications of PLC in the electricity distribution industry, such as remote switching and load shedding. We will now look at some techniques utilised for these purposes – specifically, Cyclocontrol, Ripple Control, and a more modern solution TWACS.

1.4.2 Cyclocontrol

Cyclocontrol was originally developed by the London Electricity Board [4]. It can be considered as a 'base-band' technique insofar as no modulation of a carrier frequency is involved. Cyclocontrol operates by using controlled short circuits applied to the low voltage power line, within 1.4ms of the zero-crossing points of the mains cycle.

The presence of the short circuit indicates a logic state of '1' and the absence, a logic state of '0'. Since there are two zero-crossings per mains cycle, this implies a signalling rate of 100 bits-per-second (bps) maximum (for a 50 Hz mains frequency).

The nature of the technique (requiring high power switching devices to apply the controlled short circuits) makes it impractical for use, except in a one-way 'broadcast' scenario, with messages originating from the electricity supplier and received by suitably equipped users.

Therefore, the typical uses for Cyclocontrol are those that lend themselves to a one-way communications link such as load shedding and off-peak switching. The nature of the Cyclocontrol signal means that it is able to pass through distribution transformers. It can therefore be injected into the grid at the 230 / 415 V level and will propagate through the 11 kV network, then back down to the consumer at the 230 / 415 V level.

We will next look in more detail at the Cyclocontrol switching waveform, both how it is generated, and how it is detected.

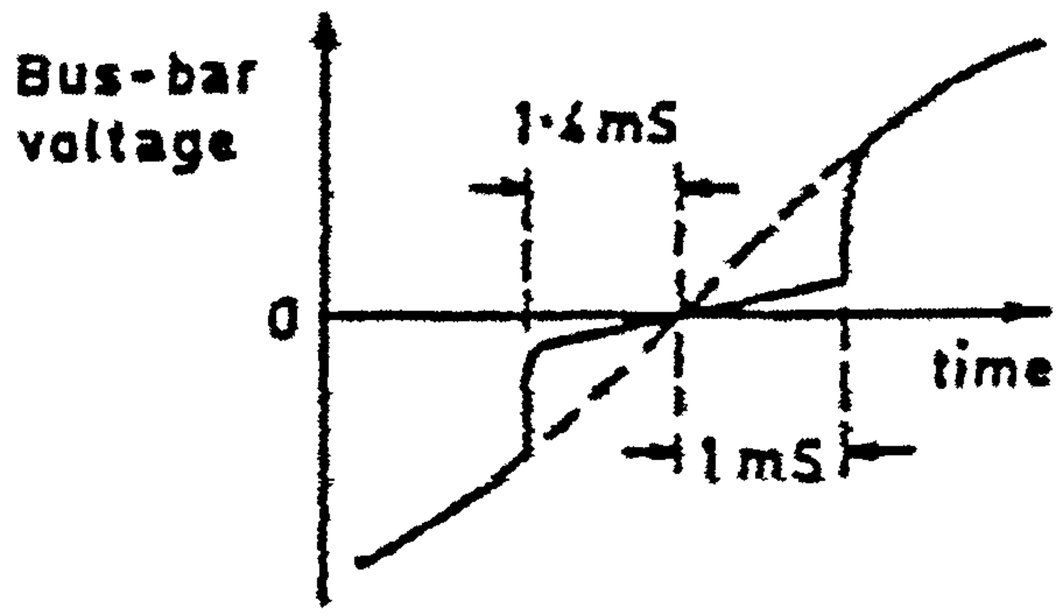


Figure 2: Cyclocontrol Transmit Voltage Waveform

The previous figure shows details of the Cyclocontrol transmit waveform, around the mains voltage zero-crossing point. The controlled short circuit is typically applied using a Thyristor (a semiconductor solid-state switch). This will cause the sudden voltage drop shown in the above figure at 1.4 ms before the zero voltage crossing point. Note that the waveform can equally be represented as mirrored about the time axis, depending upon the polarity of the mains half-cycle as it approaches the zero voltage point.

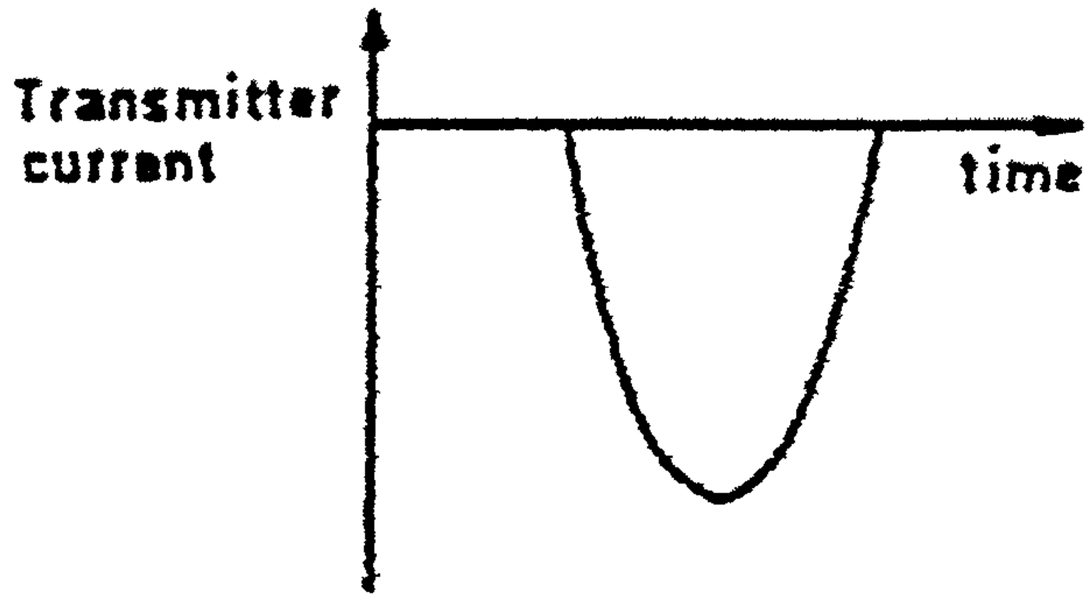


Figure 3: Cyclocontrol Transmit Current Waveform

When it fires, the current through the Thyristor will rise initially, as shown above, then begin to tail off as the mains voltage passes through the zero crossing point. The Thyristor will remain in the conductive state until the current flow through it drops below a certain low threshold value. This point is reached approximately 1 ms after the zero voltage crossing point due to inductive lag in the system.

We have already mentioned that the Cyclocontrol signal can pass through distribution transformers. In doing so, a great deal of the HF components of the waveform are lost, leaving a signal having a relatively small perturbation in the voltage waveform around the zero crossing point. This situation is illustrated in the next figure.

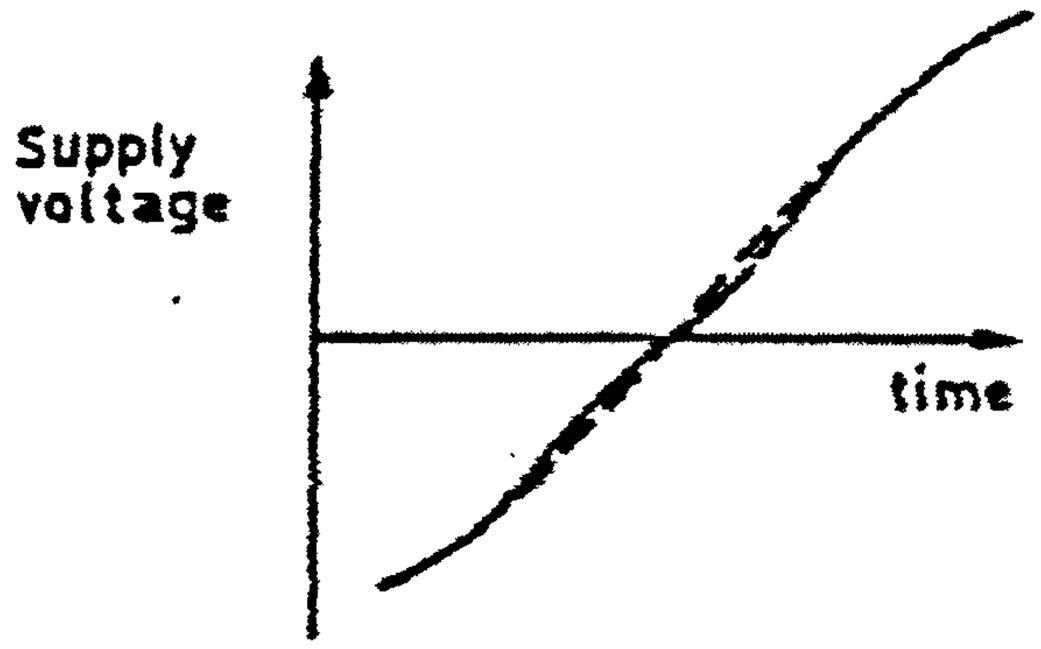


Figure 4: Attenuated Cyclocontrol Signal at Receiver

Detecting the Cyclocontrol signal, especially when it is so attenuated, presents a challenge, but can be achieved by a process of integration. This concept is shown in the next figure.

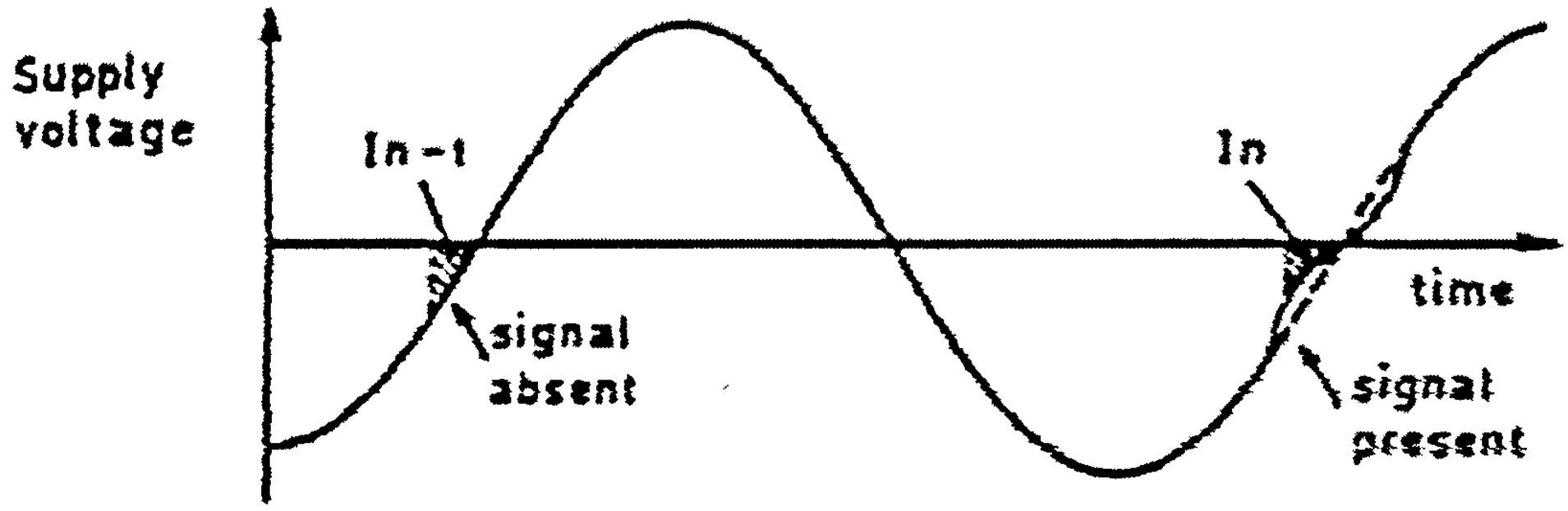


Figure 5: Detecting the Cyclocontrol Signal

The receiver monitors the voltage waveform from 1.4 ms before, and up to the zero crossing point, and calculates the integral function (shown as the shaded area in the diagram). These values are processed as follows: Should the latest integral value be *less* than the one measured during the previous half cycle, then the latest value must be a logic '1'. If the latest integral value is *greater* than the previous value, then the latest value must be a logic '0'. If the value is unchanged then the latest value must be the same as the previous value.

Next, we will look at a more sophisticated PLC technique - Ripple Control.

1.4.3 Ripple Control

Ripple control is another long established PLC technique. Here, low frequency signals, in the range 110 Hz - 750 Hz (at spot carrier frequencies chosen, with some exceptions at higher frequencies, to avoid interference from harmonics of the mains frequency) are superimposed on the mains cycle.

Again, this may be done at various voltage levels in the grid system appropriate to the application, as the signal will propagate through the distribution transformers. The signals are modulated using a pulse-coding scheme, with logic '1' being represented by a few cycles of the carrier frequency.

HARMONIC (Hz) (for 50Hz mains)	100		150				200		
ALLOWABLE HARMONIC LEVEL (%)	1.5		4				0.76		
CONTROL FREQUENCY (Hz)		110		168	183	194		206	217
RECOMMENDABLE RIPPLE LEVEL(%)		1.7		1.7	3	2		2	3

HARMONIC (Hz)		250			300		350		400
ALLOWABLE HARMONIC LEVEL (%)		5			0.51		4		0.39
CONTROL FREQUENCY (Hz)	228		270	283		317		383	
RECOMMENDED RIPPLE LEVEL(%)	2		3	3		3		3	

HARMONIC (Hz)		450		500	550	600	650	700	750
ALLOWABLE HARMONIC LEVEL (%)		0.67		0.32	3	0.27	2.1	0.23	0.30
CONTROL FREQUENCY (Hz)	425		485			600			750
RECOMMENDED RIPPLE LEVEL(%)	3		4			4			4

Figure 6: Ripple Control Frequencies and Amplitudes vs. Mains Harmonics

The previous table shows the various mains harmonic frequencies (for a 50 Hz mains frequency), with the recommended maximum level for each harmonic, and also the ripple control frequencies, with their recommended levels. It can be seen that where the ripple frequencies and harmonic frequencies coincide (600 & 750 Hz) the permissible mains harmonic level is significantly lower than the ripple level, permitting detection to occur.

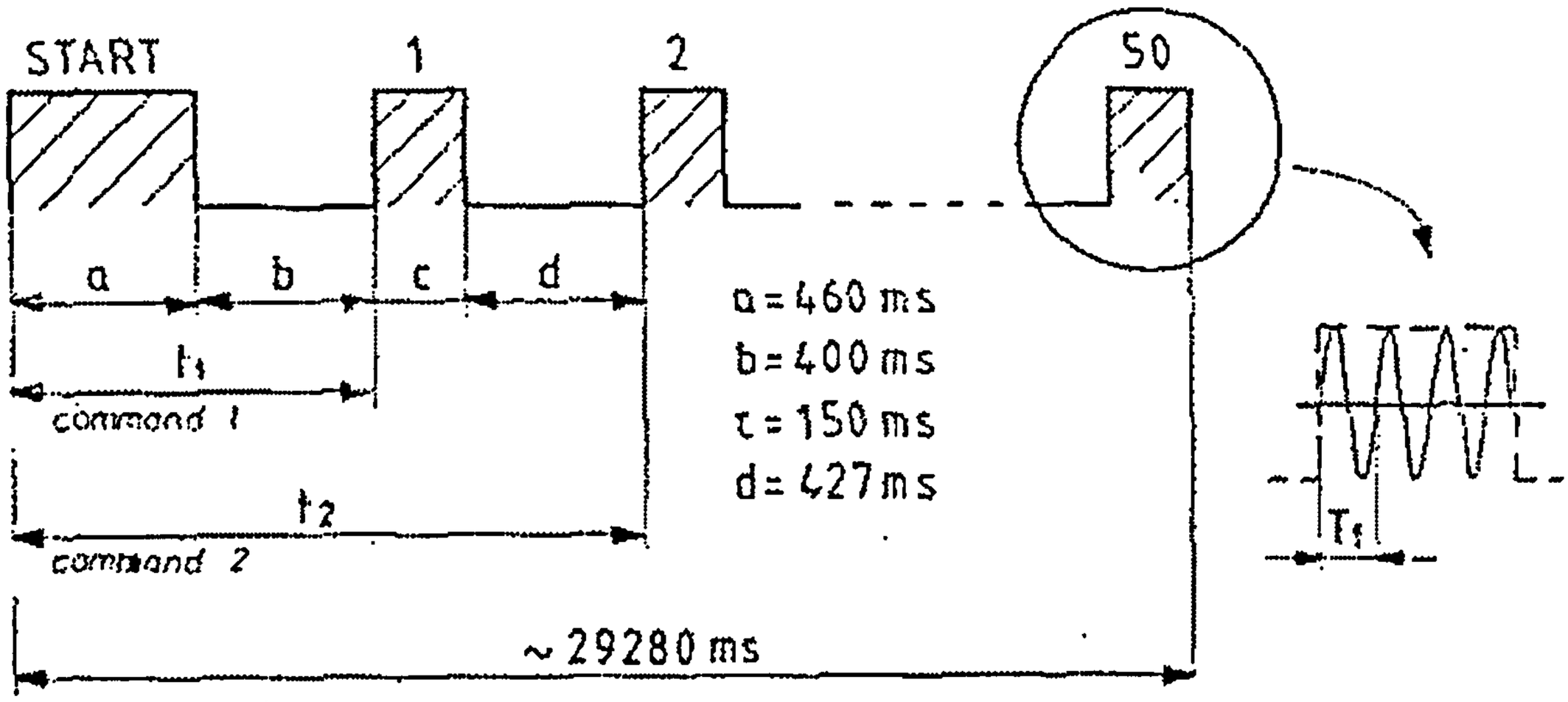


Figure 7: Example of a Ripple Control Transmission

The above diagram shows an example of a ripple control transmission pulse train, with each pulse consisting of several cycles of the carrier frequency. It can be seen that, like Cyclocontrol, this technique also suffers from a low data rate, since the entire transmission takes almost 30 seconds. It is again only a one way technique, as the ripple carrier signals must be generated at relatively high power levels.

Lastly in this section, we will look at one more example of PLC techniques used over the power distribution network - TWACS.

1.4.4 TWACS

A more modern example of a PLC system used by electricity suppliers is TWACS, standing for 'Two Way Automatic Communication System' [5]. TWACS is similar in some respects to Cyclocontrol, insofar as it utilises the injection of a signal at the mains voltage zero crossing point. Unlike Cyclocontrol, however, TWACs has the capability of passing data in both directions.

The outbound signalling technology is very similar to Cyclocontrol, based upon the modulation of the mains voltage waveform, at a precisely controlled region near the zero voltage crossings. The modulation is obtained by drawing a short, pulsed, single-phase load at the bus of a distribution substation transformer. This signal can propagate down through the distribution network to receivers located at remote sites, at the consumer voltage level of 240 / 415V.

The remote receivers are able to generate a return signal by drawing an impedance limited load current starting at a phase angle of 25° before the voltage zero crossing. This imposes a single current pulse on the overall load current, which can be detected at the distribution substation.

TWACS signals may be injected into the distribution network at the 33 kV voltage levels, or lower, and propagation distances of up to 90 km can be achieved with this technique.

Finally, in considering the applications of PLC over the power distribution network, we must look at one last major driving force in its introduction – automatic meter reading. In the next section, we will introduce the subject by considering the history of utility meter reading.

1.5 The Origin and Need for Utility Meter Reading

Ever since public utility providers (gas, water and electricity) came into existence during the mid-to-late 19th century, there has been a need for them to record the usage, by their customers, of the commodities that they provide. This implies the use of metering technology. Suitable devices were designed at an early stage in the development of the utilities, and indeed, the basic designs of electricity, gas, and water meters remain virtually unchanged to this day. To be useful to the utility company, of course, it is necessary for these figures to be gathered, hence the need for meter reading.

This task has traditionally been a labour intensive one, requiring operatives to attend the customers' premises, gain access, and to read and manually record the meter readings. In recent years, there have been steps taken to automate the process to a greater or lesser extent and we will describe these in the next section.

1.6 Modern Meter Reading Techniques

Modern meter reading techniques can be broadly split into the following categories, in order of their level of automation:

1.6.1 Manual Meter Reading:

This is the oldest method of meter reading. An operative follows a route around various customers and records their meter readings manually on paper. At the utility company, a clerk manually calculates consumption and prepares a bill. In recent times, computers have been introduced at the utility companies to accelerate the billing process and reduce clerical errors, but the basic process has not changed in over a hundred years.

1.6.2 Manual Reading with Handheld Devices:

This is an enhancement of the manual technique described above. Rather than recording readings on paper, meter readers enter the reading directly into a handheld electronic device, usually computer-based. Although the handheld device does not obtain the reading automatically, this technique dramatically improves clerical accuracy, since at all subsequent stages in the billing process, the data may be transferred electronically. Some handheld devices are smart enough to display the meter reading route and other special meter information (e.g. location of meter etc.) and also notify the meter reader if the new reading is out of range, indicating a possible reading error.

1.6.3 Remote Meter Reading:

A major disadvantage in the techniques described above is the need to gain access to the interior of the customer premises, since this is traditionally where the meters are located. One way of alleviating this is by locating the meter outside, although this poses additional criteria with regard to safety and security.

Alternatively, if a remote indication of the meter reading can be provided, usually by electronic means, then this indicator may be located in a readily accessible position, perhaps some distance from the meter itself. This technique is referred to as Remote Meter Reading (RMR).

1.6.4 The M-Bus

A practical realisation of RMR is the M-Bus [6], which was originally proposed in 1993 as a means of networking utility meters. M-bus relies on a twisted pair physical medium and is a master-slave type of network. The M-bus itself is permanently energised with a DC voltage (which itself offers the potential to power the electronics in each meter on the bus). Signalling from the M-Bus master to the slave is accomplished by the master altering this DC voltage between 36 V (representing a logic '1') and 24 V (representing a logic '0'). Signalling back from a slave to the master is accomplished by the slave modulating its own supply current by 20 mA.

M-Bus offers a notable refinement to simple RMR - because it is a network, data from a number of meters (up to 255 on any one segment of cabling) can be gathered to one point for centralised reading (useful in locations such as blocks of flats). The fact that the meter reading is in an electronic form also paves the way for the next level of automation in meter reading, described below.

1.6.5 Remote Electronic Meter Reading:

When RMR is combined with electronic data transfer (EDT) technology, the meter reading can be automatically read by the handheld device. Remote electronic meter reading still requires close physical contact between the handheld device and the meter or remote indicator, but it completely eliminates the errors associated with visual reading and manual data entry.

1.6.6 Mobile Radio Meter Reading:

With this technique, the meter reader need only come within close proximity of the customer premises. Radio frequency communication is used to send a signal to wake-up a radio transmitter located at the meter, which will then send its reading to the receiver. The receiver can be either vehicle based ('drive-by') or within a handheld device carried by the meter reader ('walk-by'). Combined with RMR techniques such as M-Bus, the readings from many meters may be acquired at one time.

1.6.7 Automatic Meter Reading (AMR):

This is the highest level of meter reading automation. With AMR the readings pass from the customer premises to the utility company over a communications network, with no human intervention required. The initial 'local' stages of the network (from the consumer to a nearby data gathering point) might utilise telephone lines, radio frequencies, power line carrier, or cable TV systems. From the local gathering point onwards, other wide-area networking techniques would probably be employed.

We will discuss the technologies used over the 'local' stage in greater detail later section, but next we will discuss the emerging factors in the utility industries that make the adoption of full AMR techniques highly desirable.

1.7 De-Regulation In the Utility Industries

In recent years, the various utility companies (gas, water, and electricity) have been de-regulated, with a view to increasing competitiveness and consumer choice. In other words, their markets have been opened up to outside competition. As a result, there are now a number of competing suppliers each of which have their own customer bases.

Such an arrangement would be impractical at a national level unless there were a shared distribution network. We have already discussed the National Grid in an electricity context, but similar systems also exist for the distribution of both gas and water. In other words, the customers of each utility company take their product off of the grid and the suppliers, wherever they are physically located, supply the appropriate amount into the grid to meet the needs of their customers.

In pre-deregulation days, it was sufficient to take meter readings from the consumer every three months or so. Such an arrangement could be used nowadays, but it would be very inefficient, since it would not be possible to accurately predict the contribution that each supplier would need to make at any moment, requiring adjustments at each billing period.

With a grid system, shared by many different suppliers, it is highly desirable that the exact share of the commodity that each supplier must satisfy should be monitored in (close to) real-time. In other words, much more frequent meter readings are required.

Electricity is perhaps the worst-case example, since, in order that the split of generating capacity between all of the individual electricity suppliers can be adjusted in (virtually) real-time, it will be necessary to monitor electricity consumption at, typically, 30 minute intervals. It is evident that automatic meter reading, as previously described, is the only realistic solution to achieve this.

1.8 Techniques for Automatic Meter Reading

It has already been noted that AMR systems are typically 'multi-level' - one communication technique may be used from the customer premises to a collection point, possibly the local sub-station, then one (or more) other techniques used to cover the longer distances to the utility company headquarters.

In our context of this thesis, it is this first stage of the route that interests us most and we will now discuss some techniques that may be employed.

1.8.1 The Public Switched Telephone Network

It is possible to employ an existing telephone line – sometimes called the 'Plain Old Telephone System' (POTS), for the purposes of AMR. This is attractive since a large proportion of the population has a telephone. Aside from the meter seizing the telephone line, in the usual fashion, in order to make an outward call, and so pass on the reading, it is also possible to send the data over the idle telephone line, at times when normal calls are not being made.

In future, techniques such as ADSL (Asymmetric Digital Subscriber Line), a broadband, permanently on, digital communications link over existing telephone lines, may prove to be another solution for telephone line based AMR.

1.8.2 The Cellular Telephone Network

Perhaps an even wider infrastructure is available with the radio-based cellular telephone network, since it does not rely on the physical telephone network connections into each property. It is possible to manufacture 'stand-alone' cellular transceiver which can be fitted into a utility meter and which can then be interrogated at will by the utility company via the cellular network.

1.8.3 Radio Networking

The cellular telephone solution already outlined is a special form of radio link, however the use of dedicated radio channels for AMR applications has been endorsed by the adoption of approved frequency bands for the purpose. In the UK, the frequency range of 183.5 MHz to 184.5 MHz has been allocated for this purpose. However, these are restricted to low-power transmissions and would realistically only be suited to short range REMR applications (walk-by or drive-by) as outlined in a previous section.

1.8.4 Power Line Communications

PLC is an obvious contender for AMR purposes, since the infrastructure (i.e. the power distribution network) will already be in place.

In a practical meter-reading scenario, it is likely that the PLC techniques will operate only over the 110/230/415V network - between the appropriate sub-stations and the consumers served by them. Beyond this, as has already been mentioned, some alternative form of wide-area network would be used. One PLC technique that has already been discussed and which can potentially be used for AMR is TWACS.

To conclude chapter one, we will summarise the background to the experimental effort in this research.

1.9 Background to the Research

In this first chapter we have introduced the broad subject area of Power Line Communications and its established application in the present day. As background, we began with a discussion of early discoveries regarding electricity, the development of the science of electrical engineering, and the practical application of these discoveries to the creation of the power generation industry. We then described the structure of the modern power distribution network.

We considered the PLC techniques that are used in the present day by electricity supply and distribution companies, namely Cyclocontrol, Ripple Control, and TWACS. We then moved on to the subject of meter reading, emphasising the developing use of automation in that area, and the driving forces behind the growing adoption of automatic meter reading, including power line communication techniques.

However, all of the power line communication techniques described so far are essentially 'wide-area', operating over the low, medium and high voltage distribution network, predominantly between consumers and electricity suppliers.

There also exists an entirely different arena of power line communication applications. In contrast, these can be described as 'local area', as they exist within single or small groups of buildings, homes, or within the extents of an industrial plant, and operate almost exclusively over the low voltage 230 / 415 V distribution network.

It is specifically the potential of power line communications in the industrial scenario that we will be considering in this Thesis, as the author works within the field of industrial control. In a previous paper, the author has described the concept of a 'Power Bus' - a localised power line based network for machine or plant monitoring and control [7].

In subsequent chapters, and before dealing with the experimental work proper, we will be discussing the relevant aspects of automation, control, and networking technology that have a bearing on the subject area of power line communications. These will include industrial and home automation, computer networking, and the growth of the industrial Fieldbus concept.

We will consider the power line as a communications medium, and discuss the various sources of signal degradation and noise that are prevalent on the power line. We will then go on to look at actual PLC techniques, modulation schemes, and the desirability for protocols and error detection/correction techniques. We also look at the international standards that are evolving to cover the subject of power line communications.

Moving onto the experimental side of the thesis, this will be concerned with the evaluation of actual PLC modem solutions in noisy electrical environments.

It is stated in the international standards for Electromagnetic Compatibility (EMC) that electronic equipment should not generate excessive electromagnetic interference, nor be excessively susceptible to such interference. Such interference might be emitted from, or accepted into, the equipment by various routes such as by RF radiation or via control or power ports i.e. power lines.

The power line communication scenario presents an interesting variation of this concept, since it will purposely generate conducted emissions on the power line as a part of its normal transmission operation, and will have to accept signals (and potentially noise) from the power line in order to receive data.

In the experiments, impulsive noise (at levels as specified in the EMC immunity standards, and generated by an actual item of EMC test equipment), and spot frequency noise at and around the PLC carrier frequencies, will be applied to a simulated power line communications link. Link and modem performance will be evaluated by recording the bit-error-rate of the link under the varying noise conditions.

To carry out these measurements, equipment to measure bit-error-rate is required. Suitable equipment was not available to the author, and so the initial part of the practical work covers the design and development of a purpose built item of equipment, which was subsequently called BERT for 'Bit Error Rate Tester'.

Once the BERT equipment was available, experimental tests were performed on two types of PL modem suitable for industrial control use in the CENELEC 'C' band.

Finally, some 'real world' tests were performed by setting up the PLC link within a small industrial company (where the author is employed), and monitoring the performance of the link under these conditions. The results are then presented and analysed, with appropriate conclusions being drawn.

To conclude the thesis, ongoing developments in PLC, especially HF techniques suitable for high-speed communications, are introduced and discussed.

Chapter 2 : The Development of Industrial & Home Automation

In this chapter we will look at the field of automation, as it is within this context that we will be investigating the application of PLC techniques. We will consider the history of automation, both industrial and in the home.

2.1 The History of Industrial Automation

Automation, within the industrial context, can be defined as the use of systems to control industrial plant or processes without the need for constant manual intervention.

Although fully automated industrial systems were not developed until the 20th Century, many simple, semi-automated devices had been in use for hundreds of years before. During the 1700s there appeared in England and Scotland a number of inventions that helped to bring about the first Industrial Revolution. These inventions included feedback systems for controlling the temperature of industrial furnaces and the action of water mills.

One of the most notable of the early feedback control mechanisms was the fly-ball governor, developed in 1788 by the Scottish inventor James Watt to regulate automatically the output of the steam engines he had invented. This used the principle of negative feedback - the mechanism senses the speed of rotation of the engine and as it rises above a certain set point, regulates the steam supply to maintain the desired speed, all by mechanical means.

As the Industrial Revolution progressed, other inventors applied the principle of negative feedback, designing equipment that could regulate the operation of machines or control the progress of an industrial process by adjusting the input parameters on the basis of measured outputs. As such feedback loops are still integral to many modern industrial processes, we will briefly describe the components that go to make one up.

2.1.1 Negative Feedback Control Loops in Industrial Automation

A negative feedback control loop consists of five basic components - an Action element, a Sensing mechanism, a Control element, a Decision element and a Program (or Algorithm).

The Action Element

- This is the prime energy source for the control loop. Examples may be electricity, steam, compressed air, or fluids (pneumatics and hydraulics).

The Sensing Mechanism

- This is the device that measures the particular parameter involved in the control loop. Examples might include pressure sensors, speed sensors or temperature sensors.

The Control Element

- This is the device that acts upon the parameter to modify it. Examples might include valves regulating fluid or air pressure, or electrical speed controllers.

The Decision Element

- This is the element which controls the overall loop and makes the decision as to what is required to bring the loop back under control.

It is this element that differentiates a manual control system from an automatic one. In a manual system, the decision element is a human being, acting on the data from the sensing mechanism(s), who then makes appropriate adjustments to the control elements. In an automatic system, this is an autonomous system, which might be mechanical or electrical/electronic in nature.

The Program (or Algorithm)

- This represents the formula required within the decision element to implement the control function required. This may be very simple - a thermostat for example may have a simple set point value and simply switch 'On' or 'Off' in response to the sensed temperature parameter. Alternatively, the algorithm may be a lot more complex. For example, a Proportional-Integral-Derivative (PID) loop applies complex mathematical functions to the input parameters, based on factors such as the rate of change of the sensed parameter, and the difference between the current value of the sensed parameter and the set point.

Such algorithms may be implemented by mechanical or analogue electronic means, but increasingly these days are implemented in the form of a stored program within a digital computer system, or a programmable logic controller. These devices will be introduced and described in greater detail in a later section.

2.1.2 Other Components in Industrial Automation

Of course, feedback loops do not represent the only elements to be found in a typical industrial automation scenario. There will also be requirements to provide sequencing, counting, and timing functions for controlling the progress of a process or action of a machine, as well as requirements for monitoring and displaying set points and alarms.

All of these functions lend themselves to automation, and in the next section we will be looking at how, over the years, differing technologies have been adopted for these uses.

2.1.3 Technology Trends in Industrial Automation

As we have already mentioned, the earliest industrial automation systems were purely mechanical in nature, in keeping with the technology available at the time. However, once electricity had become readily available, in the late 19th Century, it soon became the preferred choice as the driving force (the action element) for industrial automation.

As an aside, though, it should be noted that during the 1930s pneumatic and hydraulic systems were developed [8] where air or fluid under pressure is employed as the action element. Despite the inherently mechanical nature of these systems, quite sophisticated control functions can be attained, with the added advantage of reduced explosion risk in flammable atmospheres such as refineries, since there is no risk of electrical sparking. Indeed, such control systems can still be found in use today.

Negative feedback control loops may be realised using electrical sensing elements i.e. sensors which output an electrical signal representing the parameter being measured, feeding decision elements consisting analogue electronic amplifiers, processing the signal in a defined manner, which in turn drive electrically operated control elements.

Such equipment became feasible by around the 1920s, once the science of electronics had reached an appropriate level of sophistication, and even before this time, sequencing and timing operations were possible by making use of electrical timers and relays.

Indeed, relays have an important place in automation systems, and we will discuss them in the next section.

2.1.4 Relays in Industrial Automation.

Relays are electromechanical switches. In their simplest form, they consist of an electromagnet which, when energised with an electrical supply, moves an armature and causes a switch contact to operate. This may simply serve to permit a low level control voltage to switch a much higher voltage or current, a useful form of 'amplification' or power switching. However, considerably more sophistication is possible with relays. Consider the following:

Relays may be fitted with several contacts, all operating simultaneously from the single input to the coil. These contacts may be normally open (closing when power is applied to the coil), normally closed (opening when power is applied to the coil), changeover (a combination of both previous types, with a common connection), or indeed any combination of these types. By appropriate mechanical design, certain contacts may be forced to close before others, or in a set sequence. Longer or more complex sequencing functions may be provided by the use of motor driven cams operating banks of switches.

By interconnecting the relay contacts in an appropriate manner, it permits the creation of logic functions. For example, if three relays are taken and a single normally open contact from each is wired in series then, if we treat the relay coils as inputs and the circuit formed by the combined contacts as the output, we have a logical 'AND' gate, since ALL of the inputs have to be energised before the output circuit is made. Conversely, if the contacts are wired in parallel, we have an 'OR' gate, since energising ANY of the inputs will make the output circuit.

The above are simple examples, but in practice extremely complex combinational or sequential logic schemes can be realised using relays and associated components such as cam timers. With combinational logic, the state of the outputs depends purely on the current state of the inputs. With sequential logic, the state of the outputs depends both on the current state of the inputs, and on the previous input states. To achieve this, some form of memory element is involved, and in fact relays may easily be configured to provide such a feature. Overall, these techniques are referred to as 'Relay Logic'.

To emphasise the sophistication that may be achieved with relay logic, consider the fact that a lot of early work in the computing field [9] relied on relays to create the computing elements.

'Relay Logic' was the mainstay of industrial control until at least the 1960s. Indeed, in some smaller applications, relay logic is still used today, for its simplicity, ruggedness, relative reliability, at least with simpler logic schemes, and its ability to switch high power loads directly.

The main disadvantages of relay logic, especially in very complex schemes, are the size and complexity of the control equipment, the relatively high power consumption, and the corresponding low reliability due to the sheer number of mechanical elements involved.

The scene was therefore set for a more efficient solution. Since relays are essentially digital devices, the rise of digital electronics and computing in the 1950s and onwards would provide the necessary technology.

2.1.5 The Move towards Digital Electronics in Industrial Control

With the rise of computer technology in the 1950s there would seem to be a good incentive for this technology to be used in industrial control. However, the very high cost and relatively poor reliability of early computers made this initially impractical.

By the 1960s, smaller, more reliable, 'mini-computers' had come onto the scene, but these were still relatively high cost, although they did start to be utilised in some large-scale 'plant control' scenarios.

What was required was a small, relatively inexpensive, programmable device that could replace the bulky and complex relay logic systems. In 1968 [10] this was realised with the development of the Programmable Logic Controller (PLC).

NB. This abbreviation might be confused with the other definition of PLC within the context of this thesis – power line communications – however the correct usage should be obvious from the context in which the term is used.

We will next look at what makes up a PLC.

2.1.6 Programmable Logic Controllers

We have already mentioned that a relay logic system can be considered as having distinct 'inputs' and 'outputs'. According to the manner in which the relay elements are hard-wired (interconnected), the relay logic system 'processes' the inputs and then operates the 'outputs' according to their current (and, possibly, also previous) states.

A PLC is a solid-state device with digital processing capabilities designed, initially at least, to replace relay logic designs. The most striking feature of a PLC, as opposed to a hard-wired relay logic solution, is the fact that it can be *programmed* to perform a specific logical function. To perform an alternative function, all that is required is to reprogram the device. We will next look at the structure of a 'typical' PLC.

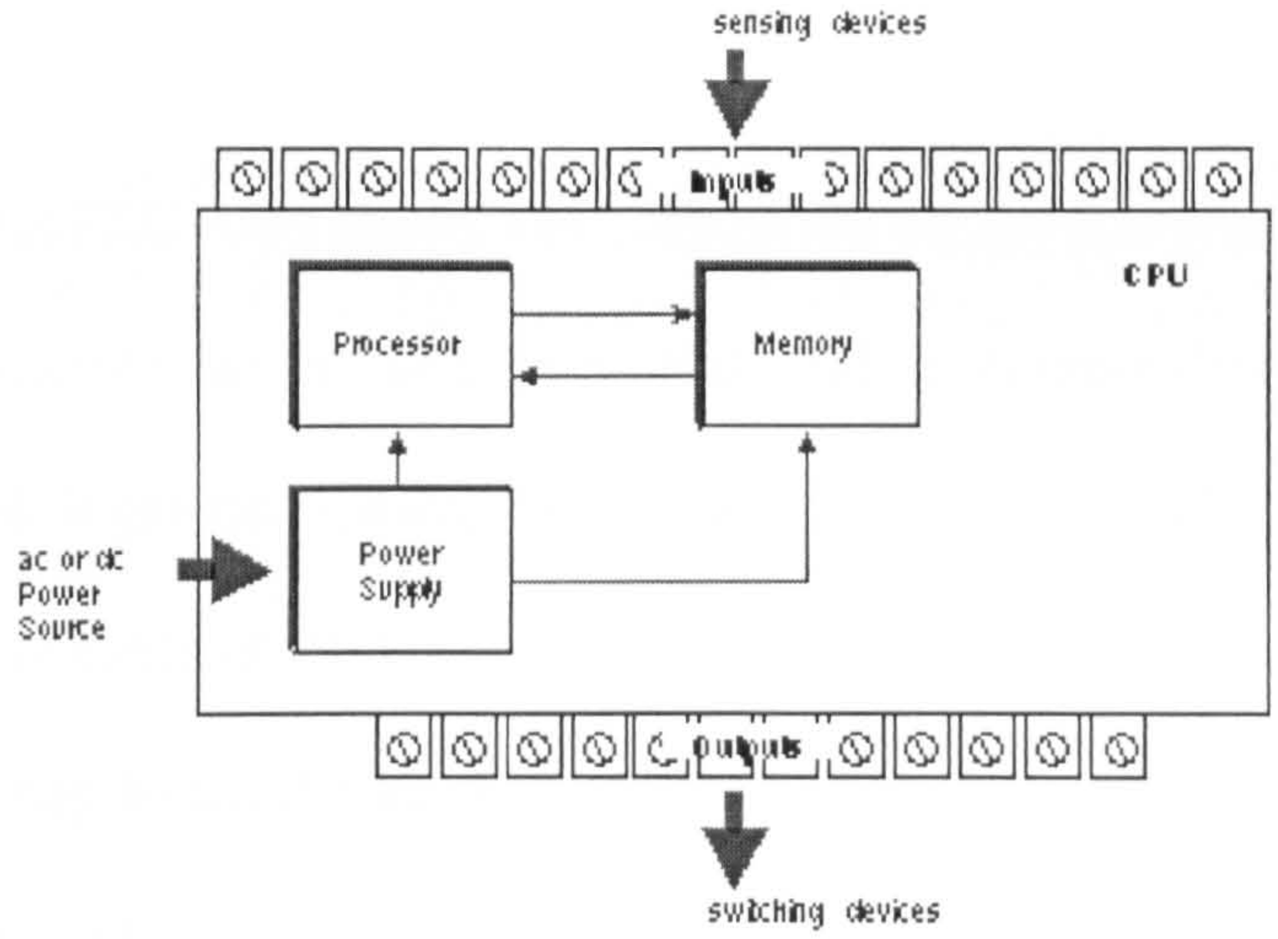


Figure 8: Programmable Logic Controller Block Diagram

A typical PLC comprises inputs and outputs (I/O), and a central processing unit (CPU). The input and output components are often built into the same physical box with the CPU, but may be modular in nature to facilitate expansion to provide a greater number of I/O points as required. Such a package provides a small, lightweight, low-cost, and self-contained solution for a wide range of control applications.

The figure below shows a typical small PLC. The physical input and output connections can be seen at the top and bottom of the housing.

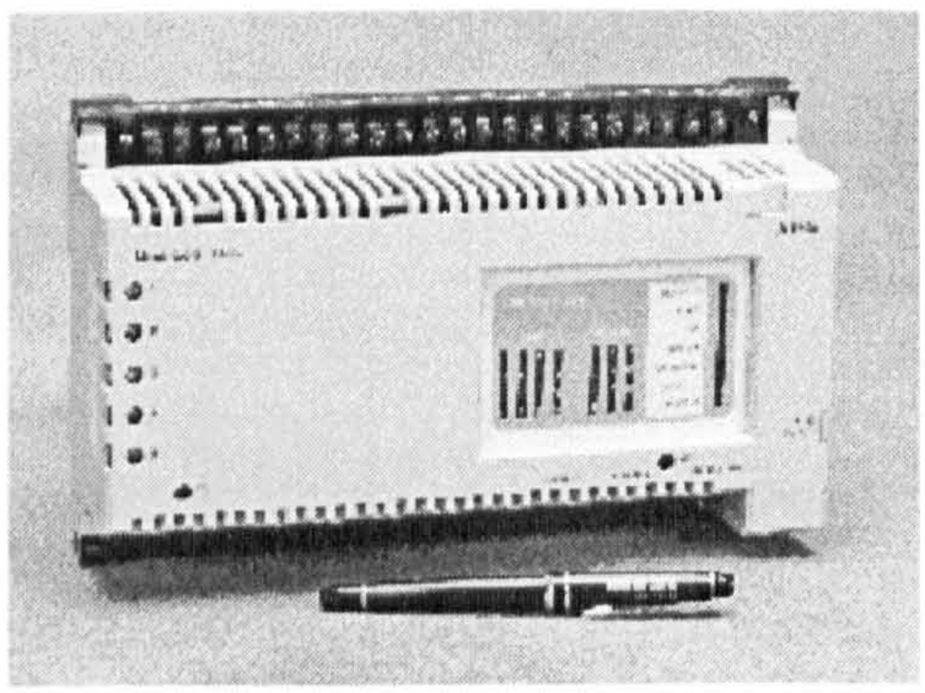


Figure 9: An Example of a Programmable Logic Controller

We will next consider the function of the different component blocks.

- **Input and Output Units (I/O)**

In the simplest PLC's, all inputs and outputs are digital (i.e. simply 'on' or 'off'). Inputs are wired to sensing devices or user controls. When an input detects that a sensor or user control is closed, it generates a logic signal understood by the CPU. The PLC outputs are wired to switching elements that operate output devices or user indicators. These switching elements may be solid-state devices, such as transistors, but are frequently simple, single contact, relays.

- **Central Processing Unit (CPU)**

Within the CPU lie the digital processor, memory, and power supply. These components interact to solve the application logic. The CPU reads the converted input signals, executes the user logic program stored in its memory, then writes the appropriate output signals to the output switching devices.

2.1.7 Programming the Programmable Logic Controller

By very definition, a PLC is programmable. The user must store a representation of the logic scheme required for the particular application within the controller. Because they were originally designed to replace discrete relay logic, and the control engineers were familiar with relay logic circuit diagrams, it was convenient to use a means of programming that mimicked the physical relay arrangement.

This resulted in a 'language' called ladder logic, a simple example of which is shown in the next figure.

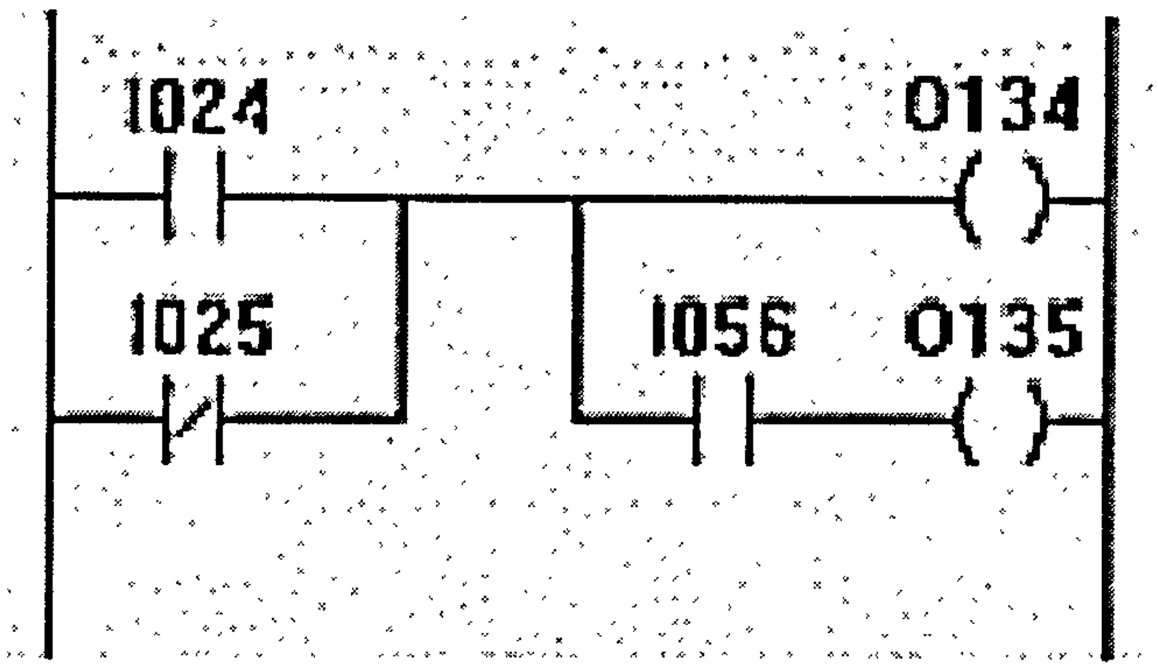


Figure 10: Example of Ladder Logic Programming

It can be seen that the above diagram looks very similar to an electrical circuit diagram, and as such would be familiar to a process engineer. The elements designated Ixxx are inputs, analogous to relay contacts, and those designated Oxxx are outputs, analogous to relay coils. Not all inputs and outputs map to actual physical I/O ports on the PLC, some may be purely internal, and used to facilitate the building of complex logic schemes.

Entry of the ladder logic program into the PLC is achieved using a programming interface. This may be a simple keypad and display, allowing each I/O device in the logic scheme to be entered in sequence for each 'rung' of the ladder, or may be a more sophisticated graphical interface, displaying the actual logic scheme, as it is created. The programming interface may be built into the PLC itself, or more commonly be a separate, hand-held item, removable after programming and debugging is complete. Increasingly, these days, PCs are used to provide a convenient programming interface for PLCs.

As well as simulating the action of simple relays and contacts, the PLC can also provide other necessary functions encountered in relay logic systems, such as timers, counters, or sequencers.

From these relatively simple beginnings, as 'relay substitutes', the technology soon advanced and PLC's increased in sophistication. We will look at this evolution in the next section.

2.1.8 The Further Evolution of Programmable Logic Controllers

Whilst the earliest PLC's were based on discrete electronic logic circuits, within a few years another evolving technology permitted much greater sophistication – this technology was the microprocessor. Indeed as computing power has decreased in cost, the stage has been reached when PLC's can often be considered as powerful microcomputers in their own right.

As already discussed, early controllers used digital inputs and outputs only. A natural progression was to provide the facility for analogue I/O. This offers the facility for the PLC to provide sophisticated feedback control functions.

Such additional facilities imply the need for a more sophisticated programming language than simple ladder logic. High level languages (HLLs) may be used in PLC's to implement these sophisticated control programs, often with ladder logic still available for those aspects of the application to which it is best suited.

As plant control schemes become more complex and sophisticated, there is a point at which individual PLC's cannot realistically accommodate the number of I/O points required. Using multiple PLC's implies that communication between them is necessary. This represents the final stage in the evolution of programmable controllers that we will discuss at this stage. In the next chapter, we will introduce computer networking, the evolution of industrial networking, and the rise of the Industrial Fieldbus concept.

Before finishing this discussion of PLC's, however, we will mention the associated technology of industrial computers.

2.1.9 Industrial Computers

For tasks requiring greater sophistication or a more elaborate user interface, and with the ever-decreasing cost of powerful microcomputer computer hardware, there are instances where it might be preferable to employ a general-purpose computer for industrial control. This may be a desktop PC, so long as it is used in an appropriate environment, or a more ruggedised device capable of operating in a harsh industrial environment. Such PCs may be equipped with appropriate digital or analogue Input / Output cards in order to interact with the process or plant being controlled, in much the same manner as a PLC.

In fact, there may be little to choose between Industrial PCs and Programmable Logic Controllers, as regards processing power and input/output capabilities, although industrial computers generally offer more sophisticated user interfaces such as visual display units and conventional keyboards.

We have already mentioned that PLC's have evolved towards a networking capability, similar to that of computers proper. In many modern applications, industrial PCs may be networked with PLC's to provide both a means of programming the PLC function or a versatile user interface overseeing the process being controlled by the PLC.

As already stated, we will be discussing such networking in greater detail in a later chapter. Next, though, we will move on to the subject of home automation.

2.2 The Rise of Home & Building Automation

The term home or building automation can be applied to *any* use of autonomous systems in the home or working environment. Indeed, on the basis of the above definition, automation can be said to have entered homes and buildings when such facilities as thermostatic control of heating and the use of time-switches to operate appliances such as heating or lighting was first developed, essentially during the early 20th Century.

In recent years, though, the term home automation has specifically come to mean the *systematic* use of automation, and furthermore, the trend towards the *integration* of all automated systems within the home together, i.e. in the form of a home automation network. Needless to say, the electronics and computing revolution of recent years has played a major role in this development.

The subject of power line communications is closely linked to the concept of Home Automation, not unreasonably, since the electricity main within a dwelling offers a ready-made network, interconnecting the majority of the devices which would need to be controlled or monitored in a HA scenario.

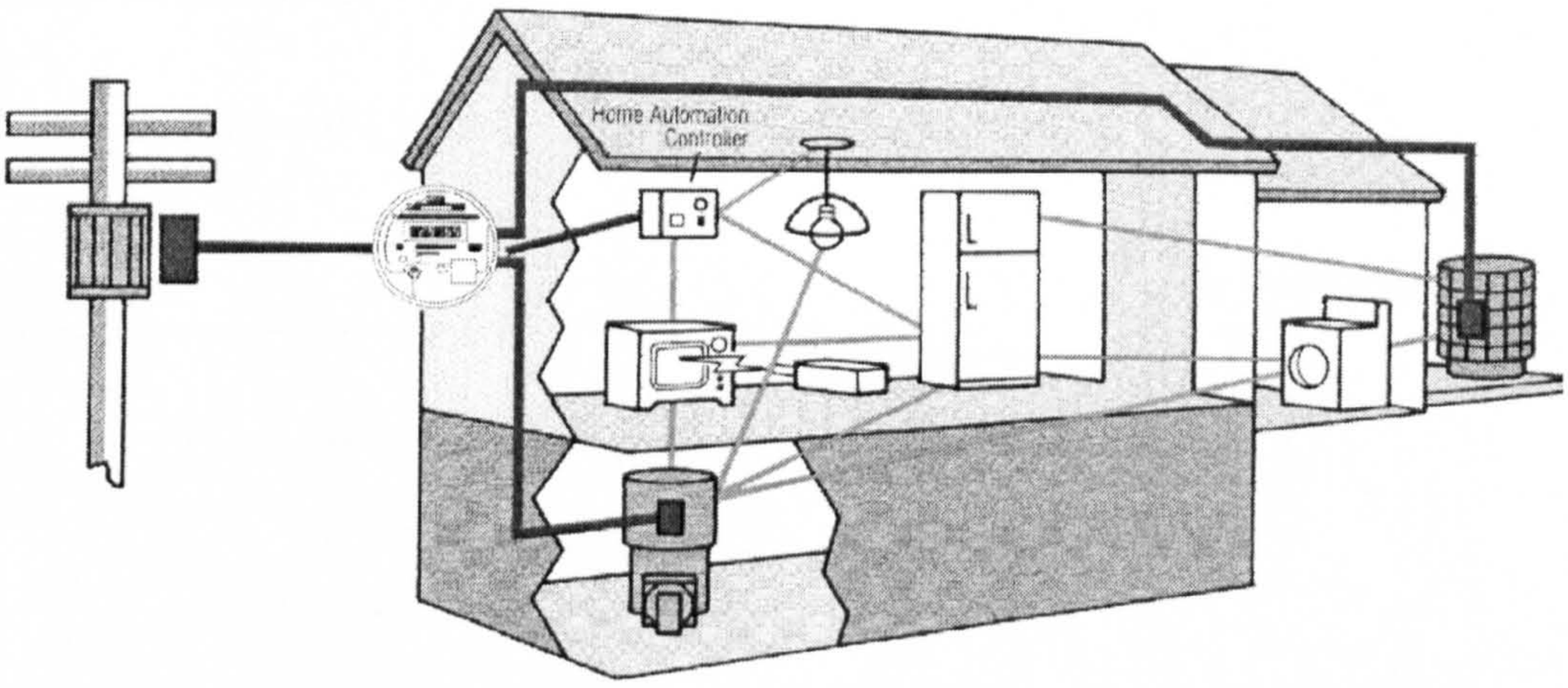


Figure 11: Typical Home Automation Scenario

The above figure shows a typical HA scenario. Appliances within the building are linked by a network to a central home automation controller. The figure also shows a utility remote meter reading network.

Unfortunately, the convenience offered by using the power line in a HA application comes with several disadvantages, since it represents a far from perfect transmission medium.

These characteristics will be described in a later chapter. Meanwhile, it should be noted that there are other potential communications media suitable for use in home or building (or indeed industrial) automation, and it we will discuss these in the next section.

2.3 Transmission Media for Industrial and Home Automation

Whilst PLC is the primary concern of this research thesis it is, of course, not the only medium suitable for home, building or industrial automation applications. We will therefore take the opportunity now to describe some of these other media.

2.3.1 Co-Axial Cable

The structure of a typical co-axial cable is shown below.

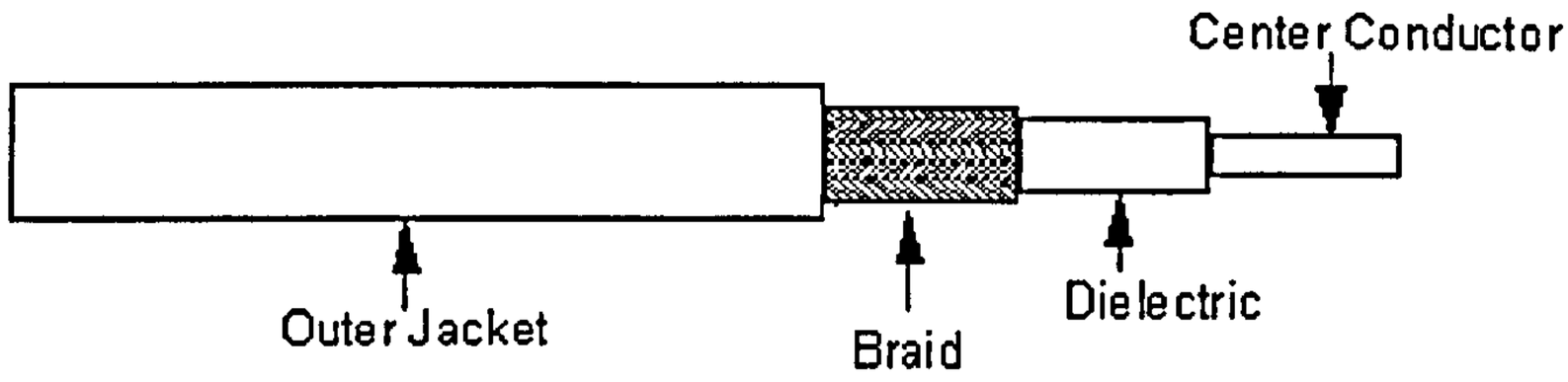


Figure 12: Co-Axial Cable Structure

Co-axial cable, so called because each of the layers (centre conductor, dielectric, braid, and outer jacket) lie on a common axis, is commonly encountered in radio frequency (RF) applications such as television down-leads, or for carrying digital signals over a base-band computer communications network, such as Ethernet.

Because of its construction, co-axial cable offers a consistent characteristic impedance, an important factor when high frequency signals are being carried.

From a practical point of view, due to its physical construction, it is perhaps not as convenient to terminate as other solutions.

2.3.2 Twisted Pair

The structure of Twisted Pair (TP) cable is typically as shown below. Like co-axial cable, it is also commonly found in computer networking and telecommunications systems.

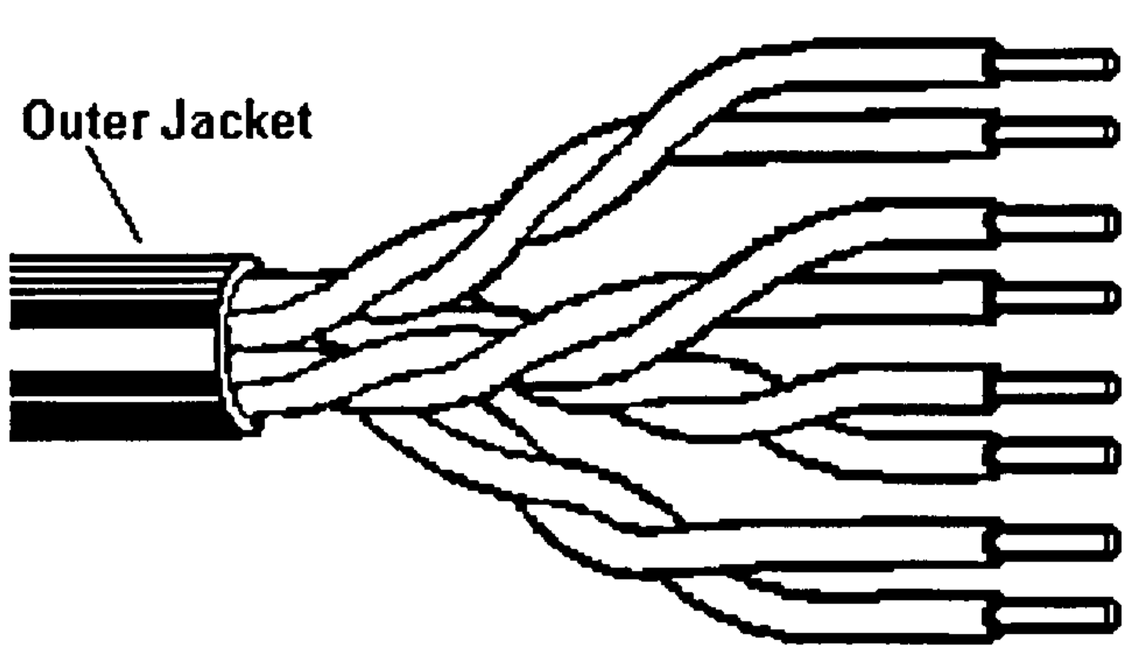


Figure 13: Twisted Pair Cable Structure

The primary reason for using twisted pair is that the arrangement offers good immunity to external electromagnetic interference. The twisting of the signal conductors means that any such interference will be induced equally in each core ('common-mode') and with the use of appropriate circuitry can be easily suppressed. Shielding can provide additional immunity, although it should be noted that the not all twisted pair cable is shielded (shielded twisted pair cable is often abbreviated as 'STP', and unshielded twisted pair as 'UTP').

Often, several twisted pair cables may be contained within a common outer covering (as shown in the above diagram), with each pair offering good immunity from both outside and mutual interference. This offers the potential for a multi-pair cable to be run around a property and used for diverse purposes such as telephony, home computer networking, and as a home automation network. Indeed, an organisation called the 'Phoneline Networking Alliance' (PNA), has proposed just such a system.

Like co-axial, twisted pair cable also offers a consistent characteristic impedance, but unlike it, is considerably easier to terminate.

2.3.3 Radio Frequency

The use of Radio Frequency (RF) as a communications media offers the convenience of requiring no physical connection between the nodes in the network (i.e. it is 'wireless').

On the minus side, to achieve good RF performance involves more costly electronics. The system must cater for interference, much as PLC techniques have to, and there is a very real risk of mutual interference between nearby systems operating on similar frequencies. Nevertheless, RF systems have a place in home and industrial automation.

In recent years efforts have been made to develop high performance RF networks, working in those microwave parts of the RF spectrum designated for Industrial Scientific and Medical (ISM) use.

There are several such systems in use, but a good example is the system known as 'Bluetooth' [11]. Bluetooth was developed by a consortium of international companies and is intended to eliminate the need for connecting wires between consumer and computer equipment, and to allow easy connectivity. Some typical characteristics of Bluetooth are as follows:

- Uses a Frequency Hopping Spread Spectrum (FH-SS) modulation scheme (this technique is explained in a later chapter).
- Operates in the 2.4 GHz ISM band.
- Operates at low RF power levels.
- Short range (Up to 10 metres typically).
- Supports voice and data communications.

Bluetooth is still at an early stage in its development, but may turn out to be useful in industrial automation applications.

2.3.4 Infra-Red

Another 'wireless' technology, Infra Red (IR) relies on a modulated beam of invisible light to send commands and data. Unlike RF, it is essentially 'line of sight', as transmitter and receiver must be visible to each other. Commonly encountered in a home automation context, for such uses as 'same room' appliance control (e.g. Television remote controls), it is likely to have few applications in an industrial environment. However, we will include it here as some home and building automation systems offer it as a media option.

2.3.5 Fibre-Optic

The functioning of an optical fibre relies on the principle of total internal reflection. When a ray of light passing through a material meets an interface with a material of a different refractive index, the ray may be refracted, i.e. bent at a certain angle as it passes from one material to the other. However, if the incident angle of the ray is below a certain value, called the critical angle, the ray will be reflected back into the first material.

This effect is termed total internal reflection. In a practical fibre optic, a narrow strand of glass or polymer is used. This ensures that incident light will easily exceed the critical angle and will pass along the fibre, even if it is bent, so long as the bend radius maintains the critical angle at all points. The inner core of the fibre will be coated with a layer of different refractive index. This may create a distinct interface, as shown in the diagram (referred to as a 'step index' fibre) or may be diffused to give a gradual change in refractive index (referred to as 'graduated index'). This has the effect of bending the beam back into the body of the fibre, rather than causing a sudden reflection, and can tend to reduce 'multi-path' effects, where a ray of light follows several routes through the fibre. This can be a benefit at high data rates, since multi-path beams can tend to mutually attenuate by interference effects.

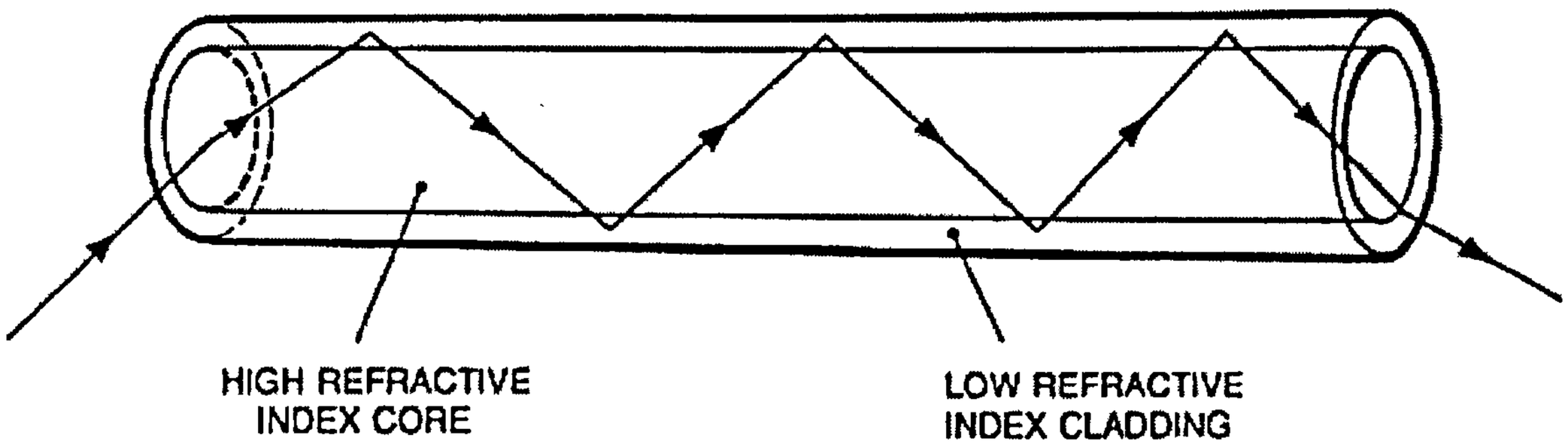


Figure 14: Total Internal Reflection in a Fibre-Optic Cable

In a communications scenario, fibre optic cable offers the benefits of absolute electrical isolation and very high immunity from external electromagnetic noise. On the minus side, it is relatively expensive, difficult to terminate, and is essentially a 'point-to-point' system. It is technically difficult (but not impossible) to tap into a fibre optic cable, or to send data bi-directionally. Consequently, sending a signal to multiple nodes would involve either a complex star arrangement, with hubs, or a chain of nodes in a ring arrangement (these networking topology terms will be explained in a later chapter).

To conclude this chapter, we will briefly look at some actual home and building automation solutions and the different communications techniques that they employ.

2.4 An Overview of some Commercial Home and Building Automation Systems

In this section we will introduce and briefly discuss some of the more common commercial home and building automation solutions.

2.4.1 The X-10 System

X-10 is perhaps one of the most widespread and popular home automation technologies at present in use. The origins of the X-10 system lie more than 20 years ago with a company called Pico Electronics of Glenrothes, Scotland. This was founded in the early 1970's and undertook diversified projects in the advanced electronics field.

One of these was for a 'wire-less' (but not necessarily radio based!) remote control system. This was based around power line communication and in keeping with their naming convention, this was referred to as 'Experiment no. 10', shortened to 'X-10'!

The system first became available in 1978 and its uses soon extended beyond the home audio applications envisaged by the original customer. Modules became available capable of controlling appliances or lighting. Many manufacturers now produce equipment compatible with the X-10 protocol. Originally just a power-line based system, X-10 now has the option of radio and infra-red based equipment for greater versatility.

The X-10 Physical Layer

X-10 is an OOK (on-off keying) system, utilising a carrier frequency of 120 kHz superimposed on the 50 Hz or 60 Hz mains frequency [12]. This carrier is transmitted in short (<1 ms) bursts starting just after the zero crossing point of the mains waveform. This point is chosen under the premise that there is likely to be less noise at this point. It also makes synchronisation simple, since a receiver can also detect this transition and need only 'listen' for a fixed periods at this point. Three-phase distribution systems are accommodated by repeating each burst of carrier at 120° intervals into the waveform after the initial zero crossing, since these represent the zero-crossing of subsequent phases. In a practical situation, X-10 signals on different phases are coupled together at the distribution panel using a simple capacitor across the phases.

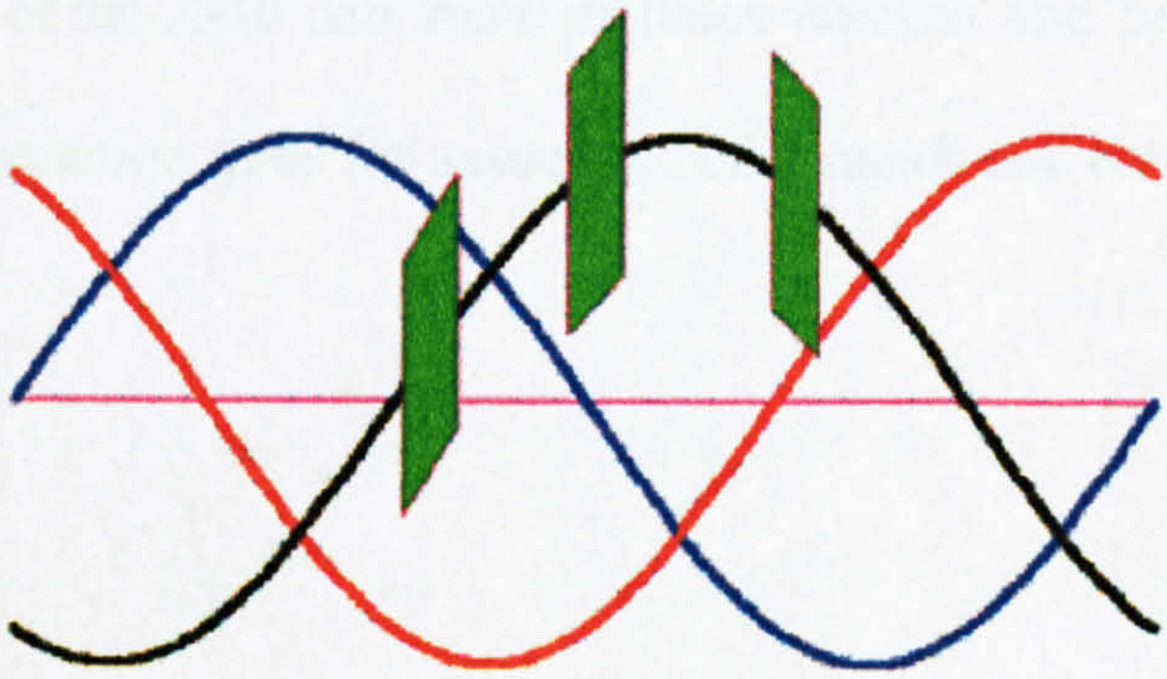


Figure 15: X-10 Signalling in a 3-Phase System

Since there are two zero-crossings for each mains cycle, this means that in a 50 Hz mains frequency situation there are 100 possible pulse windows per second, and in a 60 Hz situation, 120.

A logic '1' in X-10 is indicated by pulse, followed on the next zero-crossing, by no pulse, and logic '0' by no pulse, followed by a pulse.

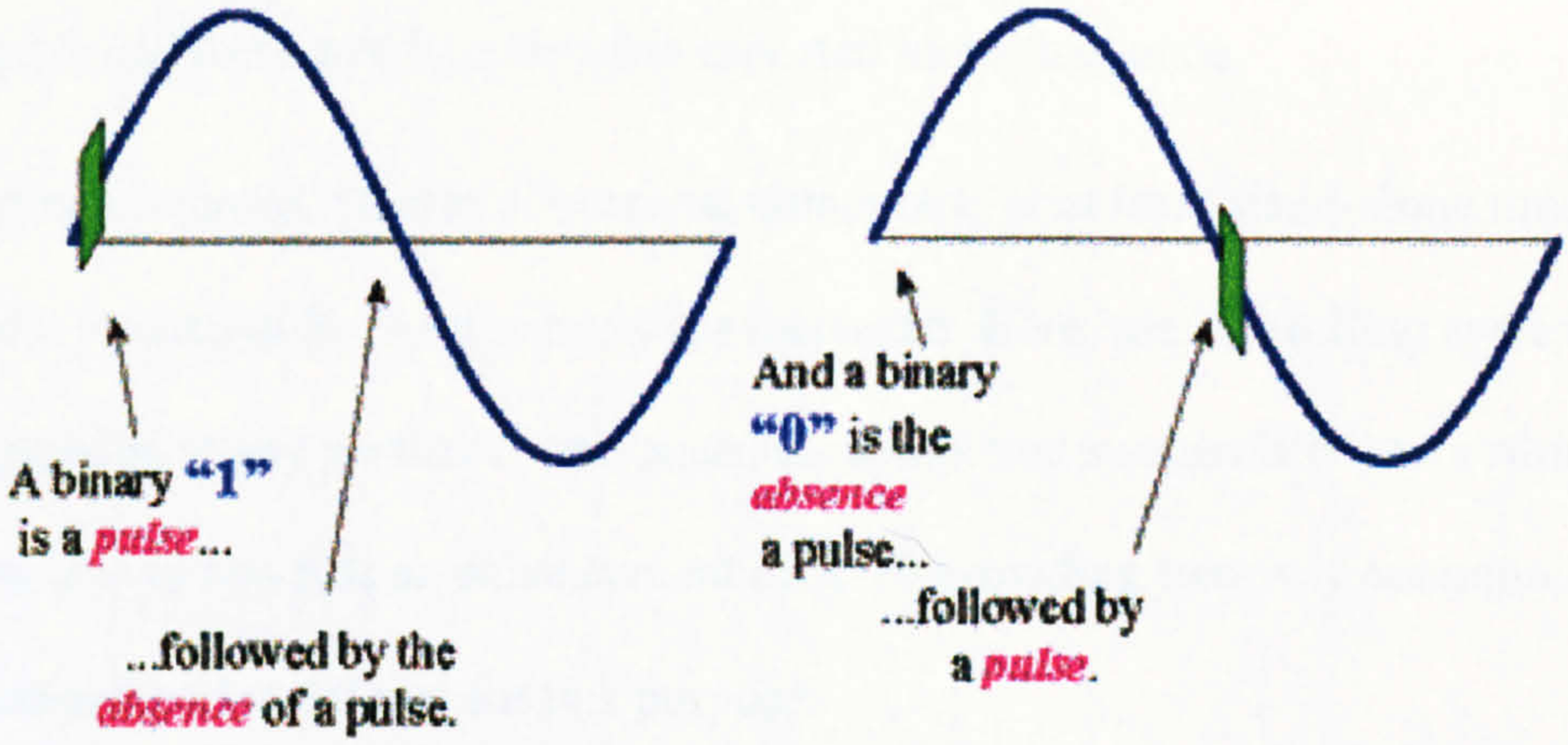


Figure 16: X-10 Logic '1' and Logic '0' Signals

It is evident that some means of synchronisation is necessary to determine the start of an X-10 transmission. This is because, for example, a string of logic '0's might be interpreted as a string of '1's, since the initial 'no pulse' would not be obvious. The start of a transmission is therefore indicated by a string of three pulses followed by a no pulse, since such a combination will not occur in normal data.

The remainder of the X-10 command includes 'address' and 'house code' (a form of extended address) information, plus the associated commands and data to be executed.

It was originally intended for X-10 to perform functions such as the turning on, and off, of lighting, appliances, etc. under the control of a human operator using, for example, a hand-held switching box. In such a simple arrangement, feedback is provided by the operator observing that the operation has completed successfully. Consequently, the basic X-10 system does not need to incorporate any integrity checking or message acknowledgement. It is purely a one-way system. The only concession to the possibility of a message being corrupted is in that it is repeated more than once.

In recent times, the use of personal computers, or at least stand-alone timer-controllers, to control X-10 operations has increased. Here, the controlling system has no way of knowing if any particular operation has completed successfully. As a result, there have been moves towards an enhancement of X-10 providing two-way communications, with command codes defined for this purpose.

2.4.2 Echelon (LonWorks)

The Echelon Corporation of Palo Alto, California was formed in 1988 specifically to develop communications technology and a protocol for interconnecting sensors, actuators, and controllers.

Echelon calls its technology LON, for Local Operating Network, to distinguish the network from a LAN, or Local Area Network, developed for computer networks and office automation. Their protocol is called LonTalk, and a complete Echelon network with supporting hardware and software is collectively called LonWorks.

Central to LON is a common interface for all devices attached to the network. This interface is called the 'Neuron Chip', an integrated circuit manufactured to Echelon specifications and sold by Motorola and Toshiba. In 1996 Echelon introduced licensing arrangements for companies to design and manufacturer interface devices that substitute for the Neuron Chip.

LonWorks networks are intended for applications spanning home and building automation, plus factory automation and aircraft. Originally a proprietary system, details of the protocol have been released and the EIA (Electronic Industries Association) HCS-1 Committee is writing a three-part standard based on LonTalk and designated EIA-709.

2.4.3 CE-Bus and Intellon

The CE-Bus 'Consumer Electronic Bus' standard was originally designed to perform Home Automation functions, but is also increasingly being used in the commercial and industrial sectors.

Development of the CE-Bus began in 1984 under the direction of the Electronic Industry Alliance (EIA), CE-Bus Technical Steering Committee (TSC).

Their goal was to develop an open protocol that would suit most consumer electronic manufacturers' requirements, and it was eventually ratified as standard EIA-600 in 1997.

CE-Bus offers seven different Physical Layers: Power Line, Radio Frequency, Twisted Pair, Infra-Red, Coaxial, Fibre-Optic and the Audio-Video Bus.

The PL layer utilises spread spectrum techniques, in the form of a 'chirp'. Intellon [13] have developed a PLC solution for home automation based around a 'chirp' system of spread spectrum PLC which complies with CE-Bus requirements. However, this solution does not comply with the CENELEC band requirements for PLC systems, which we will discuss in a later section.

2.4.4 EHS

The 'European Home System' (EHS) is an initiative sponsored by the European Community intended to encourage a standardised and interoperable system for home automation applications [14, 15]. EHS involves several physical mediums as well as PLC. The PLC technology utilises narrow-band FSK signalling, based around the SGS-Thomson ST7537HS1 modem device [16]. The protocol used is interesting as it incorporates a high level of error correction.

2.4.5 EIB

The 'European Installation Bus' (EIB) system for home & building electronics is touted as both a home automation and Fieldbus solution. Originally based around a twisted-pair physical layer, it now supports a range of other media, including power line, RF, IR, and a high-speed Ethernet-based backbone.

In a move to standardise automation systems, EHS, EIB, and BatiBUS (discussed later under industrial Fieldbus systems) are merging towards a common standard.

2.4.6 BACNet

BACNet stands for The Building Automation and Control network [17].

In the field of building automation, the BACNet standard has been developed by a committee of ASHRAE, the American Society of Heating, Refrigerating, and Air-Conditioning Engineers. BACNet is intended to interconnect sensors, actuators, and controllers for HVAC (Heating, Ventilating, and Air-Conditioning) equipment in buildings. BACNet includes a common message set and provisions to accommodate various local area network standards for transporting messages from one device to another.

BACNet transmits these messages over a variety of specified networks. Some are commonly used in office automation, such as Ethernet. The lower two OSI (Open Systems Interconnect) layers of the seven-layer LonTalk protocol are referenced as one of five options for transporting BACNet commands.

Having discussed home, building and industrial automation, and introduced some of the technologies used to implement it, we will next move on and consider the evolution of another major facet in our chosen subject area, namely computer and industrial networking.

Chapter 3 : Computer and Industrial Networking

In this chapter we will consider the development of computer networking technology and consider how it led to the kind of industrial networking that we are concerned with in this thesis.

To begin, we will introduce two generic terms commonly encountered in the context of networking - *LAN* and *WAN*.

LAN stands for 'Local Area Network' and describes a system that extends over an area no wider than (typically) an individual building or commercial/industrial site. LANs may consist of component networks using different technologies, linked together using bridges and routers. In this thesis, we are dealing with industrial automation, and industrial networks can be considered a special form of LAN. We will go on to describe some typical LAN technologies in a later section.

WAN stands for 'Wide Area Network' and, as the name suggests, covers a somewhat larger geographical area. This might be, for example, an entire town or city. In practice, a WAN may consist of a network of individual LANs, for example linking a number of industrial sites. The most well known (and extreme) example of a WAN is undoubtedly the Internet, whose extent is world-wide.

In the next section, we will look at how computer networking developed. We will begin with WANs, as these actually pre-date LANs.

3.1 Early Wide Area Networks

The impetus behind the development of computer networking [18] can be traced to the start of another technological revolution - the Space Race. Following Russia's successful launch of the first artificial satellite 'Sputnik' in 1957, pressure was on the Americans to match the achievement. As a result of this, in 1958, an organisation called 'ARPA', for 'Advanced Research Projects Agency', was formed within the American Department of Defence ('DoD'), with the aim of regaining the lead in science and technology.

Within a few years, ARPA had begun to focus on computer networking and communications technology. In 1962, Dr. J. C. R. Licklider became head of ARPA's research concerned with improving the military's use of computer technology. Of particular interest to the military was the concept of a 'blast-proof' decentralised computer network.

Dr Licklider also wanted to make the government's use of computers more interactive, and was behind a move to place ARPA's research contracts with universities, rather than in the commercial, private sector. These factors gave an impetus to the concept of computer systems at different universities being interconnected, for reasons of economy and the sharing of resources [19]. Work in this area throughout the 1960's led to the formation of what was to become known as the ARPANET.

3.1.1 The ARPANET

In the late 1960's initial proposals were made to create such a decentralised computer network. The National Physical Laboratory in Great Britain set up the first experimental network on these principles in 1968. Shortly afterwards, ARPA decided to fund a larger, more ambitious project in the USA. The nodes of the network were to made up of the high-speed supercomputers of the time.

In the autumn of 1969, the first node was installed at the University College of Los Angeles (UCLA). By December 1969, there were four nodes set up on the network, which was named ARPANET, after its Pentagon sponsor. The four computers could transfer data to each other on dedicated high-speed (50 kbps) transmission lines. They could even be programmed remotely from the other nodes. Thanks to ARPANET, scientists and researchers could share one another's computer facilities by long-distance. During 1971, the network expanded to fifteen nodes, and during 1972, to thirty-seven nodes.

Throughout the 1970s, ARPA's network continued to grow. Its decentralised structure made expansion easy and it is important to note that it could accommodate many different kinds of machine as nodes, so long as individual machines each communicated using the common protocol. With ARPANET, the foundation was laid for what would, in later years, become the Internet.

Before going on to consider the development of local area networks, which would lead to industrial networks, we will look at another important early milestone in wide area networks.

3.1.2 Aloha

Aloha is another example of an early WAN (1971), and was created in order to permit the sharing of computers amongst facilities around the Hawaiian Islands in the USA [20]. For these geographical reasons, it was radio-based, as any other medium would have proved too expensive to implement. Basically, outstations transmitted packets of data to the central computer, which sent an acknowledgement if the data was received correctly.

A disadvantage of the system lay in the fact that any station could begin transmission at any time. This meant that collisions were likely to occur if more than one station attempted to transmit and their transmissions overlapped. The only response to this was for the originating stations, in the absence of an acknowledgement signal from the central computer, to attempt retransmission. Even here, there was still the risk of overlap, and if the message failed to be delivered after a certain number of attempts, the originating stations would give up, and flag an error.

To try and improve this situation, an enhancement to the standard Aloha system (called 'Slotted Aloha') was made. In slotted Aloha the central computer transmitted a synchronisation signal spaced at intervals sufficient to allow an entire data packet to be sent and acknowledged. Stations wishing to transmit would only do so after a synchronisation pulse. This made collisions somewhat less likely (although they were not entirely eliminated) and improved the throughput of the system.

The Aloha system highlighted the need for arbitration schemes to facilitate multiple users accessing a network without excessive problems due to collision. We will be discussing these arbitration schemes in greater detail in a later section, but next will consider the development of the other classification of network – the LAN.

3.2 Local Area Networks

WANs came into existence because of the need to network expensive mainframe computers located large distances apart. As the 1960s progressed, and technology improved, manufacturers developed smaller, lower cost, computers (referred to as minicomputers). With such technology, it was economically feasible for a particular location to have many such computer systems in place.

As a result of this, it became desirable to share the resources of these machines, and this need drove the development of local area networks. We will begin with a discussion of the most popular LAN technologies - Ethernet.

3.2.1 Ethernet

Ethernet has arguably become the most pervasive technology for local area networking. Originally developed in the early 1970's [21] it continues to develop to the present day. The original concept utilised a physical medium consisting of a 'bus', or 'backbone', of heavy-duty co-axial cable, fitted with terminating resistors, and referred to as the 'Ether'. Into this were tapped transceivers that injected signals into the bus. Computers ('nodes') were then connected to this via cabling and an associated controller. It can be seen that in this arrangement, any nodes' transmission will be received by all of the other nodes on the network, termed a 'broadcast' scenario.

A sketch showing this original arrangement (drawn by one of the creators of Ethernet) is reproduced below. Data passed over this network at a basic 'raw' data rate of 10 Mbps (10 million bits per second).

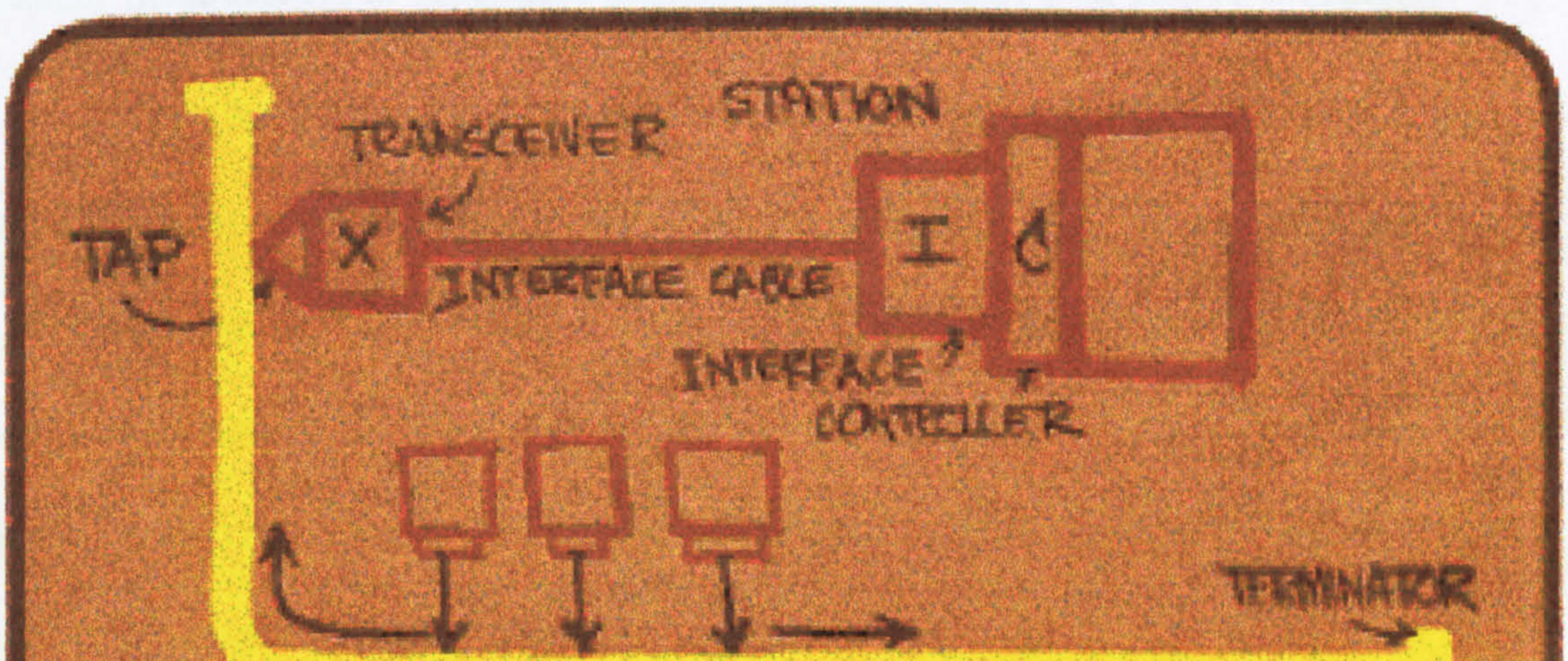


Figure 17: The Original Ethernet Concept

It can be seen from the previous diagram that transceivers could be introduced at any convenient point along the length of the 'Ether'. This original arrangement (referred to technically as 10-base 5) was nevertheless somewhat cumbersome. It was later refined with the introduction of a trunked arrangement, whereby a (thinner) co-axial cable passes directly to each computer on the network, rather than via a transceiver/controller arrangement (referred to technically as 10-base 2).

A further refinement utilises twisted pair cabling, this time in a star configuration, utilising a 'hub' or 'data concentrator' to receive data from one node and distribute it to all of the other nodes connected to the hub. This last variant of Ethernet is referred to technically as 10-base T. We will discuss the network topologies mentioned in a later section.

All three configurations are still to be found in use today, and indeed Ethernet networks can be created having a complex topology consisting of a combination of all these types. Typically, 10-base 5 might be used to form a 'backbone', passing the length of a building or site. Into this would be connected a number of hubs, servicing many individual PCs using twisted pair cabling (10-base T). 10-base 2 might be a choice for smaller installations, or be used as a means of linking hubs over shorter distances.

There have been further enhancements to the basic Ethernet system that have ensured its continued use in the future. The alternative medium of fibre optic cable is an option at 10 Mbps, and in addition, higher transmission speeds are possible. 100 Mbps is now commonplace even in low-end installations, using twisted pair or fibre optic media, and there are new transmission rates of 1000 Mbps ('Gigabit'), and even 10,000 Mbps, primarily using fibre optic media.

We have already mentioned arbitration schemes in the context of the 'Aloha' WAN. We will next discuss them in greater detail, before introducing some other LAN systems.

3.2.2 Arbitration Schemes and Other LAN Technologies

A desirable feature of any networking system where two or more nodes are sharing the medium is an arbitration scheme. This is necessary to avoid collisions between packets of data should more than one computer wish to transmit on the network at the same time. We have already mentioned Aloha, where the original, simple, scheme was inefficient under loads due to the lack of such an arbitration system.

We will next look at ways of achieving this situation. Aloha was improved by the introduction of 'Slotted Aloha', where distinct timeslots were allocated for transmission by the remote systems, scheduled by the central computer.

The type of network where a single system specifically provides some overall supervisory function is referred to as 'Master-Slave', where there is a single node designated the 'Master', with all of the others being 'Slaves'.

The allocation of timeslots by the master, as in slotted Aloha, is not the only means of achieving arbitration. Alternatively, all communication may be initiated by the Master, which requests each Slave in turn to send any data that it may have. This process is known as 'Polling'. Therefore, only one node will ever be transmitting at any one time, and contention is avoided. Unfortunately, such a scheme is inflexible in so far as communication between Slaves is not possible except via the Master. Nevertheless, this arrangement can often be found in industrial control applications where relatively simple 'Slave' processors need to communicate with a central 'Master' controller.

More commonly found, as an alternative to 'Master-Slave' systems in computing networks, is the 'Peer-to-Peer' scheme. Here, all of the nodes have equal status on the network, and can make a transmission intended for any (or all) of the other nodes. In such systems it is imperative that there be a means of avoiding collisions should more than one node wish to transmit at the same time.

The arbitration system used with Ethernet is called CSMA/CD (Carrier Sense Multiple Access with Collision Detect). We will now explain the derivation of this term.

In an un-arbitrated network system with many users - termed 'Multiple Access' or 'MA', such as the original 'Aloha' system already described, users were able to transmit at any time. As long as no other user transmitted whilst another was already transmitting, there was no problem. However, if two users transmissions overlapped, the transmissions would be corrupted. The only manner in which this could be detected would be when the receiving user did not acknowledge the transmission, or reported that the transmission was received but corrupted (depending on the extent of the corruption). This acknowledgement and error detection is a function of the transmission protocols used, and these will be discussed in a later chapter.

One way of avoiding collisions is for a node intending to transmit to first listen to the line to detect is another user is already transmitting, and not transmitting if this is the case. This is referred to as 'Carrier Sense', or 'CS', giving the combined term 'CSMA'. A limitation of CSMA is that it will not detect the instance of two users starting to transmit simultaneously.

A way around this limitation is for users to monitor the line whilst they are transmitting. Should another user start transmitting, there will eventually be a mismatch in the data which will be detected by both users, who will then both cease transmission. After a delay, incorporating a random element so that neither start again simultaneously, one of the users will begin retransmission, hopefully without contention this time. This is termed 'Collision Detection', or 'CD', and gives us the overall term CSMA/CD, as applicable to Ethernet. It should be noted that collision detection only works when the action of a conflicting signal can be detected at the sending node. It is not applicable, for example, to a radio based system.

A variation of CSMA/CD is CSMA/CA. The 'CA' in this instance stands for 'Collision Avoidance'. This technique is only possible where a collision between data packets is non-destructive, usually implying 'dominant' and 'recessive' signalling states in the transmission medium, and a protocol in which nodes have a clearly defined order of priority. These factors permit collisions to be detected without compromising data from the 'superior' node. This allows the 'subordinate' node to relinquish transmission in an orderly manner, avoiding the need for both nodes to retransmit. An example of CSMA/CA is the CAN system, which will be discussed in a later section.

CSMA techniques are not the only means of avoiding contention in a multiple access peer-to-peer network. An alternative is known as 'Token Passing'. Here, a user may only transmit when they have permission. This is somewhat similar to the master-slave system already described, except that permission to transmit is not granted by a master node, rather it is imparted by the possession of the 'token', a special form of message passed in turn to each node on the network. Once the node in possession of the token has finished any transmission which it may need to carry out, it re-transmits ('passes') the token to the next node in sequence.

Token passing schemes offer greater efficiency than CSMA techniques, since collisions, and their subsequent need for retransmission, are avoided. Another important factor is determinism - it is easy to predict with a token passing scheme the maximum delay before a node is able to pass a message. With CSMA, this delay is very variable, according to the network loading, and in extreme instances may be unacceptably long.

These arbitration schemes have been formalised as standards by the American Institution of Electrical and Electronic Engineers (IEEE). These standards also deal with other factors such as the physical layer for the network, and the network topology. We will describe these standards in a later section. However, as we have already mentioned topologies whilst discussing Ethernet, we will next describe in more detail the different terminology used.

3.3 Physical and Logical Network Topologies

We will next present examples of the common topologies in use in networking systems. The diagrams are essentially self-explanatory.

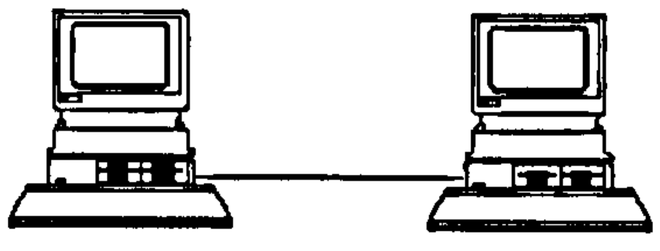


Figure 18: A Point to Point Network Configuration

Where only two computers are to be networked, this represents the simplest possible arrangement.

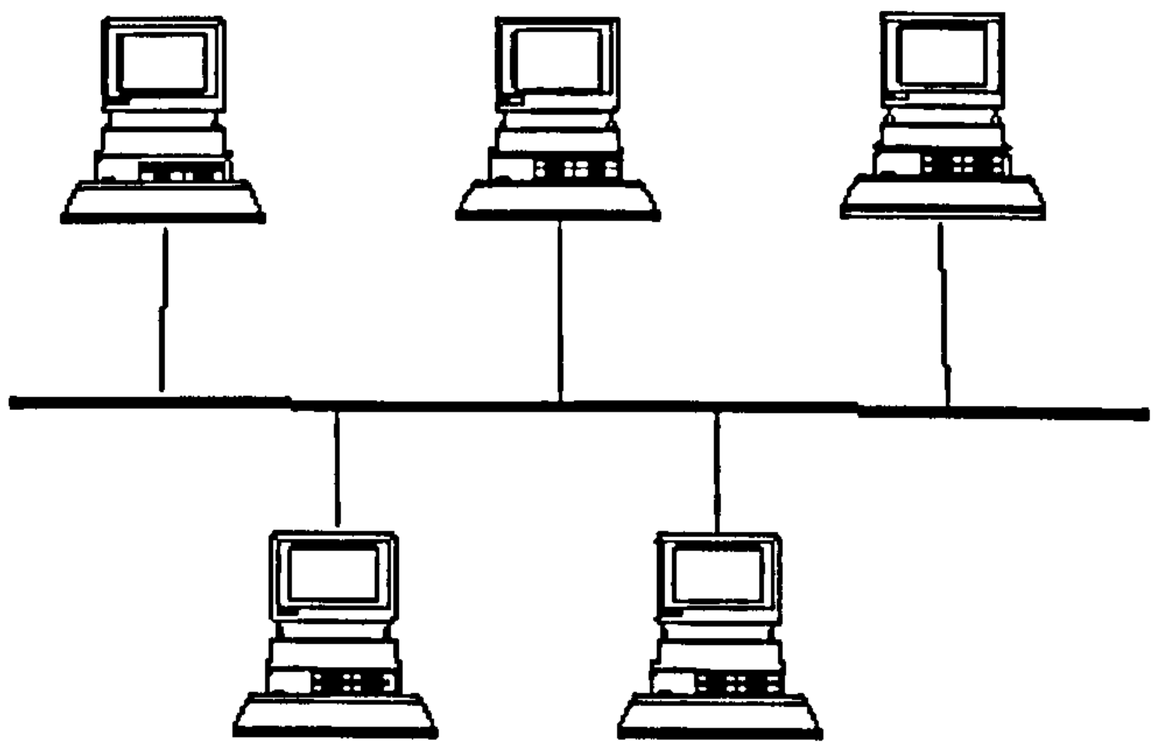


Figure 19: A Bus Network Configuration

In this arrangement, all the systems are 'hung' off a central 'bus' line.

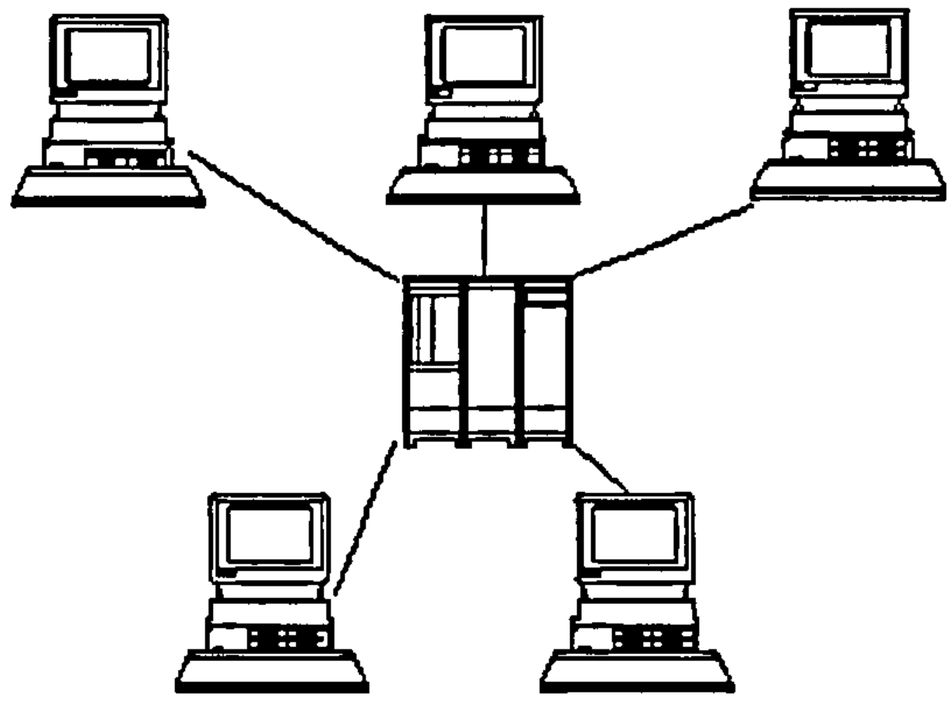


Figure 20: A Star Network Configuration

In this scheme, all of the systems connect to a central 'hub' over individual lines.

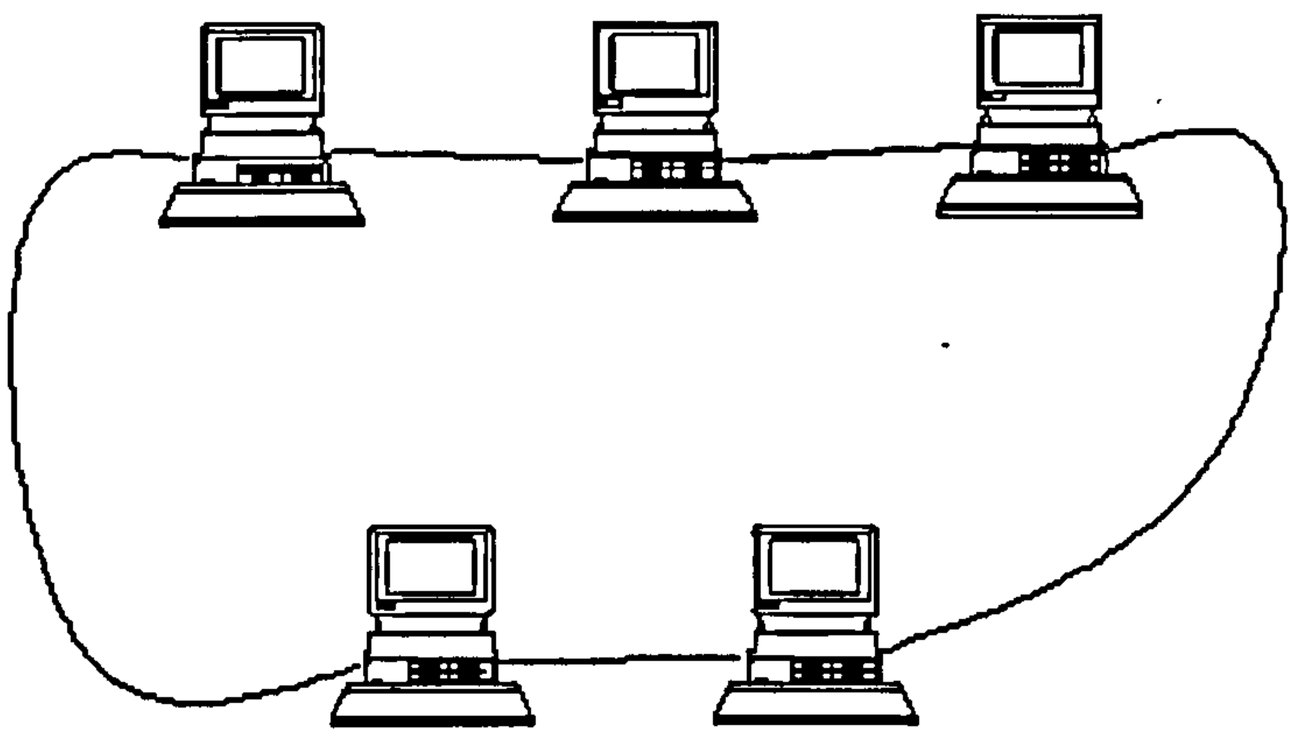


Figure 21: A Ring Network Configuration

In this scheme, each system connects to two adjacent ones to form a physical ring arrangement. Data is passed around the ring from one node to the next.

3.3.1 Logical Networks versus Physical Networks

The physical topology, as shown in the diagrams above, shows how the network has been cabled. The logical topology describes how the network operates from a communications point of view. It is thus possible, for example, to have a physical star topology, operating as a logical bus. In other words, a transmission from any branch of the star is broadcast to all other nodes. Other variations are possible, and these will be discussed next, when we deal with the IEEE networking standards.

3.4 Networking Standards

We have already mentioned that IEEE standards have been raised to cover networking. These have also been adopted as ISO standards. We will describe the common standards below.

3.4.1 IEEE 802.3 (ISO 8802-3)

This defines the original Ethernet system - transmitting data at 10 Mbps, and using a logical bus topology (physically, however, as already described, the network can be configured as a bus or a star). Data is broadcast throughout the network in no particular physical direction. All machines receive every broadcast, but only those meant to receive the data respond with an acknowledgement. The network arbitration scheme is CSMA/CD.

3.4.2 IEEE 802.4 (ISO 8802-4)

This also defines a physical network that has a bus topology, and is a broadcast network. Unlike 802.3, this network utilises a token passing arbitration scheme. This system is called 'Token Bus'. The Manufacturing Automation Protocol (MAP) standard, discussed later, uses an 802.4 physical layer.

3.4.3 IEEE 802.5 (ISO 8802-5)

This defines a network that transmits data at 4 Mbps or 16 Mbps and uses a logical ring layout, but is physically configured as a star. This system is called 'Token Ring', and was originally developed by IBM. Data moves around the ring from station to station, and each station regenerates the signal. For this reason, it is not a broadcast network.

There are other network systems in use. 'Arcnet' is a well-known one that does not conform to a standard. It uses a token-passing bus access method, but not the same one as IEEE 802.4, and 'Fibre Distributed Data Interface' (FDDI) is a new ANSI standard for a fiber-optic LAN that uses a token-passing protocol to transmit data at 100Mbps on a ring.

The purpose of the above standards is to define the network's physical characteristics and how to get raw data from one place to another. They also define how multiple computers can simultaneously use the network without interfering with each other. These are functions of what is called the Physical (dealing with the transmission medium and topology) and Data Link (dealing with the arbitration scheme) layers of what is called the 'OSI model'.

We will next describe what is meant by the term 'OSI model'.

3.5 The OSI 7-Layer Model

The term OSI is an acronym for 'Open System Interconnection' [22]. Broadly speaking, it is an effort by the ISO (International Standards Organisation), representing national standards organisations from around the world, to provide international standardisation of many aspects of computer-to-computer communication, extending from the lowest level of signalling techniques to high-level interactions in support of specific types of application.

The work on OSI was initiated in the late 1970s, and completed in the late 1980s and early 1990s. There are many OSI standards that have been created as a result of this work, but fundamental to the entire scheme is the OSI reference model.

The OSI reference model is the structure of an 'ideal' network architecture. This Model outlines seven areas, or layers, for a typical networking system. The different layers are intended to split the various functional requirements of the network into discrete and defined areas of abstraction, in order to provide maximum flexibility.

The reason that such an abstraction is desirable is that, should a single piece of software be written to encompass an entire application scenario, including communications functions, the end result is extremely inflexible. An attempt to change a single aspect of the communications system might involve complicated changes within the entire body of the software.

With a layered system, and one with an orderly communication between layers, only software covering the affected layer will need changing, a much more manageable prospect if the overall software is large in size.

The criteria used to define the layers in the OSI model are as follows:

- A layer should define the need for a different level of abstraction, without creating an unrealistic number of layers.
- The equivalent layers in different networking systems should contain similar functions.
- Changes to individual layers should not necessitate changes to other layers.
- Layers should be structured so that necessary information exchanges between layers should be at a minimum.
- Layers should exchange information only with those layers immediately above and below.

Applying these requirements, the following layers were defined and named (from highest level to lowest):

- *Layer 7* - ***APPLICATION***
- *Layer 6* - ***PRESENTATION***
- *Layer 5* - ***SESSION***
- *Layer 4* - ***TRANSPORT***
- *Layer 3* - ***NETWORK***
- *Layer 2* - ***DATA LINK***
- *Layer 1* - ***PHYSICAL***

Figure 22: The Seven Layers of the OSI Model

Typically, data passes upwards and downwards (depending on the data direction) through each layer in turn. This is illustrated in the next figure. There are exceptions to this arrangement, which will be described later.

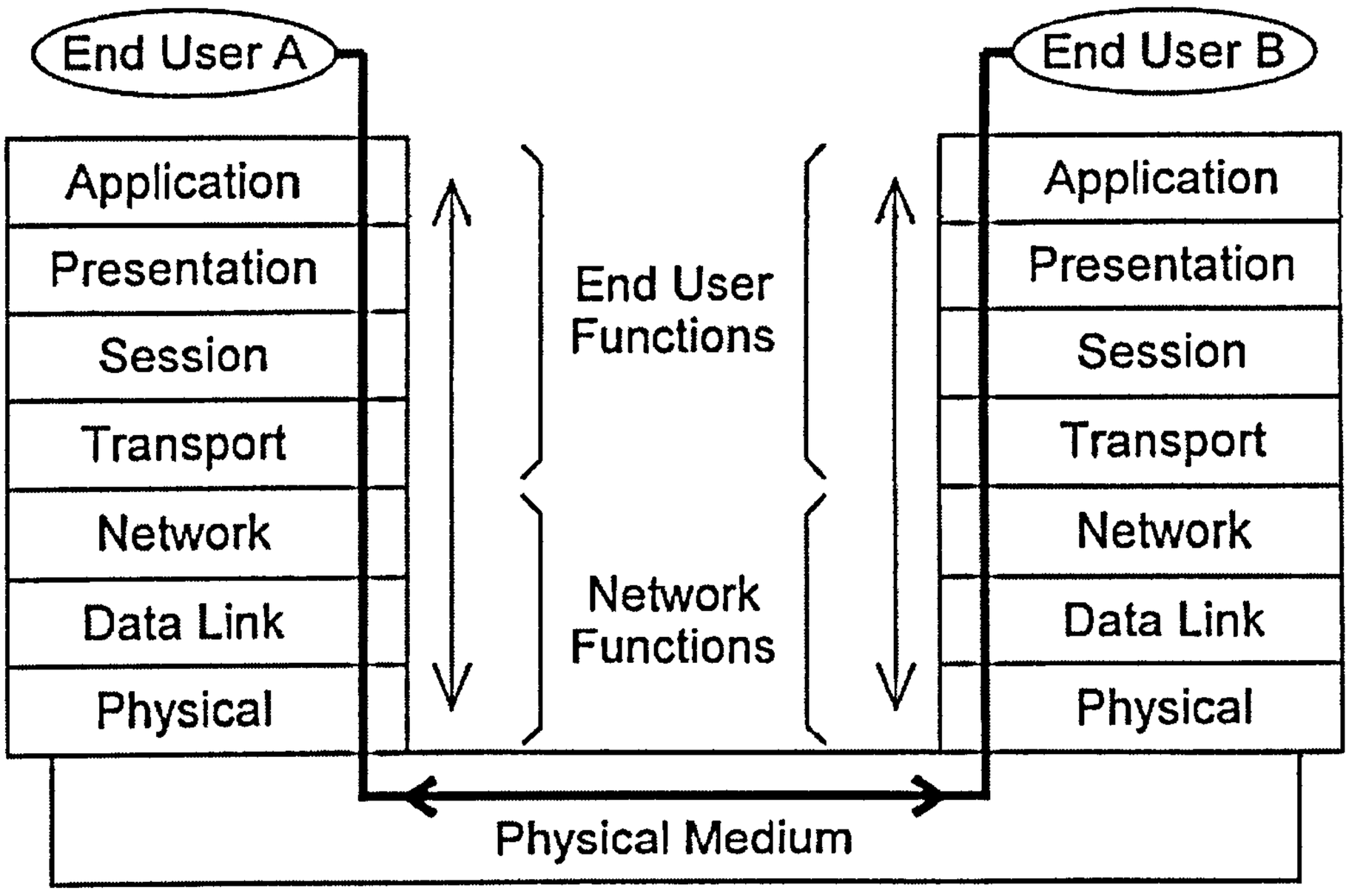


Figure 23: Data Flow through the OSI Model

We will next look at each of the layers in more detail:

3.5.1 Layer 1, The Physical Layer

This layer defines the physical means by which data is moved around the network. For example, this may involve electrical currents, physical pulses or optical pulses.

This layer also defines the means of connection to the communications system (cabling types etc.). The requirements and characteristics for transmission generally are documented in separate standards such as V.35 or RS-232. The Ethernet standards (IEEE 802 series) that we have already mentioned define the details of the physical layer (as well as the MAC functionality of the data link layer - this will be explained in the next section).

The Physical Layer is responsible for transmitting bits from one network node to another.

3.5.2 Layer 2, The Data Link Layer

The function of this layer is to reliably pass packets of information directly from one node to another. Data coming down from layer three (the Network layer) is encapsulated in a packet containing various items of additional data (the structure of layer two packets) will be discussed in greater detail in a later section. The packets are then passed to the physical layer for actual transmission. In the opposite direction, received packets from the physical layer are checked for their integrity, and the 'stripped' data passed up to the network layer.

The Data Link Layer is typically subdivided into two layers - the Logical Link Control (LLC) and the Media Access Control (MAC) sub-layers. The LLC sub-layer provides error control and works primarily with the Network Layer to support connectionless or connection-oriented services. The MAC sub-layer defines the arbitration and access protocols for the actual physical medium.

3.5.3 Layer 3, The Network Layer

This layer sets up connections and routes data from one node to another. It manages the addressing of messages and the translation of logical addresses (such as IP addresses) to physical addresses (MAC addresses). The Network Layer also determines the route data traverses between source and destination host, which may not be a direct connection. If the packets being transmitted are too large for the destination host's topology, the Network Layer compensates by breaking the data into smaller packets. These packets are then reassembled at the destination.

3.5.4 Layer 4, The Transport Layer

This layer segments and reassembles data into a data stream. It provides an end-to-end connection between source and destination hosts. When data is transmitted from a source to a destination host, the data is segmented into smaller collections of information. The segments are numbered sequentially and are sent to the destination host. When the destination host receives the segments, it sends an acknowledgement of their receipt. If a segment is not received, the destination host can request that a specific segment be re-sent. This provides error control for data transport. Additionally, this layer can set up alternative routes for data, as appropriate.

3.5.5 Layer 5, The Session Layer

This layer enables two applications on separate hosts to establish a communication connection called a session. These sessions ensure that messages are sent and received with a high degree of reliability. The Session Layer performs security functions to make sure two hosts are allowed to communicate across a network. The Session Layer co-ordinates the service requests and responses that occur when applications communicate between hosts.

3.5.6 Layer 6, The Presentation Layer

This layer determines how data is formatted when exchanged between network computers. The data received from the application layer is translated into a commonly recognised, intermediary format. The Presentation Layer is also responsible for all translation of data, encryption of data, character set conversions and protocol conversions.

3.5.7 Layer 7, The Application Layer

This layer enables programs to access network services. It does not deal with programs that require only local resources. To use the Application Layer, a program must have a communications component that requires network resources – e.g. Electronic Mail, or the World Wide Web.

It can be seen that the full seven-layer model is quite involved and complex in structure. This belies its origins in a purely computer-based communications context, where all of these levels of abstraction are necessary. In home or industrial networking, including PLC systems, the full model presented above may not be necessary, and can in fact be simplified considerably. We will look at this idea next.

3.6 Home/Industrial Automation and the Reduced OSI Stack

Within the context of a home or industrial automation system, the seven layers of the OSI model may be reduced to typically just three - the Application, Data and Physical layers.

There are simple reasons for this, apart from the fact that there is less need for the complexity of the different layers. The remote nodes likely to be found in typical home and industrial control networks will most likely be based around discrete micro-controllers, often low-cost types. To implement a full seven-layer stack would involve an unnecessary amount of system resources. Consequently, the reduced scheme would be preferred.

A notable exception to this reduced stack is found in the Echelon LonWorks system, already introduced in a previous section, where the entire seven layers are implemented. It should be noted though, that in order to achieve this, a custom microcontroller – the 'Neuron Chip', was originally utilised to implement a LonWorks node, and this device contains three separate microprocessors internally, to handle the processing overhead. As technology has progressed, and increasingly powerful microcontrollers have become available, it has become feasible to implement the LonWorks protocol on single devices. Indeed, as a move towards having LonWorks adopted as an international standard, rather than as a proprietary system, Echelon have made their protocol available in the public domain.

Having discussed the history of general computer networking, we will now move on to the subject area of networking specifically within an industrial environment. As a parallel to computer networking, early industrial networks tended to encompass a wide geographical area, i.e. they can be considered as a form of WAN.

3.7 MAP, TOP and Industrial Networking

MAP [23] stands for 'Manufacturing Automation Protocol'. Development was started in 1980, by General Motors, as a specification for a real-time protocol for use in manufacturing. This would operate at 10 Mbps over a broadband cable within a factory environment and utilised a token passing protocol.

The protocol was eventually expanded to include a 5 Mbps network capable of interfacing with manufacturing robots, and other automated tools. The overall concept of MAP was intended to permit all aspects of the design and manufacturing process to be integrated and connected over the MAP network. For example, a part could be created using computer aided design (CAD) and the information for the manufacture of the part passed via the MAP network direct to the machine tools which would perform the manufacturing operation.

TOP stands for 'Technical and Office Protocol'. It is a very similar in concept to MAP, and was originally devised by the Boeing Company. However, it relies on an Ethernet CSMA/CD network rather than a token ring.

The overall concept of a MAP or TOP network is shown in the following diagram.

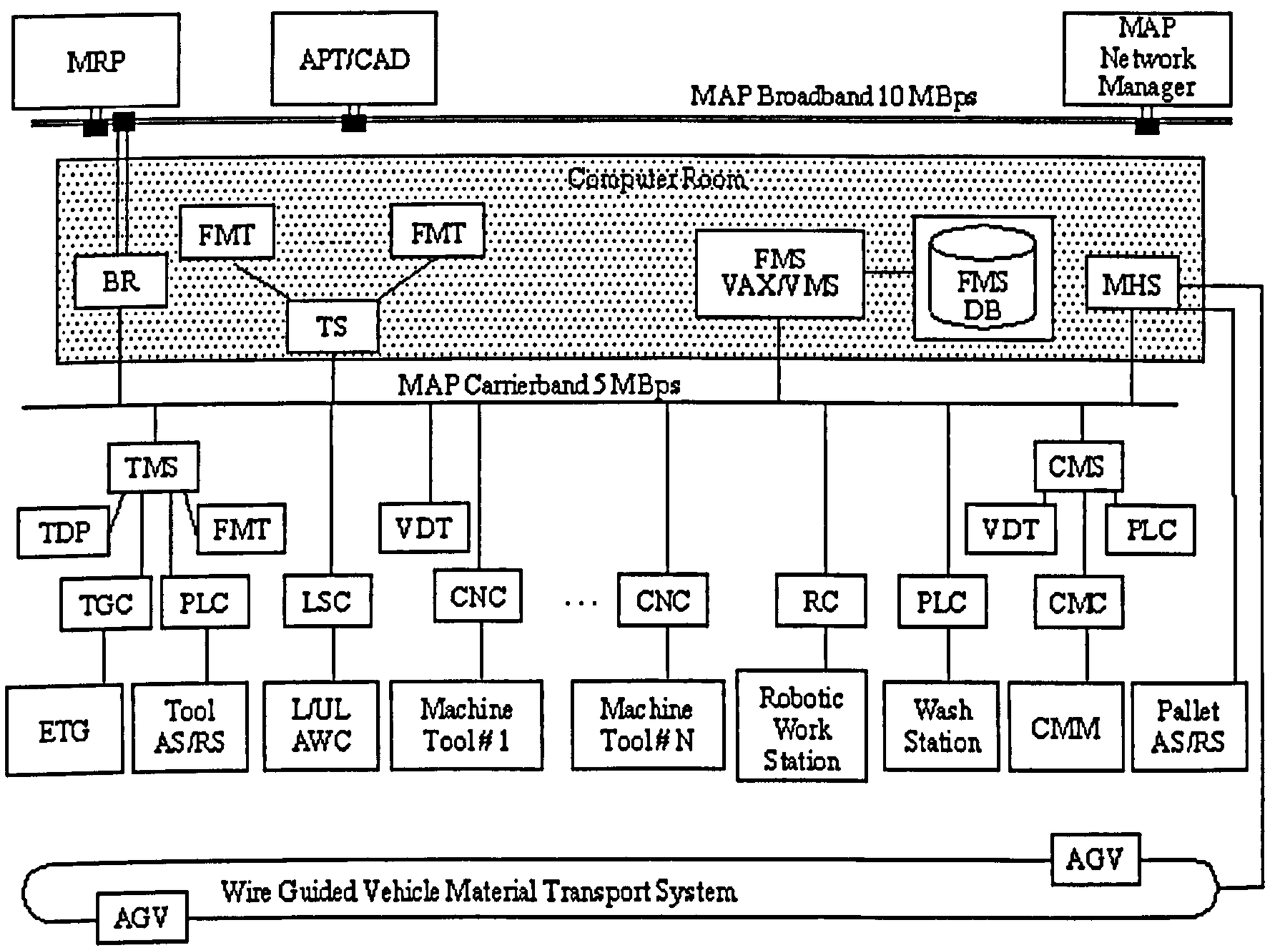


Figure 24: Diagrammatic Representation of a MAP Network

The previous diagram contains many abbreviations pertinent to the overall manufacturing task being performed by the MAP network. For completeness, we will briefly describe some of them.

- MRP stands for 'Manufacturing Resource Planning'. It is a method for the effective planning of all resources within a manufacturing company.

- CAD has already been mentioned, standing for 'Computer Aided Design'.

- APT is a language for numerically controlled machine tools, and likely to be generated by CAD applications to control the actual manufacturing operation.

- MHS stands for 'Message Handling System'.

- PLC has also already been mentioned, standing for 'Programmable Logic Controller'.

- CNC stands for 'Computer Numeric Control', and describes a type of machine tool that may be automatically operated.

- AGV stands for 'Automatically Guided Vehicle', under the control of other devices on the MAP network.

Summing up, it can be seen that MAP and TOP are essentially 'high level' networks, with all of the nodes on these networks being sophisticated devices in their own right.

The concept of an Industrial Fieldbus expands the industrial network concept down to the lowest level of sensors and actuators (indeed, some Fieldbus solutions are referred to as sensor/actuator busses). For example, a conventional Programmable Logic Controller (as already discussed in a previous chapter) will have a number of inputs and outputs all discretely wired to the PLC. A Fieldbus will integrate them all into a network in their own right. In the next chapter we will look at the evolution of the Fieldbus concept.

Chapter 4 : Towards an Industrial Fieldbus

What is the definition of a Fieldbus? The U.S. based Fieldbus Foundation describes it as follows: 'Fieldbus is an all-digital, serial, two-way communications system that interconnects measurement and control equipment such as sensors, actuators and controllers. At the base level in the hierarchy of plant networks, it serves as a Local Area Network (LAN) for instruments used in process control and manufacturing automation applications and has a built-in capability to distribute the control application across the network'.

They also state that a Fieldbus must be an open system that is supported by several vendors, and not tied to a single technology. The various commercial Fieldbusses available, however, are not interchangeable. The differences between them are so profound that they cannot be easily connected to each other, even though they may have certain characteristics in common, such as the physical layer.

Before moving on to discuss Fieldbusses proper, it is worth considering that there are some more localised forms of bus, intended for short range communications within an item of equipment. We will next take a look at these.

4.1 Local Control Networks

There has long been an incentive to use some form of serial communication between devices within an item of electronic equipment. This is primarily due to the potentially high number of interconnections between different devices (and in many ways this is a parallel to the situation found, on a wider scale, within the industrial scenario that we have already described in earlier chapters).

Consider the following scenario - a microprocessor interfaces to a number of peripheral and support devices such as ROM, RAM, and I/O devices. If discrete connections between all these devices were the only option, there would need to be dozens of lines in total. In reality, of course, a parallel bus arrangement is used, carrying address and data in parallel to all of the devices. Even so, this still requires a significant number of lines, which must be routed to all the devices connected to the central controller.

Of course, sophisticated modern microcontrollers have many of the required peripherals 'on-chip', but even so, there is always likely to be a requirement for additional specialised peripheral devices.

Should some of these be located physically remote, then the added complication of bus buffering is required. It is so much simpler if a serial link is used, requiring only two (or even just one) line to pass to each peripheral device.

If the serial bus also carried address information, decoded by each peripheral as appropriate, then the bus may be run to each device in turn, further reducing the number of I/O lines required on the central processor, and effectively forming a small localised network.

Several variations of such a serial link exist, but we will look specifically at two, which are notable for having, if not by design, but by subsequent enhancement, the ability to operate over somewhat greater distances. Indeed, one of them, CAN, may be considered as simple forms of Fieldbus in its own right, as we will discuss later.

We will begin, though with a look at the well established I^2C bus.

4.1.1 The I^2C Bus

The term I^2C is short for IIC, standing for 'Inter Integrated-Circuit Communication', which succinctly describes the purpose for which it was developed. The I^2C bus [24] was created by Phillips Semiconductors some 20 years ago. It is a synchronous communications system, and requires two signal lines. These are called SDA (Serial Data) and SCL (Serial Clock). As their names suggest, SDA carries data, and SCL is a clock signal used for synchronising the data transfer.

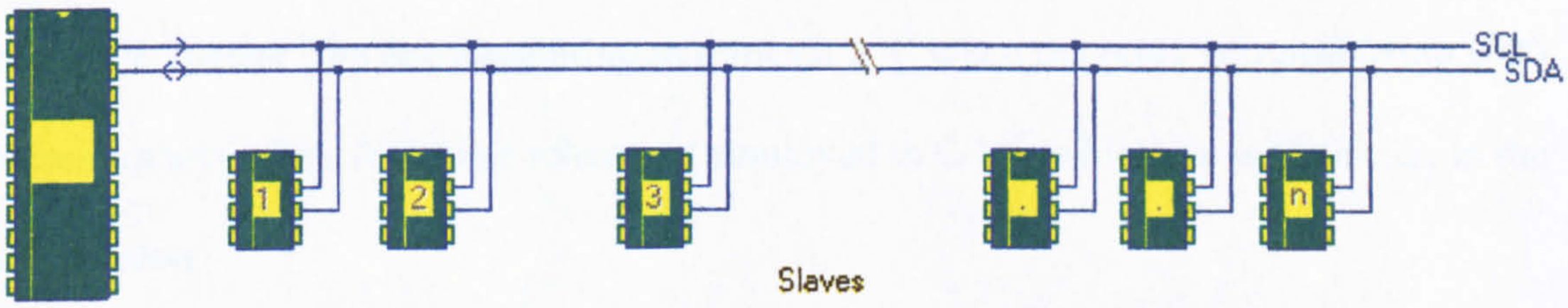


Figure 25: I^2C Bus Arrangement

These are open collector inputs/outputs, equipped with (typically) a 4k7 pull-up resistor (not shown on the above figure). At rest, both SDA and SCL are pulled HIGH (at the positive supply voltage, designating a logic '1') by these resistors. The basic I^2C scheme is a master-slave set-up, and all commands originate from the master. This is usually the central microprocessor/microcontroller in the system.

The original version of I^2C operates at a signalling rate of 100 kbps. This has been enhanced to provide an option of 400 kbps, and still further to give an option of 3.4 Mbps. These different speeds may be mixed on the same I^2C bus. Typically, I^2C devices are stand-alone, or integrated within a microcontroller.

Interestingly, I^2C supports a multi-master option, permitting more than one master to share a single bus. Here, of course, it is necessary to have a scheme to avoid contention should more than one master wish to use the bus at the same time. This aim is achieved by the master node listening before transmitting, and holding back if another transmission is heard. Should two masters start to transmit simultaneously, this is handled gracefully thanks to the 'dominant'/'recessive' transmission scheme that arises because open collector outputs and pull-up resistors are used (the 'low' state is dominant). All masters transmitting monitor the bus as they do so. As soon as a difference in the bit stream is detected the 'recessive' master (the one attempting to transmit a '1' when the other is transmitting a '0') ceases transmission. A similar scheme is employed in CAN, which we will discuss in the next section.

4.1.2 The CAN Bus

CAN stands for 'Controller Area Network' [25], and has its origins in the automotive industry, where it was intended for simplifying vehicle wiring looms (for this reason it has also been known as the 'Controller Automotive Network'). CAN is a serial bus, having robust error-handling, and operates at speeds of up to 1 Mbps. Distances of up to 40 m may be covered at 1 Mbps, increasing to 1 km at a lower speed of 20 kbps.

Typical physical layers found in can are a Single-wire (plus ground) or a Two- wire differential signalling system, based on the RS-485 standard, using twisted pair cabling. . The number of nodes in a simple CAN installation is limited only by electrical characteristics of the physical layer, whilst RS-485 CAN is limited to 30 nodes per network segment.

Like I^2C, the CAN physical medium supports 'dominant' and 'recessive' states, and this is employed in the arbitration scheme which we will discuss later. In addition, especially in automotive applications, there may be DC power supplied along with the CAN signal.

The logical structure of a CAN network is as follows: All nodes are peers and every node receives every message. Physically, the network topology can encompass any of the variations applicable to twisted pair media, e.g. Trunk, Star, Ring, or combinations of these.

An important concept within CAN signalling is the 'message id'. Message ids are used to identify every type of event or command in the system and, also, to assign a level of priority to the message itself. Specific message ids tend to be assigned to single nodes only, and serve as a means of a node identifying that a particular message is meant for it. The priority assigned to a message id is utilised in the CAN arbitration system.

In the event of two or more nodes starting to transmit simultaneously, the first variable part of the data packet will be the message id. As with I^2C, all nodes monitor the transmission line and when a dissimilar state is detected, the 'recessive' nodes stop their transmissions, allowing the 'dominant' node to continue. Since, in CAN, the low state is dominant, then the lowest message id numbers have highest priority. Message id's can be 11 bits in length, or 29 bits in what is referred to as 'extended' CAN format.

As with I^2C, CAN is typically implemented using a CAN controller which may be standalone or a part of the system microcontroller.

The overall ruggedness of CAN means that it is often applied as a Fieldbus in its own right (termed CAN-Open). In addition, there are other commercial Fieldbus offerings utilising a physical layer based on CAN and RS-485 techniques.

We will discuss these in the next section, along with some other current Industrial Fieldbus solutions.

4.2 Some Other Industrial Fieldbus Solutions

This is by no means a definitive list of Fieldbus systems, rather it intended to give a 'flavour' of the types of the technologies available. We will start with some basic 'sensor-bus' type systems before moving on to more sophisticated Fieldbus networking schemes.

4.2.1 HART

HART is an acronym for 'Highway Addressable Remote Transducer'. The HART system [26] was initially developed by the Rosemount Company to provide enhanced signalling facilities for existing 4-20 mA systems. It could even be considered as a form of 'DC power line carrier' in so far as the 4-20 mA loop constitutes the power line and the HART signal is sent as a modulated carrier frequency superimposed on the current flow.

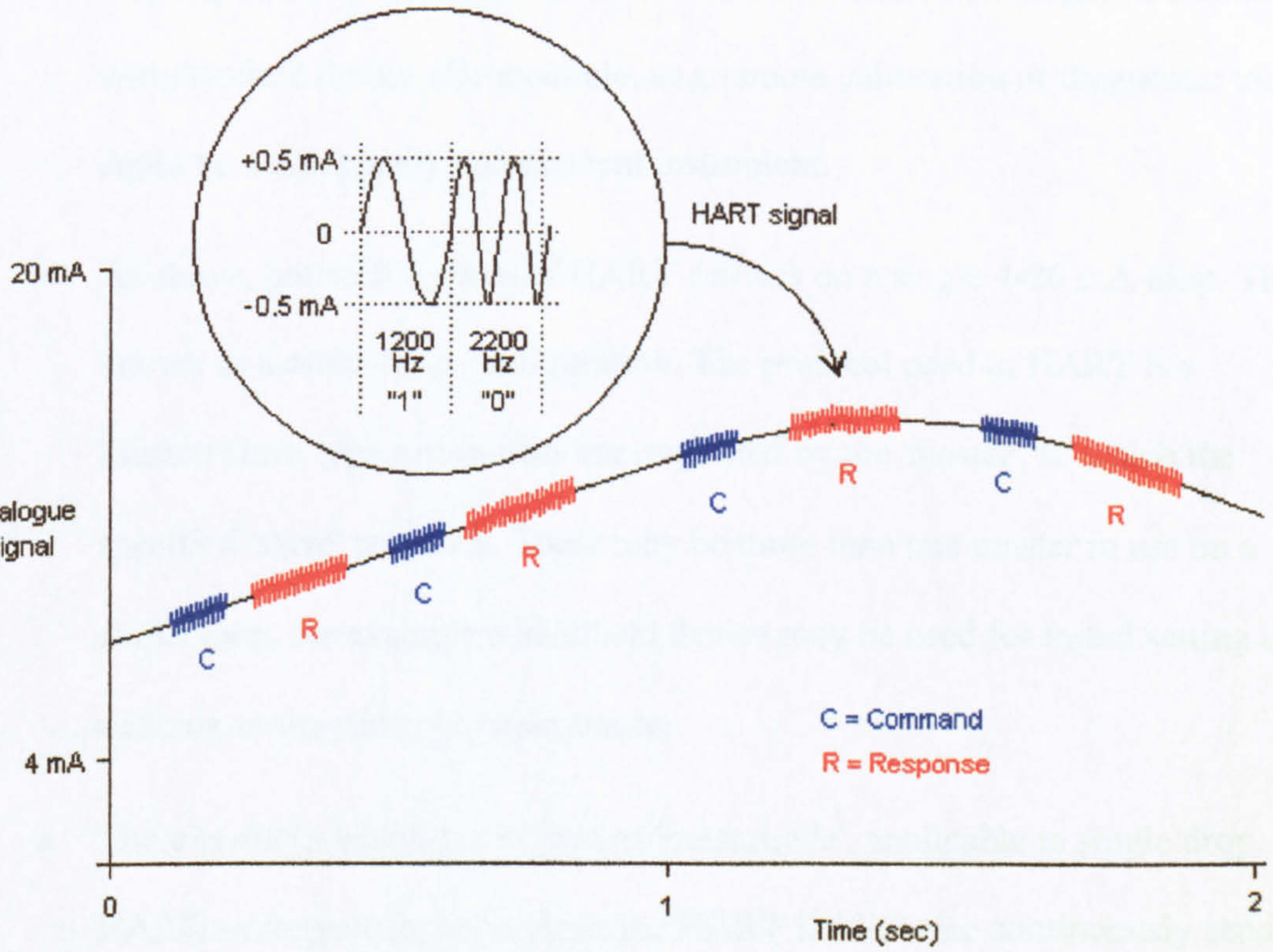


Figure 26: HART Waveform Super-Imposed on 4-20 mA Loop

The digital signalling in HART is based upon the Bell 202 standard for telephone modems, and utilises an FSK signal at carrier frequencies of 1200 Hz (representing logic '1') and 2200 Hz (representing logic '0'). The basic signalling rate of the HART system is 1200.

When utilised with a 4-20 mA loop, the tones modulate the current flow in the loop by a maximum of +/- 0.5 mA. Because this modulation has an average amplitude of zero, there is no overall effect on the operation of the existing analogue 4-20 mA loop, and any devices connected to it.

HART is a flexible system, and we will now describe some typical connection scenarios for it:

- A single 4-20 mA loop runs from a single field device, with a HART transducer offering two way communications. The HART transducer might be associated with the field device (for example, as a remote calibration or diagnostic tool), or could be a completely independent instrument.

- As above, but with a *chain* of HART devices on a single 4-20 mA loop. This is known as a multi-drop configuration. The protocol used in HART is a Master/Slave type - responses are requested by the 'master', to which the specified 'slave' responds. There may be more than one master in use on a single loop, for example a handheld device may be used for initial setting up in addition to the control system master.

- There is also a technique known as 'burst mode', applicable to single drop HART arrangements only. Here, the HART field device continuously sends data to the host, which simply accepts and processes it.

- Whilst originally used with 4-20 mA loops, HART can also operate over a conventional physical communications medium, capable of carrying the audio tones.

Messages in HART are formed from 8-bit data bytes, encapsulated using the standard start, stop, and parity bits found in the RS232 specification (this permits the use of standard communications circuits, for simplicity). A series of data bytes are (asynchronously) formed into packets containing identification, address, and checksum information.

We will discuss all of these aspects of communications in a later chapter and, as it is a typical example of such, will also discuss the HART packet structure in more detail.

4.2.2 BatiBUS

BatiBUS was developed by the Merlin Gerin, Airelec, EDF and Landis & Gyr Companies. The physical layer of BatiBUS consists of a twisted pair cable, carrying a 15V DC power supply. Signalling is at a rate of 4800 bps, and is achieved by 'shorting' (logic '1') or 'opening' (logic '0') the circuit. The 15V supply may be used to power a number of simple nodes on the network – typically up to 75, based on each consuming a maximum of 2 mA.

The maximum distances achievable in BatiBUS depend on factors such as the cable capacitance and resistance. There are no restrictions on the topology of the network - bus, tree, ring, or star may be used, or indeed a combination of these.

At the data link level, the network is a peer-to-peer scheme, based around a CSMA/CA protocol, with each node having a pre-set address.

BatiBUS has been documented in European and International standards.

4.2.3 BitBus

BitBus was developed by the Intel Company in 1984 as a means of adding remote I/O capability to its Multibus logic controllers. It uses a physical layer based on the RS485 standard, with a differential voltage signal sent over a screened twisted pair cable, arranged in a bus topology. BitBus operates at signalling rates of 62.5 Kbps or 375 Kbps and is another example of a Master - Slave system.

Distances of up to 13.2 km at 62.5 kbps may be achieved with the use of multiple repeaters. Single segments may be up to 1200 m long for 62.5 kbps signalling, or 300 m for 375 kbps. Up to 32 nodes may exist on one segment, up to a maximum of 250 in total.

BITBUS is an industrial network optimised for the transfer of small messages (typically 10 to 250 bytes) at workshop or factory level. Since 1991 BITBUS has been adopted as international standard IEEE 1118.

4.2.4 DeviceNet

DeviceNet was developed by the Allen-Bradley Company in 1984, and is based on CAN technology, used with the RS485 specification for electrical signalling.

DeviceNet offers a maximum of 64 nodes on a network, over a distance 100 to 500 m, at signalling rates of 125, 250 and 500 kbps. DeviceNet is fundamentally a Master/Slave system, but for increased flexibility, various types of messaging are supported, and it also utilises a producer/consumer based model (this term is described later when considering the FIP Fieldbus). We will now describe these different messaging types.

Polling: The master node individually asks each device to send or receive an update of its status. This requires an outgoing message and incoming message for each node on the network. This is the most precise but least time efficient way to request information from devices.

Strobing: The master node broadcasts a request to all devices for a status update. Each device responds in turn, with node 1 answering first, then 2, 3, 4 etc. Node numbers are assigned to prioritise messages. Polling and Strobing are the most common messaging formats used in DeviceNet.

Cyclic: Nodes are configured to automatically send messages at scheduled intervals. This can be used in conjunction with Change of State messaging (see below) to indicate that a node is still functional.

Change of State: Nodes only send messages to the scanner when their status changes. This occupies an absolute minimum of time on the network, and a large network using Change of State messaging can often outperform a faster polling network. This is the most time efficient but least precise way to obtain information from devices because there is no longer any deterministic indication of when a particular node will next send data

Explicit Messaging: Commonly used on complex devices to download parameters that change from time to time but do not change as often as the process data itself. An explicit message provides a multipurpose communication path between two nodes and provides a means for performing two-way functions such as device configuration.

Fragmented Messaging: For longer messages that require more than the DeviceNet maximum of 8 bytes of data per node per scan, the data can be broken up into a number of 8 bytes segments and re-assembled at the other end. This requires multiple messages to send or receive one complete message.

UCMM (Unconnected Message Manager): DeviceNet UCMM nodes are capable of peer-to-peer communication. Unlike the standard Master/Slave configuration, each UCMM node can communicate with another directly, without having to go through a master first. This ability requires more resources within the nodes than simple Master/Slave messaging.

These multiple messaging formats, which can be mixed on a single DeviceNet network, enable the most efficient solution to be realised for a given for a given control application.

4.2.5 SDS (Smart Distributed System)

SDS was developed by the Honeywell Company, in 1989, and is also based on CAN technology, used with RS485 electrical signalling. The maximum number of nodes on a network segment is 64. SDS works over distances of 100 to 500 m at signalling rates of 125, 250, 500 and 1000 kbps.

SDS is another Master/Slave system, but is notable, compared to the other CAN-based solutions, in that it is event-orientated. Messaging is primarily by change of state and cyclic means - status changes on the network are reported only when they occur, with the cyclic messaging ensuring the integrity of the nodes. This drastically reduces traffic on the network compared to polling schemes. Successful message transmission is verified by the master, which sends a confirmation signal back to the slave node. Message prioritisation and the use of cyclic messaging serve to ensure that important data can be relied on to get through when needed, and a worst-case response time can still be guaranteed.

SDS is primarily intended for use in simple sensor bus applications, where the simplicity of the node hardware means that it can be made physically very small.

4.2.6 Interbus-S

The Interbus-S system was developed in the mid-1980s by the Phoenix Contact Company and several German technical institutions. The aim of the Interbus project was to simplify signal wiring in industrial applications. Interbus was first marketed in 1987 and subsequently made an open standard in 1990. It has been defined in European standard EN 50254.

Interbus is a serial bus system for transmitting data between different types of control systems and distributed input/output units. The serial transmission of data is carried out via a bus cable, which connects the controller board to the installed modules (slaves) in the system.

The physical layer used by Interbus depends on the distance between the particular nodes on the network. Remote nodes use RS-485 or fibre optical cabling, allowing long distances to be covered. More local nodes can use simpler CMOS signal levels. All Interbus communications take place at a rate of 500 kbps.

Interbus is a master - slave network that is designed as a data ring. The Interbus master (and there can be only one) is the central device for controlling the data ring. It exchanges data across the Fieldbus with the slave devices on the network.

The network has the structure of a distributed shift register. Every node in the network exchanges data with the master through internal data registers, which form part of the shift register that makes up the network. Although logically the network topology is that of a ring, the go and return lines of the ring are implemented within the one cable so that the network appears to have a star or tree structure.

4.2.7 FIP

FIP stands for 'Factory Instrumentation Protocol'. It utilises a bus topology, with shielded twisted pair cabling, at data rates of 31.25 kbps, 1 Mbps or 2.5 Mbps, or fibre optic cabling at 5 Mbps. There may be up to 64 nodes per bus cable segment (which may have a length of 1 Km or more, depending on the data rate, cable type and number of nodes), and up to 4 segments may be connected together through repeaters.

At the Data Link level, FIP utilises what is referred to as a 'Producer-Consumer Model'. Basically, this is a special form of Master - Slave system, as previously described. In FIP, the master is referred to as a 'Bus Arbiter' (BA).

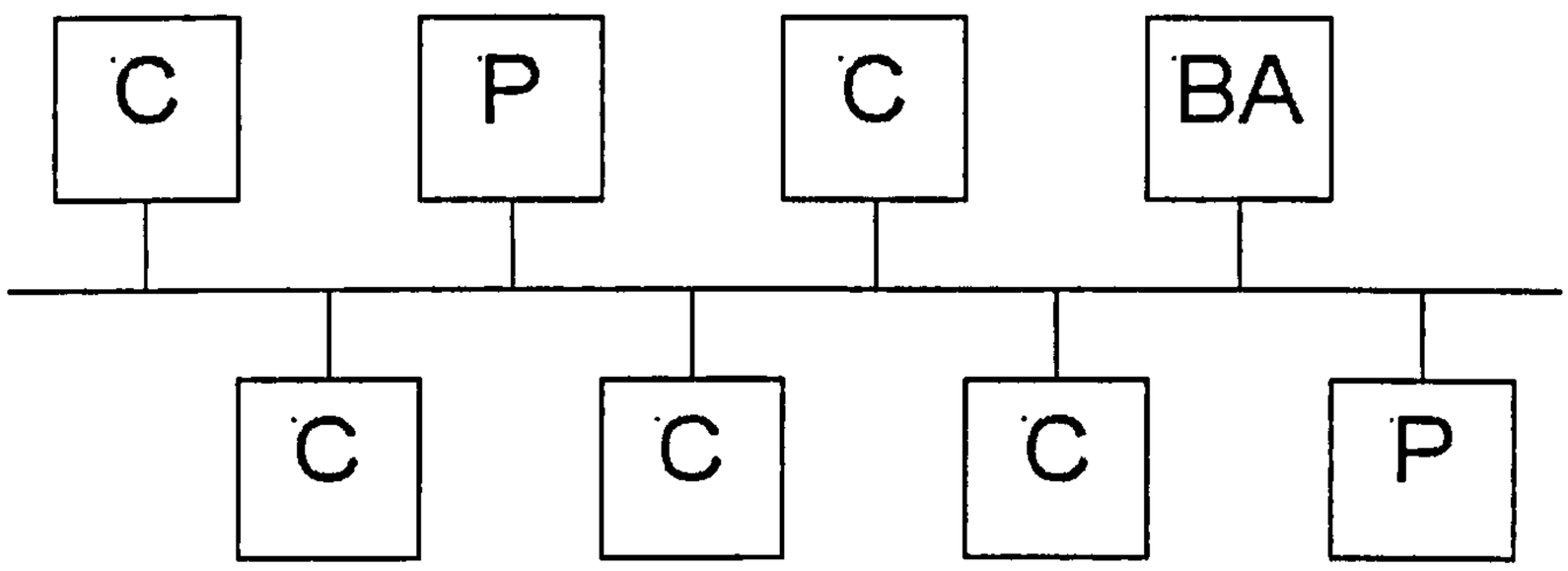


Figure 27: The FIP 'Producer/Consumer' Mechanism

The Bus Arbiter ('BA' in the above diagram) periodically requests certain parameters (or 'variables') over the network. The node responsible for the particular variable - the 'Producer' ('P' in the above diagram), then sends the value of the variable over the bus (this is similar to the system used with CAN). Any other nodes requiring this data - the 'Consumers' ('C' in the above diagram), simply read it from the bus at this time. Neither the Bus Arbiter nor the Producer node needs to know which nodes are consuming the data. The Bus Arbiter polls all the required variables within a defined time scale, ensuring determinism, and consequently, the 'Producer-Consumer' mechanism is very effective for time-critical data.

FIP is one of the Fieldbusses incorporated in standard EN 50170 (General Purpose Field Communication System).

4.2.8 P-Net

In 1983, the Swedish Process-Data Company developed P-Net as a standard for data communication in process control. P-Net [27] is based on an RS-423 physical layer, utilising shielded twisted-pair cabling. This allows a cable length of up to 1200 m without repeaters. Data is sent as an asynchronous transmission in 'Non-Return to Zero' (NRZ) code.

By way of explanation, NRZ coding is the simple technique whereby a logic '0' is represented by one signalling state, and logic '1' by another. By contrast, for example, in 'Non-Return to Zero Inverted' (NRZI) coding, a logic '0' might be represented by a *change* of signalling state, and a logic '1' by the signalling state remaining unchanged (the opposite coding situation could equally be applied). This is illustrated in the figure below.

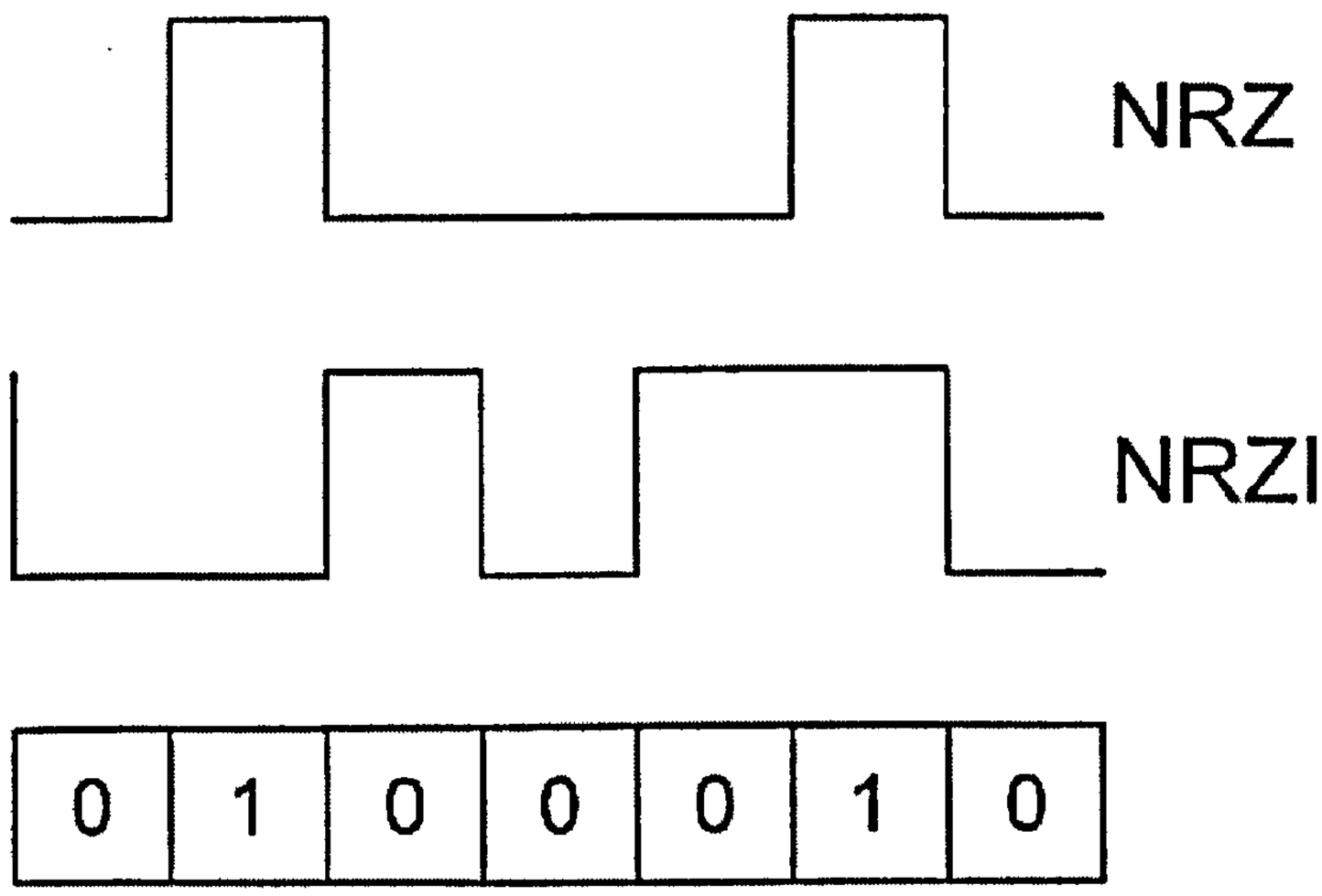


Figure 28: Example of NRZ and NRZI Coding

P-Net interfaces are electrically isolated, and up to 125 nodes can be connected to each cable segment. P-Net is a multi-master/slave system and utilises a protocol based on the reduced 3-layer OSI model already described.

Since P-Net is multi-master, an arbitration scheme is required, and P-Net uses a special form of token passing called 'virtual token passing'. This does not involve any actual message being sent over the bus, rather a time delay mechanism is used.

Each P-NET master is given a unique node address, between 1 and the number of masters expected within a system. Whenever the bus is idle, a counter in each master is incremented. After a delay, related to its node address has passed, a particular master is permitted to take control of the bus. It if does not need the bus it takes no action and the count increments until another master is enabled. As soon as any master uses the bus, the counters are reset and the sequence repeats. This arrangement also covers the instance of missing or non-contiguously numbered masters. The system can accommodate up to 32 masters on the bus in this fashion.

In July 1996, P-NET became part of the European Fieldbus Standard - EN 50170, and since December 1999, part of the new International Fieldbus Standard - IEC 61158.

4.2.9 Profibus

Profibus is a contraction of 'Process Field Bus' [28]. It is also based on an RS-423 physical layer, although in addition it can utilise fibre-optic and intrinsically safe (IS) links. The term 'Intrinsically Safe' refers to a technique employed in 'hazardous areas', areas where potentially explosive atmospheres may exist (examples of such areas might be refineries and similar plants, hence it is a concept very important in industrial automation). Put simply, IS techniques aim to limit the level of electrical energy present in equipment in the hazardous area, to a level too low to ignite an explosive atmosphere should a spark occur [29]. This is typically achieved by utilising special circuits to limit the electrical energy passed into the hazardous area, and to ensure (by their design) that equipment located in the hazardous area does not store excessive energy in operation.

The signalling rates in Profibus can vary between 9600 bps and 500 kbps.

Profibus is a broadcast bus protocol that operates as a multi-master/slave system. Its physical topology is that of a bus. Nodes are connected either directly to the bus cable, or can be connected via stub lines, but only at signalling rates below 1.5 Mbps.

It is possible to have up to 32 nodes per bus segment, or if repeaters are used, up to 127 nodes per segment. For flexibility in a control scenario, the system permits 'live' installation / removal of devices without affecting other nodes on the network.

There are three distinct versions of Profibus that have been tailored for different applications. The three versions of Profibus are:

- **Profibus DP** is optimised for speed and low cost. This version of Profibus is for communication between automation and control systems and distributed I/O at the device level and utilises an RS-485 or fibre optic physical layer.
- **Profibus PA** is designed for process automation. It can easily used in intrinsically safe areas because both communication and power is supplied over the same 2 wires.
- **Profibus FMS** is a general-purpose version for all applications. It uses an RS-485 or fibre optic physical layer and allows multi-master communication.

All three versions of Profibus share a common underlying bus access protocol. As we have already stated, the Profibus is a Master - Slave system, with a Multiple master option. Single master operation is conventional in form, but in multiple master mode it is necessary to arbitrate which master has access to the bus. This is achieved by additionally incorporating a token passing protocol between the masters.

Profibus is also one of the Fieldbusses incorporated in standard EN 50170 (General Purpose Field Communication System).

4.2.10 Foundation Fieldbus

The Foundation Fieldbus was developed by an organisation called the Fieldbus Foundation. The Fieldbus Foundation was formed by a group of automation companies with the goal of completing the development of a single, open, international and interoperable Fieldbus standard. It was based on the work of the International Electrotechnical Commission (IEC) and the Instrumentation Society of America (ISA) (now called the International Society for Measurement and Control).

Foundation Fieldbus is a broadcast system, like Ethernet, where each node must be able to 'hear' the messages broadcast by any other node on the network. The bus cable consists of only two wires, which serve the dual purpose of supplying power to all nodes as well as transmitting the data over the network. The physical topology, as for other Fieldbusses already described, is a bus structure with the option of spur lines.

The maximum number of devices on the network is determined by factors such as the power consumption of individual nodes and the length of the trunk line. The length of the trunk line can be extended using bus repeaters.

The maximum number of devices is 240 per link with the number of devices per spur line depending on the length of the spur line.

As already mentioned the FF cable carries DC power as well as the signal. The signal is in the form of a Manchester Bi-phase waveform, at a level of +/- 10 mA into a 50-Ohm load, creating a 1 V peak-to-peak signal on top of the DC supply voltage line. The bit rate is 31.25 Kbps and the DC supply voltage can be in the range 9 V DC to 32 V DC.

Foundation Fieldbus has a sophisticated set of data-link access controls. There is a centralised scheduler on the network called the Link Active Scheduler (LAS). This operates a 'Producer-Consumer Model' as already described, requesting nodes to return data at predetermined times. This data is then available to any other nodes that require it. This permits the network to behave in a deterministic manner with respect to time critical data.

Additionally, during any free time slots when no deterministic data transfer is scheduled, the LAS operates a token passing scheme, giving other nodes an opportunity to pass other (non time-critical) data.

The LAS function is carried out by a device known as a Link Master Device. There may be more than one of these on the bus, and it is therefore feasible for the bus to operate in a multi-master mode.

The Fieldbus solutions that we have described are not the only ones in existence - there are many more, some proprietary, some open. Whilst there are certain similarities between particular systems, for example, they may share a physical layer, they are nevertheless essentially incompatible. In the next section, we will discuss the moves underway to achieve interoperability within Fieldbus technologies.

4.3 The Move Towards Fieldbus Interoperability

With the proliferation of different Fieldbus technologies that began to develop during the 1980's, it became a goal of the International Standards Organisations to steer users towards a simplified framework of a standard Fieldbus solution.

As has already been mentioned, many Fieldbus solutions became National Standards in their own right. This in itself was an impetus for National Standards bodies involved to push for that particular standard to be included in any proposed International Standard.

Manufacturers with proprietary Fieldbus solutions would also tend to press for their technology to be adopted as a part of the proposed standard. Likewise, existing users of these technologies were less willing to change.

Because of these factors, the standards that have evolved have tended to be very much a compromise, and in fact incorporate elements of existing commercial technologies. There are two main Fieldbus standards that we must look at, EN 50170 and IEC 61158.

4.3.1 EN 50170 and IEC 61158

European standard EN 50170 ('General Purpose Field Communication System'), first published in 1996, is really only a formalisation of three existing, and non-interoperable Fieldbus specifications - Profibus (the DP and FMS variants), P-NET and WorldFIP.

However, supporters of EN 50170, who wish it to be accepted world-wide, state that this is justified because these technologies are proven and well established, whilst opponents suggest that they are all out of date! It is proposed that other technologies may be added to EN 50170 in future, for example, Foundation Fieldbus and Profibus PA.

As early as in 1985 the IEC (International Electrotechnical Committee), in association with the ISA (Instrumentation Society of America) started its efforts to develop one uniform international standard for Fieldbusses. This standard came to be designated as IEC 61158 (Fieldbus Standard for use in Industrial Control Systems).

The standard consists of eight parts, covering the definition of all aspects of the proposed new Fieldbus. The standard contains 'profiles' that permit the Fieldbus to be tailored for particular application areas.

The supporters of IEC Fieldbus cite its flexibility and sophistication, whilst opponents claim that it is overcomplicated and unproven.

It can be seen that despite the best efforts of the standardisation bodies, there is still some way to go before there is any semblance of a 'universal' Fieldbus.

That concludes our discussion of modern Fieldbus technologies. It can be seen that these tend to utilise discrete signalling media, most frequently twisted pair. Using the power line as a medium does not yet feature significantly in the Industrial scenario, although it is more common in home and building automation systems.

It is the belief of the author that PLC techniques can offer a useful additional facet to Fieldbus and local control networks, where the application suits the limitations of PLC technology.

We will go on to discuss these potential applications in a later section. Next, though we will begin to look at the power line itself, and its suitability (or otherwise) for data transmission.

Chapter 5 : The Power Line as a Transmission Medium

Transmission lines, as encountered in normal communication systems, have well defined, uniform, electrical characteristics. For example, we have already discussed twisted pair and co-axial cabling when discussing networking systems. The purpose of such transmission lines is essentially to permit the passage of the high frequency signals without undue attenuation or distortion. Transmission line theory dictates that, for this to occur, the transmission line must present a unified characteristic impedance to the signals being transmitted. The physical construction of the cabling is a major factor in providing this.

The power line, on the other hand, is *quite* different. It is optimised for the transmission of high energy 50 Hz or 60 Hz mains power. At such low frequencies, the nature of the mains cabling will have no significant effect on the propagation of the mains energy, so consequently, mains wiring within a building or plant can be extremely complex and undisciplined in structure. Its topology might consist of a complex mass of rings, stars, busses, or spurs, with no thought for correct termination for high frequency signals.

Any other type of transmission over the power network is inevitably going to be a serious compromise. Furthermore, since the power line is shared in this fashion, by-products of its primary function, in the shape of noise and other effects are inevitably present. Other transmissions sharing the medium will pick up such noise as a side effect.

Many studies have been carried out to attempt to quantify the characteristics of the MV and LV power distribution network from the point of view of PLC applications, the following references being an example: [30, 31, 32, 33, 34, 35, 36, 37].

If it is possible to sum up these findings in a few words, it is to state that the power line represents a highly variable and unpredictable medium for the transmission of data. Impedance's at our communications carrier frequencies are both variable and of a low order - often below 10 ohms, there are other phenomena which may further alter the impedance or cause spurious resonance effects, and also many varied noise sources.

In the next section, we will look at the commonest of these, beginning with external sources of signal degradation.

5.1 Sources of Signal Degradation Encountered on the Power Line:

5.1.1 Shunt Capacitance

This is commonly encountered as a means of 'Power Factor Correction' (PFC). The term 'Power Factor' recognises that in the real world, few electrical loads are purely resistive in nature, and in fact most have a notable inductive component (e.g. motors, relays or solenoids). This means that the electrical energy is not being utilised at maximum efficiency, due to the differing phases of the V/I waveforms feeding into the load. A power factor of '1' represents a purely resistive load, and a PF of '0', a purely inductive or reactive load.

This inductive component can be nullified by the judicious use of capacitance placed, in the case of shunt connection, across the power line.

Unfortunately, these capacitors will tend to also shunt our PLC signals and in addition can introduce resonance effects, in combination with the impedance of the transmission line, further inhibiting our signals.

5.1.2 Series Capacitance

This is a technique also encountered as a means of correcting power factor. As the name suggests, the correcting capacitance is introduced in series with the power line. Unlike shunt capacitance, this will have little attenuation effect on the PLC signal, although there is still a risk of resonance effects. It is a less common technique on LV distribution networks.

5.1.3 Lightning and Transient Arrestors

These typically consist of an air gap and/or a non-linear resistance (varistor), intended to absorb lightning surges by virtue of the air gap sparking or the varistor starting to conduct when excessive voltages are present on the power line. Any effects on PLC systems are likely to occur as a result of any capacitance of the air gap or the varistor device, which may be a significant factor at the frequencies of our PLC signals.

5.2 Typical Types of Load Encountered on the Power Line:

Having dealt with the characteristics of the power line itself, and some associated ancillary devices, we will now consider the various types of load that will be connected to it and which also affect power line signal propagation.

5.2.1 Resistive Loads

Simple loads such as heating elements fall into this class, and in principle, it is relatively easy to calculate their effect on PLC. It must be remembered that there may be some associated L & C effects to be taken into consideration as well.

5.2.2 Capacitive Loads

Many loads exhibit a capacitive effect, due to their internal wiring capacitance or the use of suppression capacitors across the power lines. These will have a shunting effect on PLC signals and may, in addition, induce resonance's (see below). Equipment utilising switched mode power supplies, which simply rectify the incoming mains voltage, also effectively present a shunt capacitance to PLC signals, as well as introducing impedance modulation effects (discussed below).

5.2.3 Resonant Loads

As mentioned above, the interaction between capacitive loads and cable inductance can cause resonance's that may prejudice PLC transmissions by shunting or blocking the wanted signal. Such effects are inevitably unpredictable due to the nature of the power line itself.

5.2.4 Impedance Modulating Loads

'Impedance modulation' effects can occur in equipment such as that incorporating switch-mode power supplies, where large values of capacitance are effectively placed across the mains supply via rectifiers. These capacitors are effectively only in-circuit for that part of the mains cycle whilst they are being charged (i.e. whilst the mains voltage exceeds the current voltage across the capacitor). This 'topping up' effect results in periodic changes in the effective impedance presented to the power line by the equipment.

Next, we will move on to consider some of the types of noise which will be encountered on the power line.

5.3 Sources of Noise Encountered on the Power Line:

5.3.1 Background Noise

This is typically a low-level noise originating from a range of sources, possibly external to the power line itself, and impinging onto it by such means as inductive pick-up.

5.3.2 White (Smooth Spectrum) noise

This is broad band noise caused by such devices as non-synchronous, brushed, electric motors. It is typified by the fact that it covers a wide bandwidth with no significant dominant frequencies.

5.3.3 Synchronous noise

This is noise generated at multiples of the mains supply frequency (50 or 60 Hz) typically caused by devices that operate in synchronisation with the mains cycle, such as Thyristor (SCR) dimmers.

5.3.4 Non-Synchronous noise

This type of noise is periodic, but not based on the mains frequency. Examples include television sets or switching power supply circuits.

5.3.5 Impulse noise

This is non-periodic, irregular pulses or spikes, often of high amplitude, caused by such functions as remote lightning strikes, the switching of heavy loads, capacitor banks etc.

Having now mentioned sources of noise on the power line, we will go on to discuss the standards that govern the subject area of electromagnetic interference.

5.4 EMC Standards

A major part of the research contained within this thesis concerns the performance of PL communications links under the influence of external noise and interference. As has already been noted, the power line is extremely unpredictable with regard to such factors. It would be useful, therefore, to have some defined benchmarks when considering the operation of PLC links under such conditions.

Luckily, such benchmarks do exist, in the form of international standards covering the area of Electromagnetic Compatibility (EMC).

The definition of the term EMC (Electromagnetic Compatibility) refers to the performance of an item of equipment within the realm of electromagnetic energy, both in the context of that items' immunity from, and emissions of, such energies [38]. As such there are two fundamental classes of EMC standard - 'Emission' standards, and 'Immunity' standards. In this research, we are interested in the immunity standards as they apply to the effects of such interference on the performance of our power line communications system.

It must be noted, however, that by their very principle of operation, PLC systems can be classed as 'Emission' sources under the terms of the EMC standards. Consequently, it may be necessary to limit the level of their carrier signals.

Before looking at the specific EMC standards, we will consider the structure of the various international standards organisations.

5.4.1 The IEC, ISO, CENELEC and EMC Standards

Work on the many international standards in existence is carried out by the various standards organisations and their internal 'Technical Committees' (TCs). The IEC is the 'International Electrotechnical Commission', which works in co-operation with the ISO ('International Standards Organisation') to promote international standardisation.

Within the IEC there are two technical committees primarily working on EMC matters, and many more with some involvement. Technical Committee 77 (TC77) 'Electromagnetic compatibility between equipment including networks' is primarily responsible for IEC 1000 'Electromagnetic Compatibility' family of standards.

These IEC standards have no legal standing, but are the basis of national or European standards, which we will discuss in a later section. The other technical committee is CISPR, a French acronym for the 'International Special Committee on Radio Interference', who generate their own publications dealing with limits and measurement of radio interference characteristics. The body in charge of overall co-ordination of EMC activities at the IEC is the Advisory Committee on EMC (ACEC).

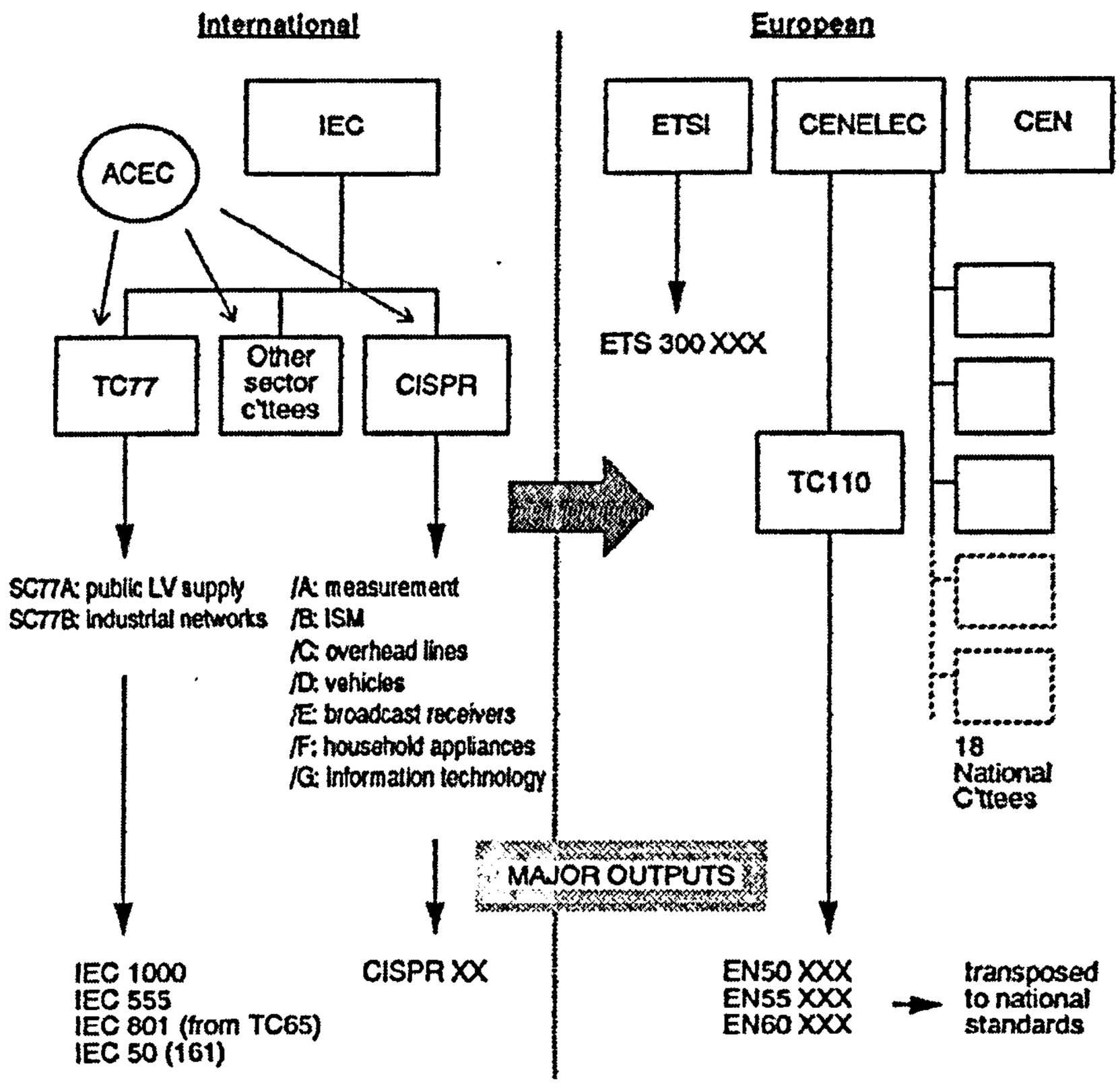


Figure 29: EMC Standards Committee Structure

At a European level CENELEC, another French acronym standing for the 'European Committee for Electrotechnical Standardisation' is responsible for generating European standards.

It is primarily the generic European standards that we will be using within this research, and we will introduce them next.

5.4.2 Emissions Standards

The original purpose of the EMC emission standards was to ensure that equipment did not cause problems to other equipment by virtue of the extent of emitted interference from the equipment. Obviously, there are several mechanisms by which such interference may be propagated:

- As electromagnetic (radio) radiation.
- As conducted interference, over power or data lines.

The primary EMC emissions standards are EN 50081, Part 1 [39], and EN 50081, Part 2 [40]. Part 1 of the standard provides the requirements for emission of electromagnetic disturbances from electrical and electronic apparatus intended for use in the residential, commercial and light industrial environments and for which no dedicated product or product-family emission standards exist. Part 2 is similar in scope, but covers the industrial environment.

5.4.3 Immunity Standards

The original purpose of the EMC immunity standards was to define the limits to which equipment would remain unaffected by interference from external sources of EM energy. These sources can be categorised as follows:

- Electromagnetic (radio) radiation.
- Conducted interference, over power or data lines.
- Electrostatic discharge (ESD) into the equipment.

The primary EMC immunity standards are EN 50082, Part 1 [41], and EN 50082, Part 2 [42]. The scope of the EN 50082 standards is similar to that for 50081, but concerning an immunity scenario.

As already noted, these are not the only standards in existence, there are others that cover specific types or families of equipment, and the already mentioned, extensive, IEC 1000 family of standards.

Having discussed the EMC standards for emission and immunity, within the context of conducted interference, a common technique for minimising the effects of this is to utilise a filter in the power line. Since these also have implications for PLC, we will discuss their use in the next section.

5.5 The Use of Filters in PLC Applications

Although the previous sections tend to paint the power line in a most unfavourable light as a communications medium, steps can be taken to improve matters. Perhaps the most important of these involves the use of filters.

In the context of electronic systems, the purpose of filters can simply be defined as to select, pass, or block certain frequencies or frequency bands.

From an EMC viewpoint, we need to pass the 50 / 60 Hz mains power, whilst attenuating the effects of higher frequency noise signals, hence a low pass filter arrangement is commonly used, similar to that shown below.

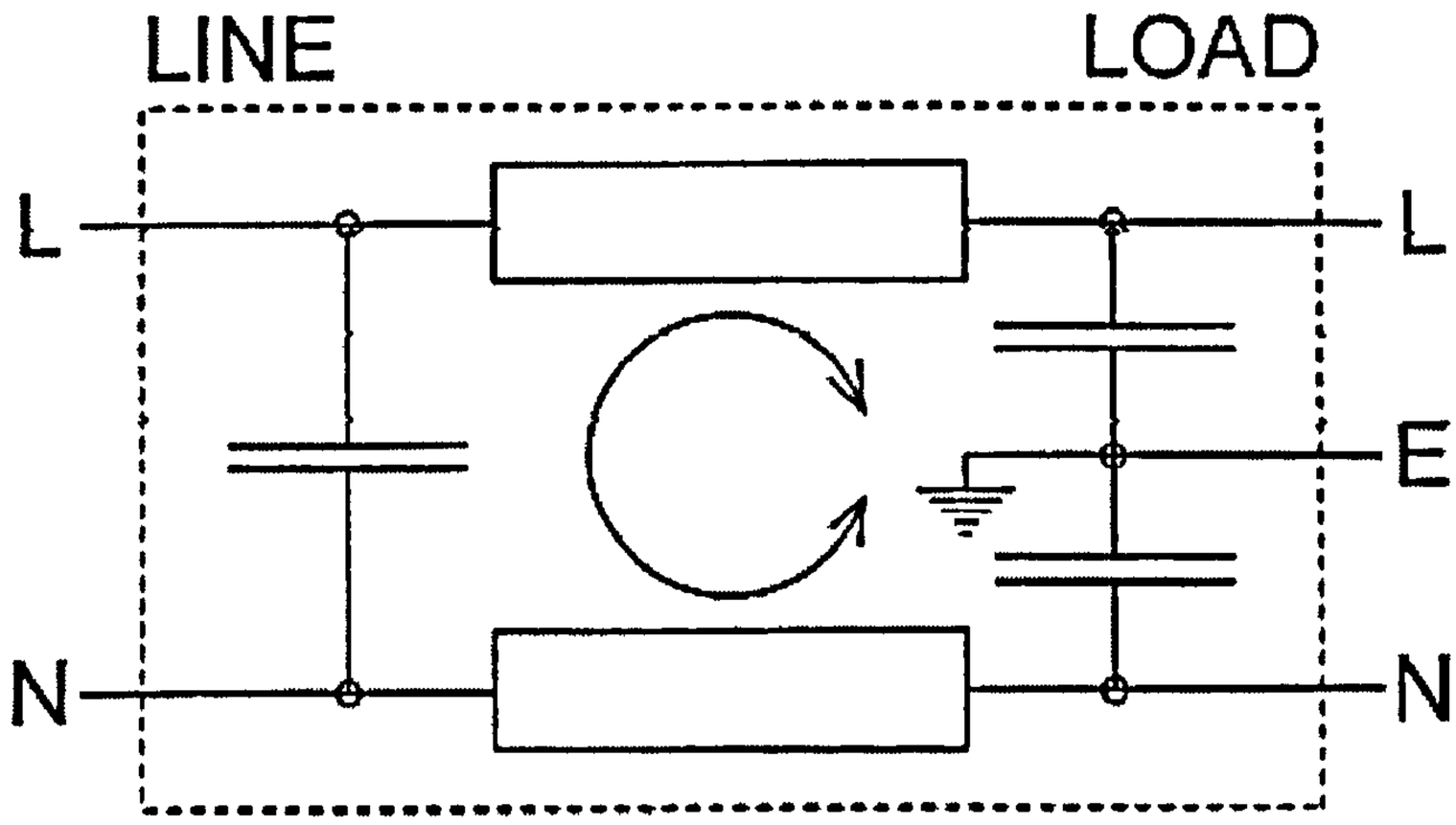


Figure 30: Typical Power Line EMC Filter

It can be seen that the combination of series inductance and shunt capacitance essentially forms a low pass filter intended to attenuate power line noise, both common mode (between Live-Neutral, and Earth), and differential (between Live and Neutral). It is not, however, ideal from the PLC point of view, as the capacitance across the Live and Neutral terminals will (as has been already described) tend to attenuate PLC signals.

A similar arrangement, in 'reverse' order, can be utilised to prevent 'noisy' items of equipment from passing generated noise onto the power line, but again there are penalties from the PLC viewpoint due to the presence of the shunt capacitance.

Modern equipment and appliances will already have appropriate filtering and suppression built in to meet the requirements of the various EMC standards. For our purposes though, such filters would also have to be carefully designed so as not to inhibit the PLC signals. The use of such a filter will give a further advantage from the PLC viewpoint, as it will tend to mask the impedance of the load to which it is connected. This is because the series inductance's in the circuit will present a high impedance at the frequencies of our PLC signals.

However, since, in a real world application we cannot guarantee that all loads would have appropriate filters, we must consider in our experimentation the 'worst case' scenario, with a noisy and low impedance power line.

Another important use for filters in PLC systems is for isolating a PLC system within a particular building, part of a building, or item of plant. This will prevent PLC signals from passing to an area for which they are not intended, and vice-versa.

These ideas are among those embodied in the 'Power Bus' concept that the author has outlined in an existing paper [7]. They will be discussed in more detail in a later chapter.

The need for filters in practical PLC systems has already been recognised by the standards bodies and has resulted in draft standard prEN 50065-4-1 [43]. They define the use of PLC filters (called 'de-coupling' filters) as follows:

- To limit the transmission area of wanted signals to the area in which the mains communications system operates.
- To reduce unwanted signals from the other side of the mains port.
- To allow simultaneous communication on both sides of the filter.
- To set a suitable impedance to the mains power ports at the signalling frequency.
- To provide a return path for the (PLC) signal when needed.

It can be seen that the above points address the issues previously raised in this section concerning the desirability of utilising filters in PLC applications.

That concludes our discussion of the power line as a transmission medium. In our experimental work, described in a later chapter, we will be subjecting PLC modems to conducted interference sources, at the levels laid down in the immunity standards already mentioned, and evaluating their performance under these conditions.

In the next chapter, we will start considering the techniques available for practical power line communication. We will begin by discussing the various modulation schemes that may be applied.

Chapter 6 : Power Line Communication Techniques

6.1 Modulation Techniques for PLC:

In the field of PLC, we are concerned with the concept of transmitting digital information over the power line medium. We have already described base band techniques such as Cyclocontrol and TWACS, but in this research, we are primarily interested in modulated carrier schemes. These permit PLC operation within defined frequency bands, as outlined by CENELEC in standard EN 50065, which will be described in a later section.

There are many means of digitally modulating a carrier frequency, and we will describe the common ones in the following sections. We will concern ourselves only with techniques applicable to PLC, and will disregard other transmission systems that may be encountered in other communications areas (e.g. radio), unless relevant.

6.1.1 Amplitude Shift Keying (ASK)

In ASK, a change of signalling state is represented by a change of amplitude in the carrier frequency. Signalling state may be represented by two (or more) different amplitudes of the carrier (although the greater the number of states, the poorer the noise performance, since it becomes less easy to discriminate between the various amplitudes).

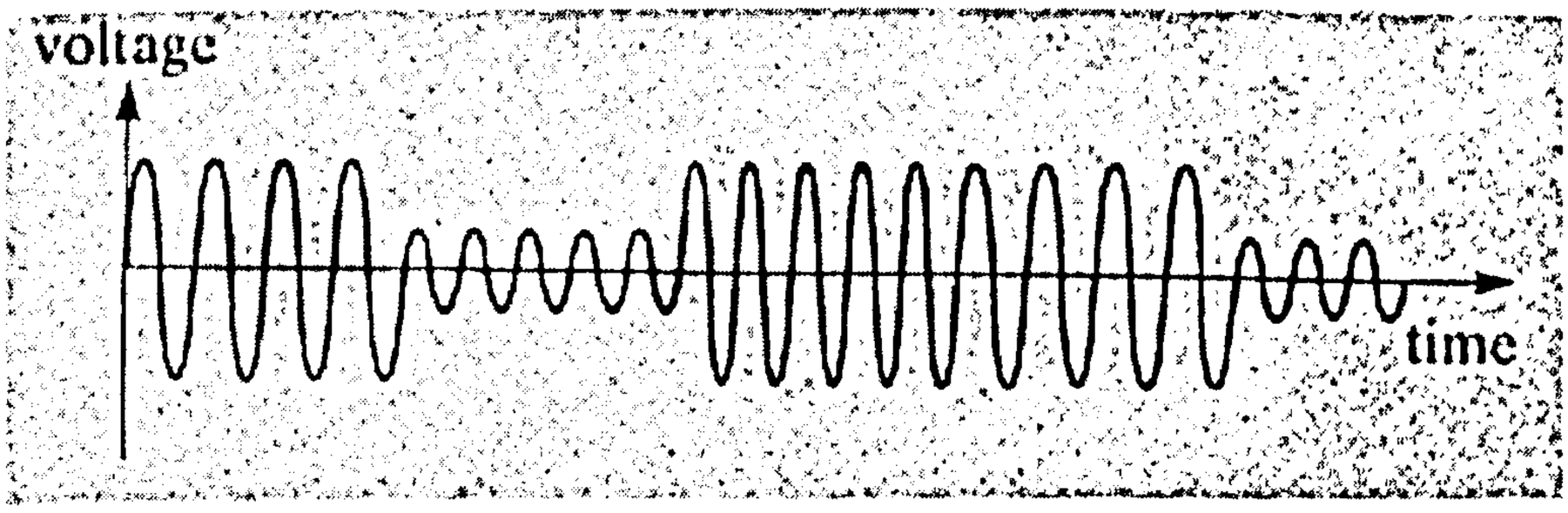


Figure 31: Amplitude Shift Keying (ASK) Waveform

Two states is the more usual arrangement (called Binary-ASK), with one state often being no carrier at all, referred to as On-Off-Keying (OOK).

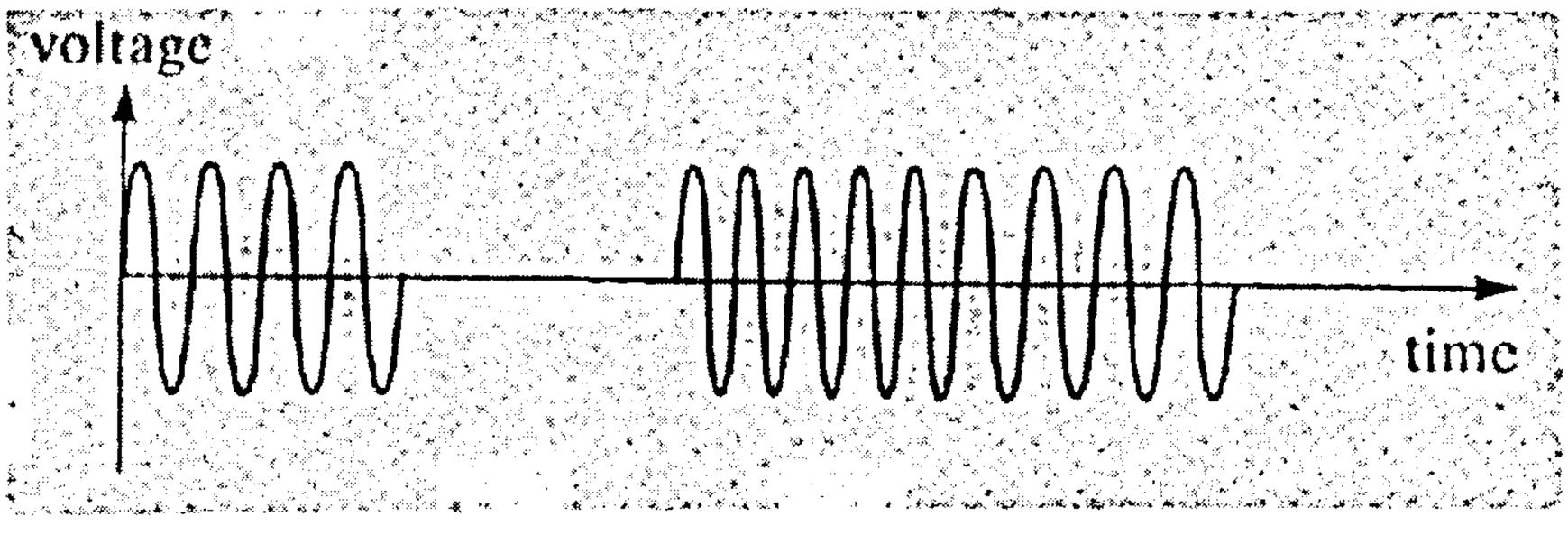


Figure 32: On-Off Keying (OOK) Waveform

The X-10 system already described utilises an OOK technique, based around a carrier frequency of 120 kHz. The Philips TDA5051 power line modem device [44] is an integrated power-line modem which provides OOK facilities. It can be tuned to operate over a range of frequencies, but would be most appropriate for use in at a 132.5 kHz centre frequency, in conformance with EN 50065 requirements.

6.1.2 Frequency Shift Keying (FSK)

In FSK, a change of signalling state is represented by a frequency shift in the carrier frequency. This is illustrated in the diagram below. Notice the irregularities that occur as the frequencies change. These are undesirable in a real works FSK application, as they will result in out of band frequency components being generated.

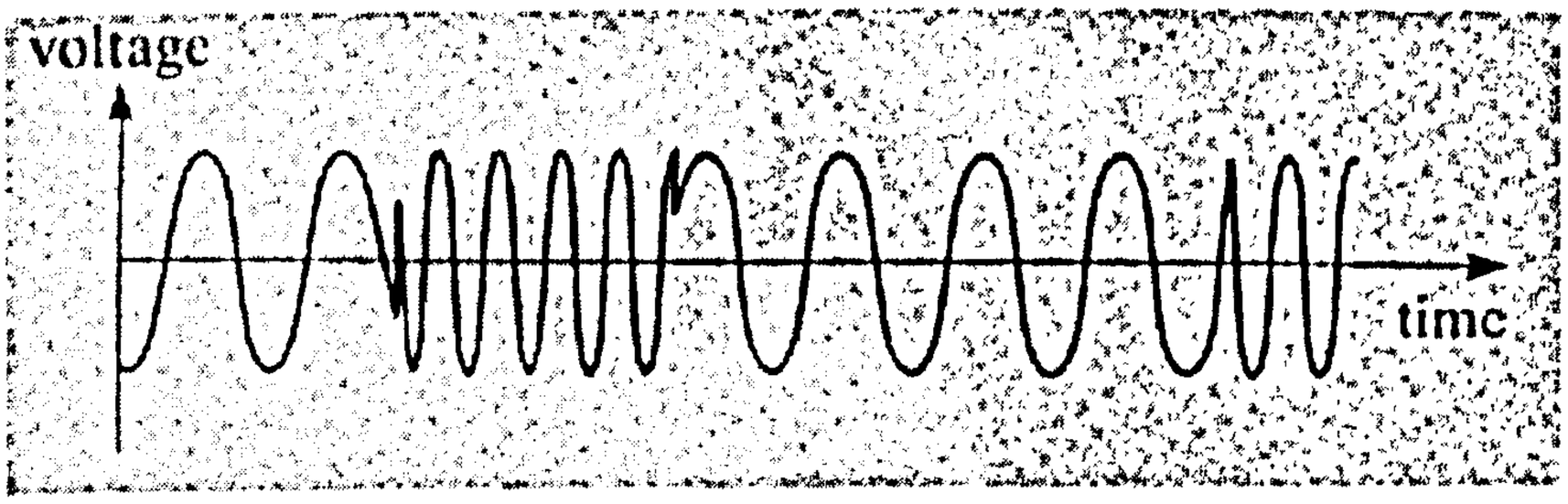


Figure 33: Frequency Shift Keying (FSK) Waveform

It is preferable for the transition from one frequency to another to be smooth, and this is referred to as continuous phase FSK. This lack of sharp edges in the waveform results in a lower bandwidth requirement. This is illustrated in the diagram below.

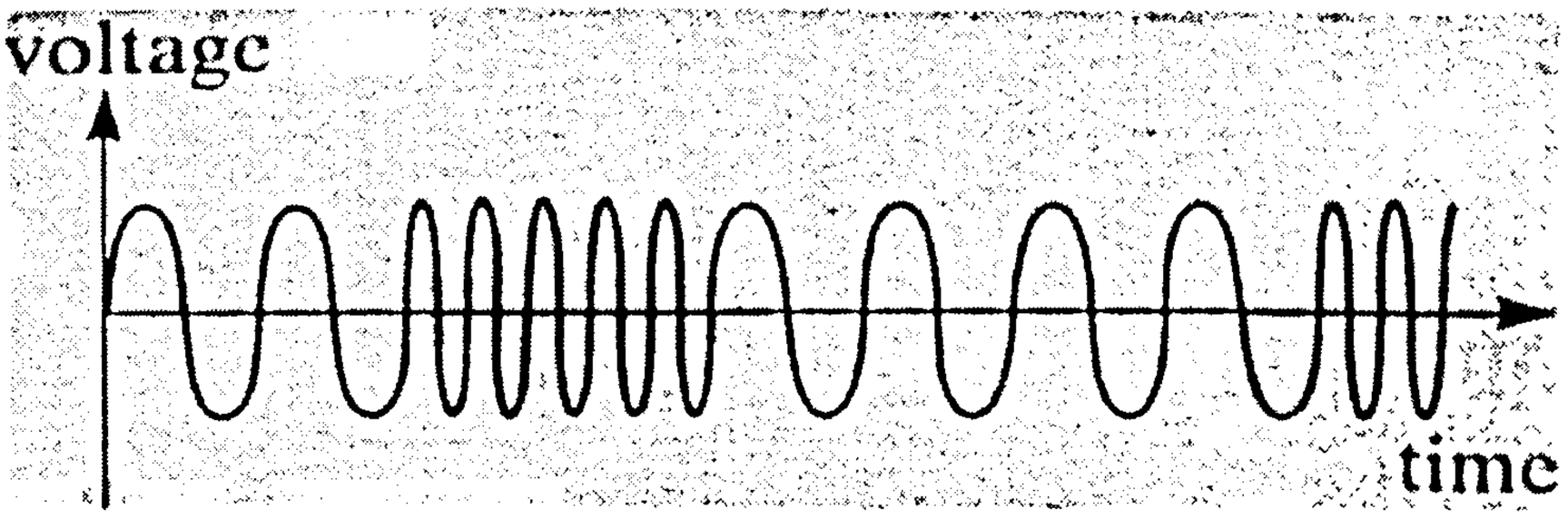


Figure 34: Continuous Phase FSK (CPFSK) Waveform

The frequency shifts involved in FSK may be quite large, called 'Spread FSK' (SFSK), which can have advantages when noise obliterates one or other frequency, since the other may still be detectable as a simple ASK signal. However, in practice, bandwidth limitations may not permit this technique to be employed.

More usually, the frequency shift is relatively small. For compliance with the EN 50065 access protocol (to be described later), this shift should be centred around 132.5 kHz. An example of this technique is the Thomson ST7537HS1 device [16]. The device utilises two signalling frequencies of 133.05 kHz and 131.85 kHz (in fact, not quite symmetrical about 132.5 kHz, but close enough!). This device is specifically intended for compliance with the 'European Home System' (EHS) initiative, which has already been discussed.

6.1.3 Phase Shift Keying (PSK)

In PSK, a change of signalling state is represented by a phase shift in the carrier frequency. For digital systems, this shift is usually a discrete jump of a fixed phase angle. The following diagram shows a phase shift of 180 degrees between states, giving a total of two possible signalling states.

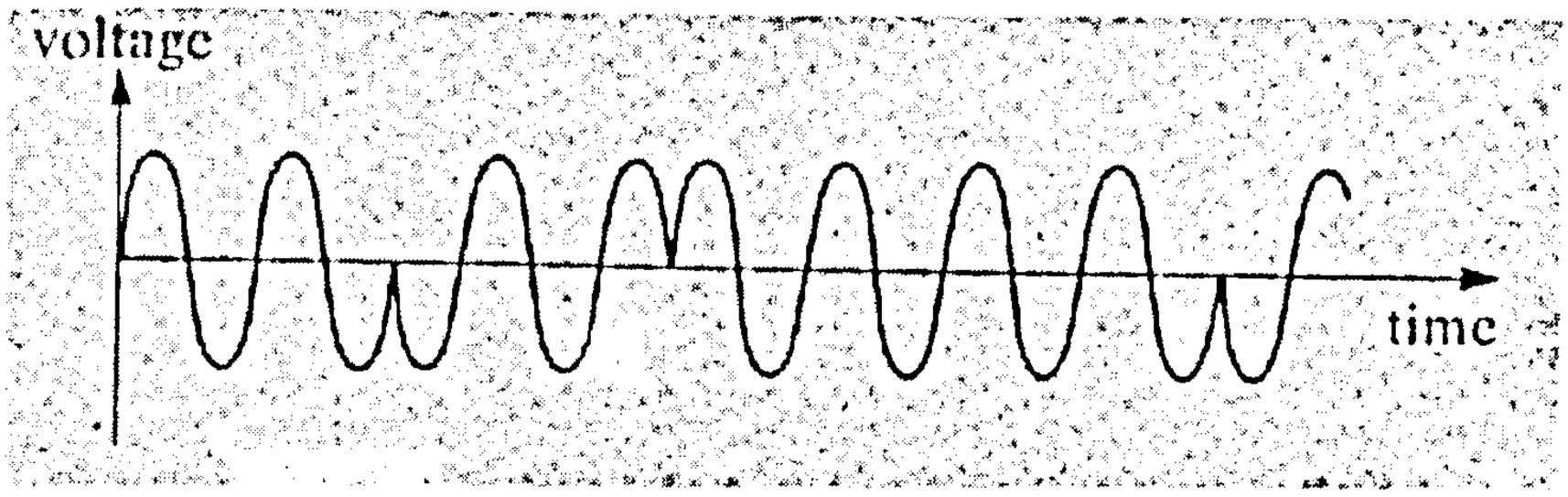


Figure 35: Digital Phase Shift Keying (DPSK) Waveform

Other values of phase shift are possible. For example, four discrete phase shift values (called quadrature PSK, or QPSK) offers the possibility of increased data rates, since each signalling state can represent two binary digits. Further increases in the number of signalling states, and therefore data rate, can be achieved by combining PSK with other techniques such as ASK, but with the increased disadvantage of increased receiver complexity and reduced immunity to noise sources.

An EN 50065 compliant example of PSK techniques is the Echelon LonWorks PLT-22 'C' band power line modem [45].

6.1.4 Spread Spectrum (SS)

Very much a current technique, spread spectrum can be simply defined, as the act of deliberately causing a communications signal to occupy greater bandwidth than simple signalling theory states is required. The reasons for doing this are generally either for data security, or to overcome noise problems on the communications channel. It is the latter which is most applicable to PLC applications because, by spreading the bandwidth, the carrier is less likely to be affected by noise occupying only parts of the available bandwidth. A disadvantage, however, where compliance with EN 50065 is required, is that the available bandwidth is not usually high enough to support SS. This is particularly true for 'consumer' use within the relatively narrow CENELEC 'C' band which we will be using (we will discuss these bands in a subsequent section).

There are actually several modulation techniques that produce a spread spectrum signal. We will introduce the commonest ones here.

6.1.5 Direct Sequence Spread Spectrum (DS-SS)

This is probably the most sophisticated spread spectrum technique. In Direct Sequence, the wanted data stream is modulated (by phase modulation) with a pseudo-random bit-stream, at a significantly higher bit-rate, to cause the spread in the bandwidth. A carrier signal is then modulated with this combined bit stream to give the final spread spectrum signal.

Demodulation involves correlating the incoming bit stream with the original pseudo-random spreading signal, re-generated at the receiving end in synchronisation with that at the transmitter. DS is a technique often used for secure radio links as the signal (when monitored with a normal radio receiver) typically does not rise above the background noise floor. In any case, without knowledge of the exact de-spreading bit stream, decoding the signal is almost impossible.

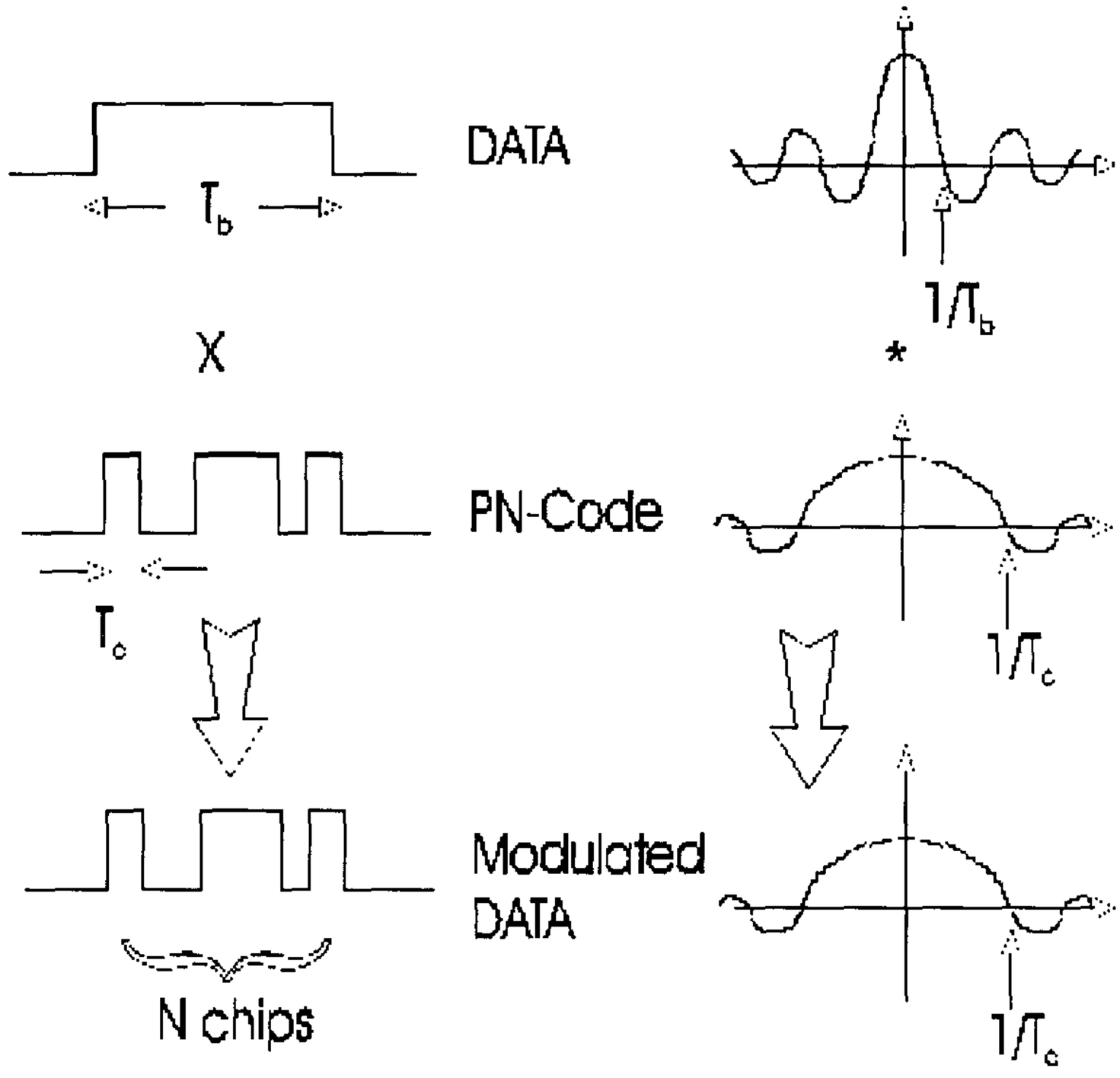


Figure 36: Example of Spreading in DS-SS

The above diagram illustrates the basic principle of direct sequence spread spectrum. The original data signal, shown at the top left of the diagram, has a relatively narrow spectral characteristic, shown top right. The pseudo-noise (PN) spreading signal, shown at the mid-left of the diagram, has a higher bit rate, and a correspondingly wider spectral characteristic (mid-right). When the two signals are combined, by a simple phase modulation, (bottom left), the resultant signal retains the wide bandwidth of the spreading signal (bottom right).

Direct sequence spread spectrum is not generally used in PLC applications but, as has previously been mentioned, is frequently chosen for tasks such as wireless networking. We will next look at another SS technique, variations of which are utilised in both radio and PLC applications.

6.1.6 Frequency Hopping Spread Spectrum (FH-SS)

Another SS technique is 'Frequency Hopping'. Here the carrier frequency (or frequencies) deliberately change, either at set time intervals, or in response to other conditions.

Frequency changes in the time domain, may occur in a controlled, pseudo-random, fashion in order to provide security from interception. Alternatively, the frequencies may change in response to conditions on the transmission medium (i.e. power line noise within a certain frequency band causes the carrier to change to a frequency outside of that band).

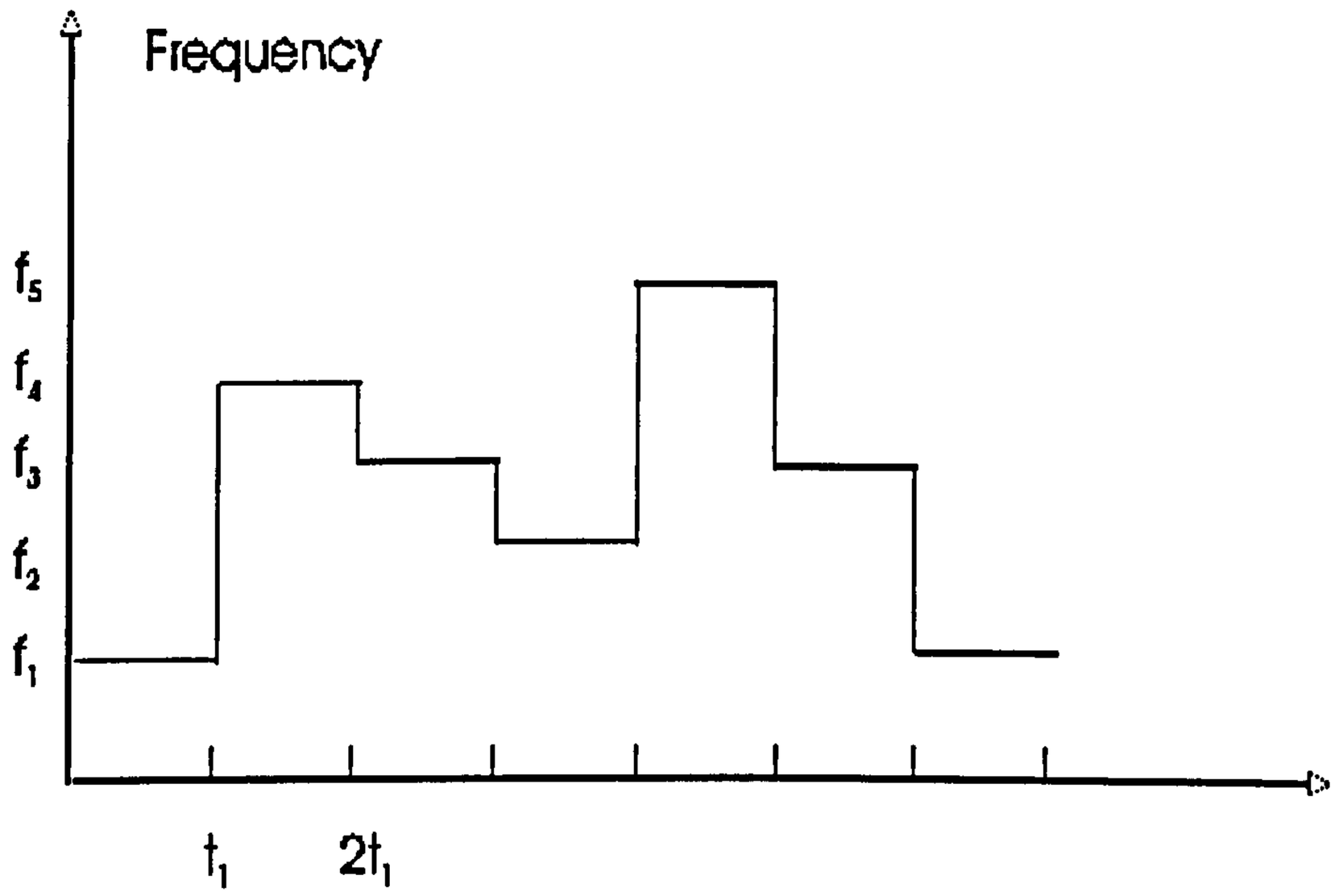


Figure 37: Example of Time Domain FII-SS

The above diagram shows a simple example of a time domain based frequency hopping spread spectrum system. It can be seen that for the initial time interval $\mathbf{t_1}$, the system uses carrier frequency $\mathbf{f_1}$. Between $\mathbf{t_1}$ and $\mathbf{2t_1}$, the carrier frequency changes to $\mathbf{f_4}$, and then, at subsequent intervals of $\mathbf{t_1}$, to $\mathbf{f_3}$, then $\mathbf{f_2}$ and so on. The sequence of frequency changes will follow a defined sequence and as long as the receiver knows that sequence it will be able to track the transmitted signal.

FH-SS is used in the Cyplex IC/SS PLC system [46, 47]. This system may be viewed as a frequency-hopping spread-FSK system, with a choice of frequency pairs falling within the CENELEC 'A' band of 9 kHz to 95 kHz, for use by the utility companies.

Four frequency pairs are available (called 'tunes'). These are 76.190 kHz and 61.905 kHz, 66.667 kHz and 52.381 kHz, 42.857 kHz and 23.810 kHz, and finally 33.333 kHz and 14.286 kHz. As can be seen, the various combinations occupy a wide part of the available bandwidth.

A complex control scheme is employed within the IC/SS chip set to govern the use of these tunes. The controller continuously monitors the power line and if conditions are found to be degenerating using a particular tune, then the master node (IC/SS is a master-slave system) initiates a change to another 'tune'.

This technique is not suited to some of the lower bandwidth sections of the frequency spectrum and is not appropriate to our work in the CENELEC 'C' band.

6.1.7 'Chirp' Spread Spectrum

Lastly, we will consider the 'Chirp' technique for spread spectrum. Here, the signalling state is represented by a carrier frequency, which sweeps over a particular frequency range for each bit transmitted. The idea is that noise occupying a small part of the chirp bandwidth should not defeat the reception of the rest of the chirp. This technique is most commonly found in PLC applications, but can also be applied to radio, and the sweep pattern may be quite complicated. Again, the relatively high bandwidths required make chirp less favourable to EN 50065 compliant solutions.

An example of a 'chirp' SS device for PLC applications is manufactured by the Intellon Corporation [13]. The waveform employed is shown in the next figure:

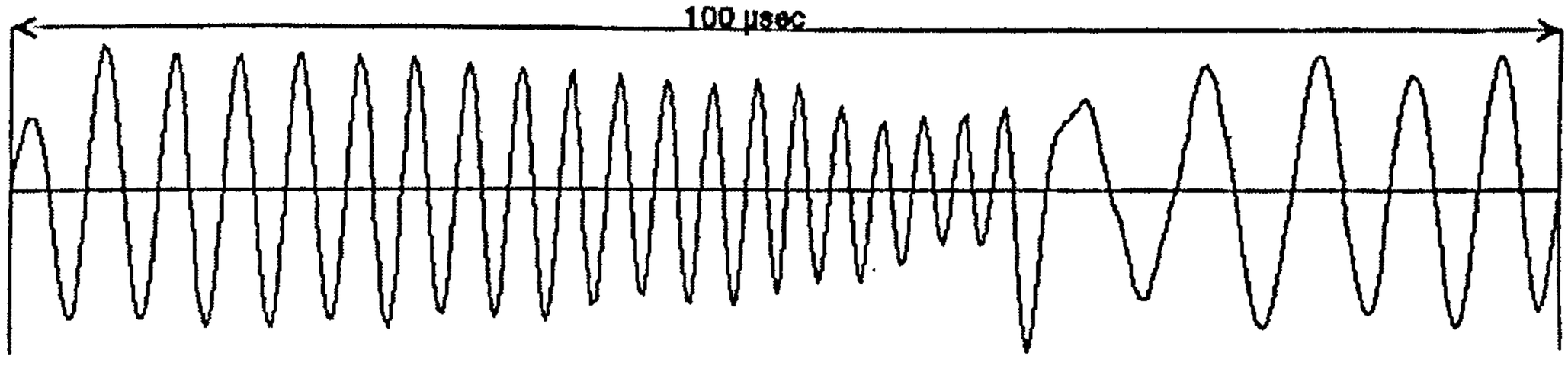


Figure 38: The Intellon 'Chirp' Waveform

It can be seen that the chirp waveform extends in frequency from 100 kHz to 400 kHz. This is well outside of the CENELEC band-plan, but is permissible for use in the USA, where it is used for the PLC medium in the CE-Bus automation system.

We have already mentioned the CENELEC band plan for power line communications systems several times. It would be prudent, therefore, to now discuss the family of standards in which these bands (and indeed many other aspects of PLC) are defined.

6.2 EN 50065 - The PLC Standard

The EN 50065 series is the family of standards that attempt to regulate the development of PLC applications within Europe, at least at the lower end of the frequency spectrum. There are also moves afoot to develop high frequency (HF), high speed, PLC systems, and we will be discussing these at the end of this Thesis.

We will begin by looking at the various parts of standard EN 50065.

6.2.1 EN 50065 : Part 1

To date, only one part of EN 50065 has been formally adopted as a standard, rather than as a draft – EN 50065 : Part 1 [48]. We will look at this standard in more detail shortly, but meanwhile will briefly introduce the other, draft, standards that currently go to make up the EN 50065 series:

6.2.2 EN 50065 : Part 2

This part of the standard deals with the immunity requirements for PLC equipment, within residential, commercial and light industrial environments [49, 50, 51]. Its recommendations are essentially in line with those of the full EMC standard EN 50082, upon which we will be basing our experimental work.

6.2.3 EN 50065 : Part 4

This part of the standard deals with the use of filters as a component of PLC systems [43]. We have already discussed this subject in an earlier chapter.

6.2.4 EN 50065 : Part 7

This part of the standard deals with the subject of the impedance that equipment connected to a PLC system should exhibit so as not to unduly compromise communications [52].

As already noted, only part 1 of EN 50065 is currently a full standard. Its title is: **Specification for Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148.5 kHz. Part 1. General requirements, frequency bands and electromagnetic disturbances.**

Several issues relevant to this research are covered in this standard, and we will now describe them in turn:

6.2.5 The EN 50065-1 Frequency Bands

The frequency bands allocated to different PLC applications are outlined in the table below.

Frequency Band	Sub-Band	Application	
3 kHz – 95 kHz	3 kHz - 9 kHz	The use of frequencies in this band shall be restricted to electricity suppliers.	Use restricted to electricity suppliers
	9 kHz - 95 kHz		Use restricted to electricity suppliers and their licensees
95 kHz – 148.5 kHz	95 kHz - 125 kHz	The use of frequencies in this band shall be restricted to consumers.	The use of this band does not require an access protocol
	125 kHz - 140 kHz		Signalling in this band requires the use of the access protocol described in clause 5 of the standard
	140 kHz - 148.5 kHz		The use of this band does not require an access protocol

Figure 39: CENELEC EN 50065 PLC Signalling Bands

It can be seen that within the context of this research, we are considered a 'consumer' and thus are limited to the frequency band of 95 kHz to 148.5 kHz. More specifically, we will limit ourselves to the sub-band of 125 kHz - 140 kHz, as this is specified as requiring an access protocol to be in place.

6.2.6 The EN 50065-1 Access Protocol

The purpose of the access protocol mentioned above, within the sub-band 125 kHz to 140 kHz, is to enable several PLC systems to operate over the same section of power line *even systems utilising differing signalling techniques or protocols.* The access protocol laid down in EN 50065-1 can be summarised as follows.

- All systems shall use the frequency 132.5 kHz (band centre) to indicate that a transmission is in progress. *In other words, whatever the signalling technique employed, it shall generate a significant spectral component at this frequency that can be detected by other (not necessarily compatible) systems.*

- No transmitter or group of transmitters shall transmit continuously (defined as having no gaps greater than 80 ms) for a period exceeding 1 second. After each transmission, they shall not transmit again for at least 125 ms.

  The 1s limit prevents a single system 'hogging' the PLC channel. The 125 ms gap gives other systems the chance to gain access to the channel once the currently transmitting system has finished.

- All PLC devices connected to the channel shall have a signal detector capable of sensing a signal of 80 dB (μV) (equivalent to 10 mV) within the frequency band 131.5 kHz - 133.5 kHz *(i.e. covering the access frequency defined above)*. Devices shall only transmit when they have sensed the band to be out of use for a set period. This period is randomly chosen, with at least seven different values, between 85 ms and 115 ms. *This random waiting period lessens the likelihood of two nodes attempting to transmit simultaneously.*

6.2.7 The EN 50065-1 Output Levels

Finally, EN 50065 concerns itself with specifying signal levels for PLC transmitters, and also, in consideration of EMC requirements, limits for out of band emissions. Summarising, these output levels are as follows:

Within the band 3 kHz - 9 kHz

- An output level of 134 dB (μV) *(5 V)* with respect to earth.
- An output level of 89 dB (μV) *(28 mV)* differential.

Within the band 9 kHz - 95 kHz

- An output level (for narrow band transmissions) of 134 dB (μV) *(5 V)* at a frequency of 9 kHz, falling to a level of 120 dB (μV) *(1 V)* at a frequency of 95 kHz.
- For wide band transmissions, an output level of 134 dB (μV) *(5 V)*

Within the band 95 kHz - 148.5 kHz

- 116 dB (μV) *(630 mV)* for general use.
- 134 dB (μV) *(5 V)* for special use (e.g. Industrial).

In addition, the standard defines limits for conducted and radiated interference generated outside of the normal operating band.

That concludes our look at EN 50065. Next, we will consider the requirements of protocols for use in PLC applications. We will concentrate on the low levels of the OSI stack (levels 1 & 2), directly involved in the transport of the data between nodes.

6.3 The Need for Protocols in PLC Applications:

We have now looked at some modulation techniques applicable to a PLC environment. These form an important part of the Physical Layer (Layer 1) of the OSI model, as already introduced.

Moving up a level in the OSI stack, in a real-life communication situation, we must ensure that the 'intelligence' passes through the medium (the Power Line in this case) without corruption. There will be several influences that will prevent this.

- Imperfect characteristics of the transmission medium which will corrupt the data being sent. The power line, is a particularly bad example of this, as has already been discussed.

- The necessity for many nodes to exist on the medium at the same time, and to communicate amongst each other in an orderly manner. This implies either some form of arbitration scheme, or collision detection/avoidance mechanism.

It is these points which are addressed by the use of a communications protocol.

6.3.1 What is a Protocol?

In 1948, Claude Shannon, the digital communications pioneer, made the following comment: *'The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.'*

This rather succinctly defines the purpose of a communications protocol. A protocol is a set of rules for communicating between systems. Protocols govern format, timing, sequencing, and error control. Without these rules, the receiving node will not be able to make sense of the stream of incoming bits.

In the following sections, we will be looking at all of these aspects of a communications protocol, beginning with timing, or synchronisation.

6.4 Synchronous and Asynchronous Transmission

Fundamental to a serial communication system is the requirement for a receiving node to tell when items of data are being presented to it. This implies that some form of synchronisation must exist between transmitter and receiver.

There are two types of digital serial transmission commonly encountered: 'Synchronous' and 'Asynchronous'. Their names are indicative of how they achieve the synchronisation function.

6.4.1 Synchronous Transmission

When a serial bit stream is received, it is necessary for the receiver to know exactly when a particular bit position occurs, in order that its state is correctly registered. The term synchronous implies that this information is inherent in the transmitted signal. This can be achieved in several ways.

Perhaps the simplest, and used on some base band systems (such as I^2C, which we have already described), is to have a separate line carrying this 'clock' information, as shown in the figure below.

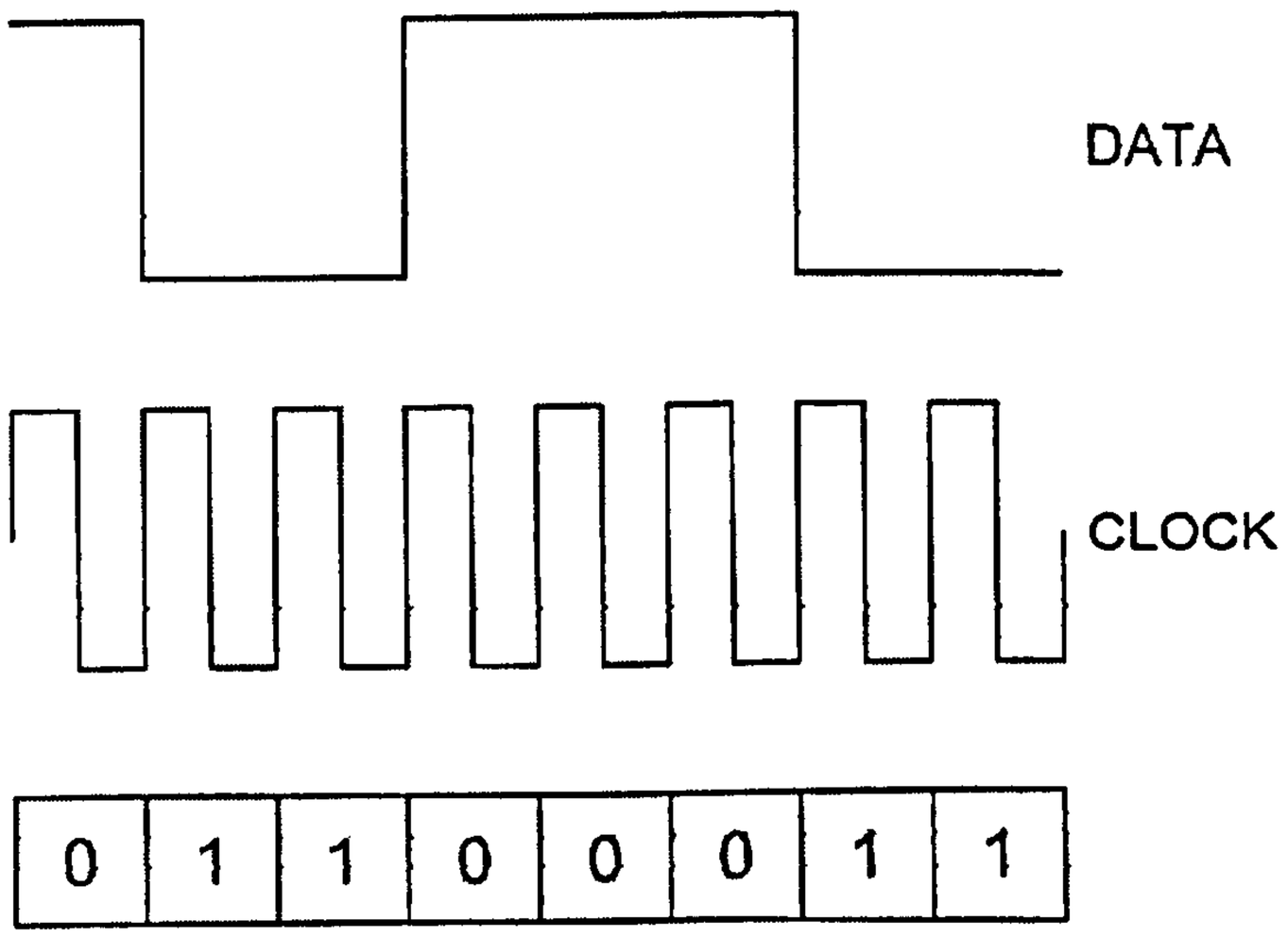


Figure 40: Example of a Synchronous Transmission

In this example, the receiver will sample the data on a high-low transition of the clock line, since this corresponds to the centre of each data bit. However, a penalty of this technique is that an extra signal wire is required.

A better technique is to have a local clock signal, at the receiver, at roughly the correct frequency, and to 'lock' this to the incoming data stream. The technique utilises a type of circuit referred to as a phase locked loop (PLL), commonly encountered in communications system performing such tasks as frequency synthesis. Once the clock is locked, the receiver can safely check the transitions of the received data based on this local clock.

Obviously, it is necessary for the clock to remain 'in-lock' for the duration of the data packet being received. This is not too difficult to achieve, so long as there are sufficient bit transitions within the data stream.

Commonly, synchronous data protocol packets will start with a 'preamble' sequence of bits. Amongst other purposes (such as adjusting the gain of any amplification stages), this can help provide the initial synchronisation of the local clock. Once initial lock is achieved, a transition every cycle is not required to maintain lock.

Long ‘trains’ of data '1's or '0's, which might run the risk of the PLL losing lock, can be avoided by techniques such as 'bit stuffing' or other coding schemes which guarantee regular transitions in the data stream.

6.4.2 Asynchronous Transmission

In asynchronous transmission, there is no need for a local clock to lock onto the bit rate of the incoming data stream. In this technique, the data is split into small blocks (typically 8 bits in length). Each block is then framed by additional bits, whose purpose will now be described.

The start of each block is defined by a 'start' bit, which is, by definition, the inverse of the 'idle' state of the transmission line. When this start bit is detected by the receiver, a time delay is initiated, sufficient to take the receiver into the middle of the next bit (i.e. 1.5 bit periods), which is the first data bit. The data is sampled at this point, then a further delay of one bit period is initiated, and the second data bit sampled, and so on, until all data has been sampled. There next follows an (optional) parity bit, the function of which is described below, and finally 1 or 2 'stop' bits, defined as being at the idle state for the line. Immediately the stop bit period is over, a new transmission may begin immediately, or the line may carry on in the idle state. It can be seen that, should the accuracy of the local clock/timer differ from that of the transmitter, there will arise a cumulative error. As long as this error does not exceed 0.5 bit periods in either direction, then the received data will be sampled correctly. Over the relatively small frames involved (typically no more than ten bits) there is no problem achieving this accuracy.

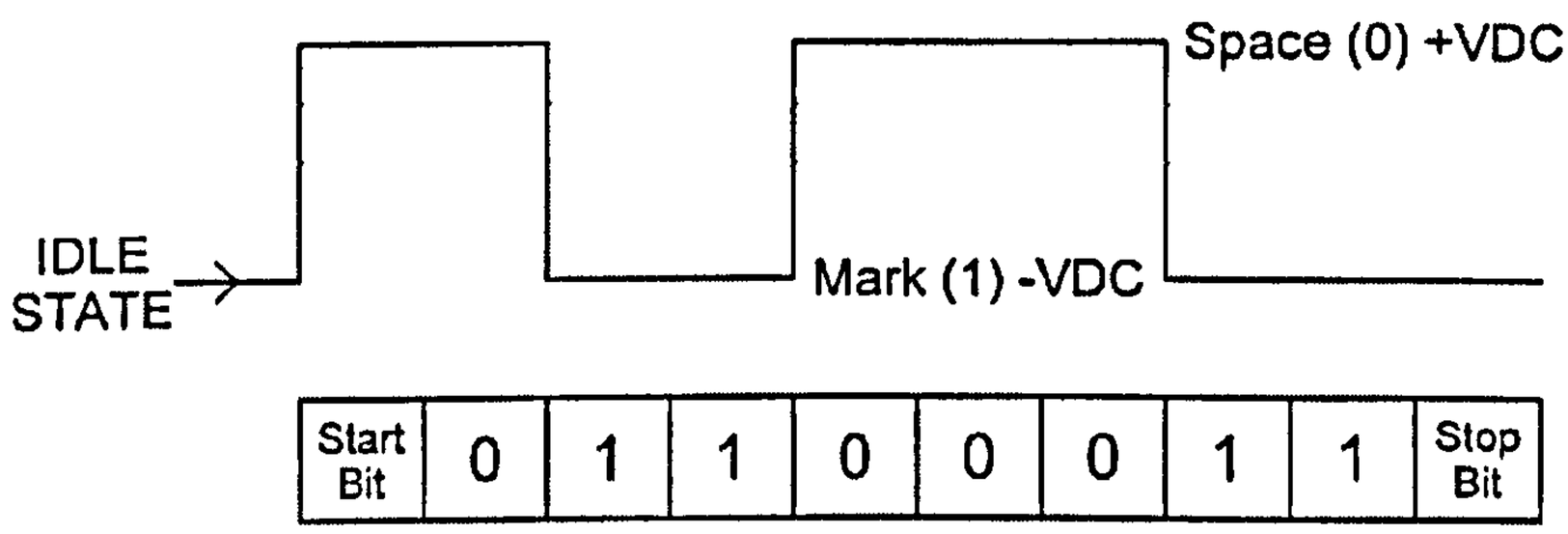


Figure 41: Example of an Asynchronous Transmission

The major disadvantage of asynchronous transmission is the relatively high overhead. It can be seen that to transmit eight bits of data, at least ten bits are required (eight data bits, 1 start bit and 1 stop bit). In reality, the overhead can be even greater if error detection techniques such as parity are utilised.

Protocols using data packets can be constructed from a stream of asynchronous characters, thus permitting the use of standards communications circuits. An example of this if the HART system already described.

Having synchronised our receiving and transmitting nodes, we must next make sure that our data has been received correctly. We will discuss techniques for this in the next section.

6.5 Techniques for Error Detection and Correction

6.5.1 Parity.

This is perhaps the simplest technique for detecting an error within digital data. The principle is simple - a given block of data, of fixed length, is analysed in terms of the number of high (logic '1') bits. Depending on the parity chosen ('odd' or 'even') the parity bit is set or reset so that the total bit count (including the parity bit) is odd or even as appropriate. This technique is commonly used in asynchronous transmission techniques such as RS-232.

At the receive end, the data block is analysed and the result compared against the state of the received parity bit, taking into account the parity scheme in force. As a technique, it is capable of detecting an odd number of bit errors within the data block - a single altered bit (data or parity) will result in the parity rule being violated. It can be seen however, that if two bits are corrupted, then the parity bit will again agree, and the error will not be detected. In general, an odd number of bit errors will be detected, but an even number not so.

6.5.2 Checksum

This is applicable to data contained within packets. Here, the entire packet is 'summed' according to a predefined formula. The resulting data is the checksum value, which is sent along with the rest of the packet. At the receiving end, the summing process is repeated and the result compared with the received checksum. If the two values differ, then the data has been corrupted. The receiving station will signal this to the receiver by either making no response (where an 'acknowledge' (ACK) response is the normal response), or a 'negative acknowledge' (NAK) response. The transmitting station will then know that it should re-transmit the data.

6.5.3 Error Correction Techniques

One stage further from the concept of detecting an error is that of being able to correct it 'on the fly' without the need to retransmit the data. Many techniques can be used for this purpose. One of the simpler of these is the 'Hamming Code'.

Hamming coding, is really an enhancement of the parity technique already discussed [53]. Consider the following diagram:

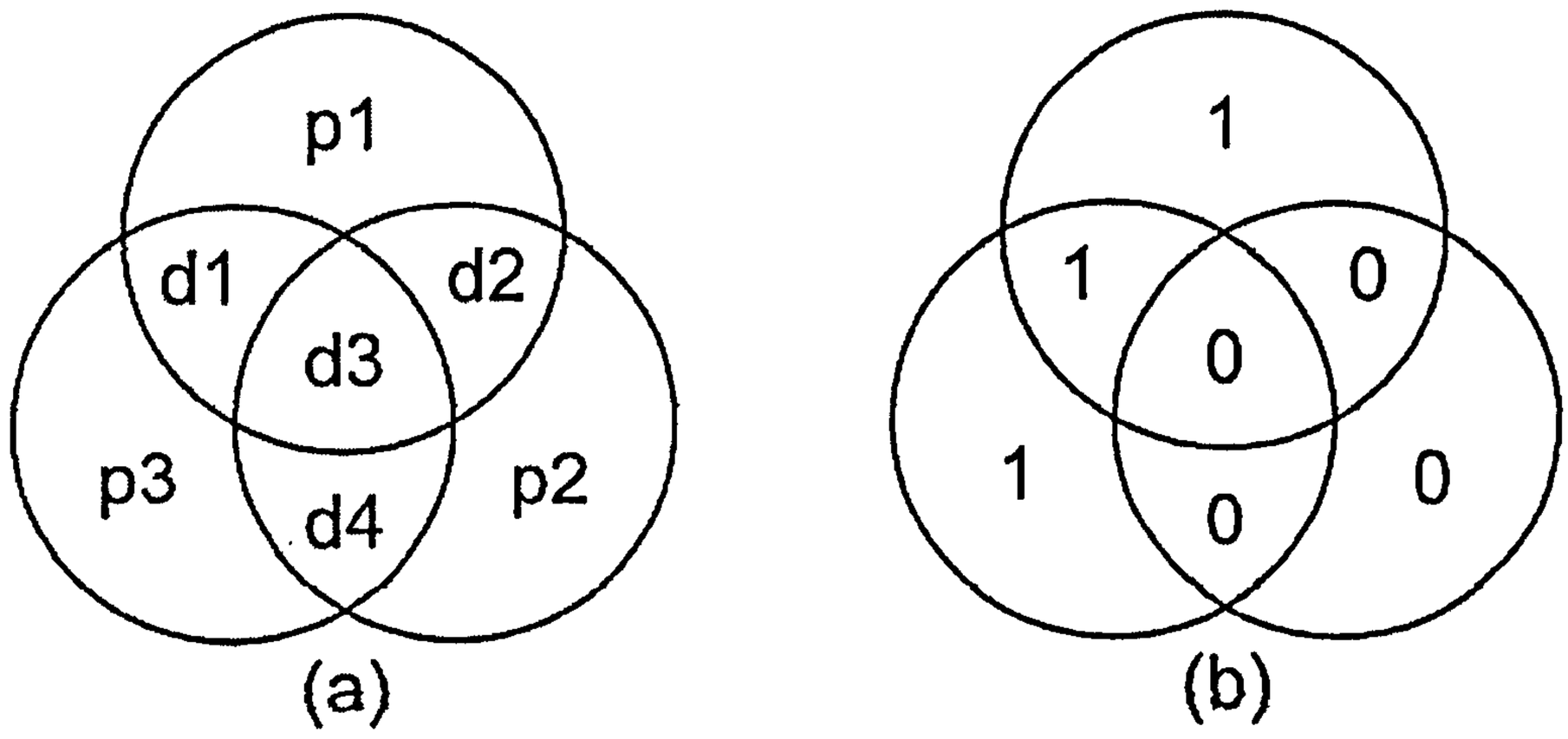


Figure 42: Example of Hamming Coding

In part (a) of the above diagram, d_1, d_2, d_3 & d_4 represent a four-bit data word, and p_1, p_2 & p_3 represent parity bits corresponding to the data bits enclosed within the corresponding circle. In other words, p_1 is the parity bit for d_1, d_2 & d_3, p_2 is the parity bit for d_2, d_3 & d_4 and p_3 is the parity bit for d_1, d_3 & d_4.

Part (b) of the diagram represents the coding for the data word '1000'. It can be seen that even parity has been applied as each circle ends up with an even number of bits. The calculated parity bits are sent along with the data giving the overall transmitted data '1000110'. This is referred to as a 7:4 Hamming code, as it requires a total of seven bits to convey four data bits.

Decoding and checking the received data is carried out as follows: The received parity bits are checked against their corresponding data in the same manner as shown above and any errors noted. According to which of the three parity checks fail, it is possible to detect, *and correct*, a single bit error within the data.

For example, if data bit d_1 is corrupted, it will cause both the parity check including p_1, and that including p_3 to fail. Most importantly, it is the only single-bit failure that will have this precise effect. Data bits d_2 & d_4 will have a similar effect on the parity checks involving p_1 & p_2, and p_2 & p_3 respectively. A corruption of data bit d_3 will cause all three parity checks, p_1, p_2 & p_3 to fail. Finally, should any of the three parity bits become corrupted, they will only affect their associated parity check group.

Therefore, having detected the single bit failure, it can be corrected and the data passed on without the need for retransmission. The scheme also offers the potential to detect (but not correct), any number of errors within the data word.

That was an example of a 7:4 Hamming code, suitable for a medium where no more than one error is to be expected within a single group of seven bits. There are other Hamming schemes available that offer a greater error recovery potential, as well as other more sophisticated forms of error correction scheme such as Trellis coding or Reed-Soloman coding.

We will not be considering them further in this Thesis. This is because a notable downside of all such techniques is that they require a considerable overhead in terms of additional data quantity (for example, a 75% increase in the data word size, for the 7:4 Hamming example.

Such techniques are useful in applications where retransmission is not a viable option. For example, when a real-time response is essential, such as in the playback of Compact Discs, or where long time-scales and persistently noisy channels are the norm, such as the transmission of images from space probes.

In practical communication applications, the overhead required for forward error correction schemes is too great, it is simpler to have an error detection/retransmission scheme such as parity, checksums or CRC.

We have already mentioned that many protocols require data to be in the form of a 'packet'. We will next consider the structure of a 'typical' data packet used within a communications protocol.

6.6 The Structure of a 'Typical' Data Packet

In many communications protocols utilising data packets, the packets all have a broadly similar structure. In this section, we will outline the various elements that go to make up a 'typical' data packet, in this case, from the HART Fieldbus protocol already discussed in an earlier chapter.

The structure of a typical HART packet is shown in the diagram below:

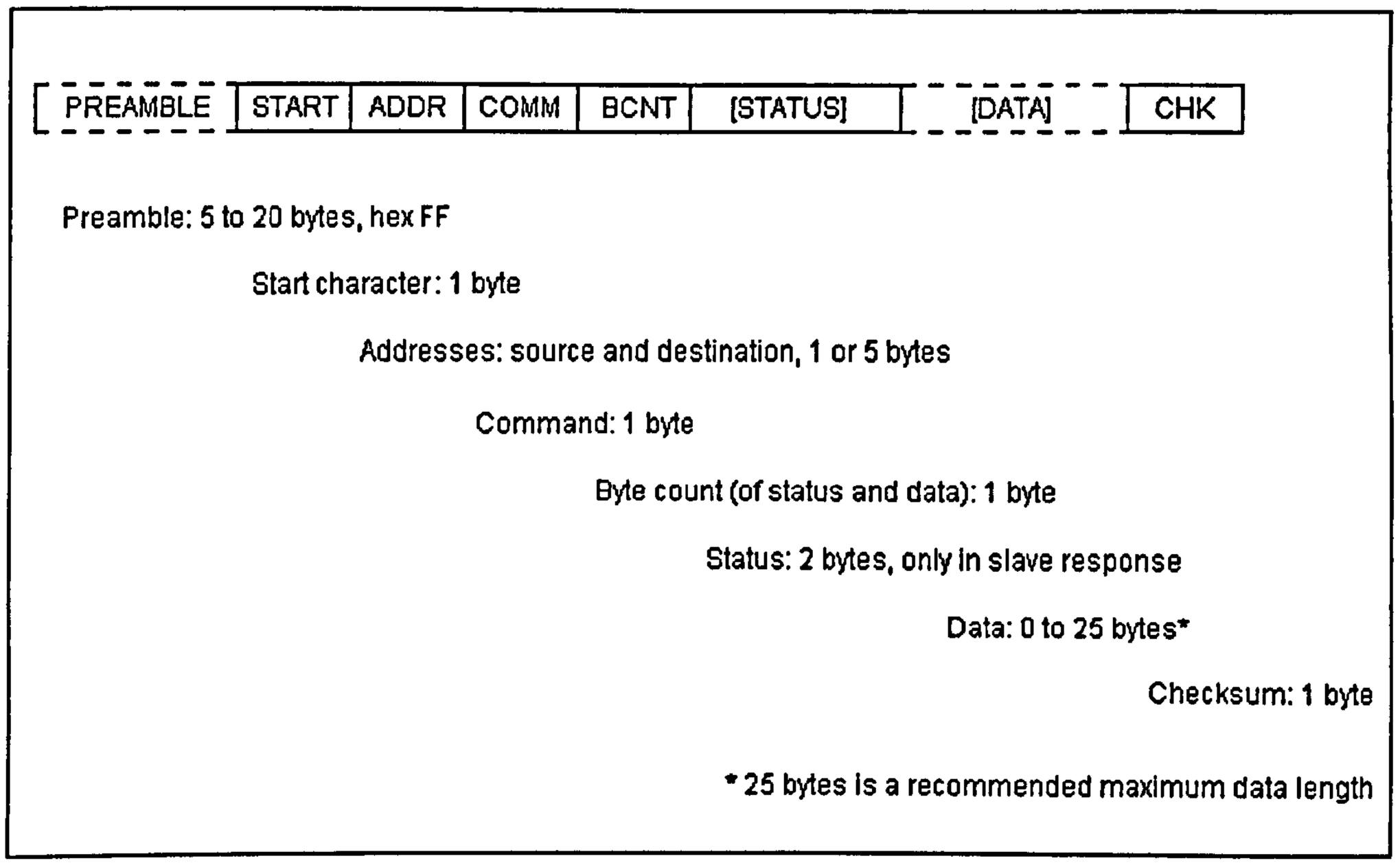


Figure 43: HART Packet Structure

As has already been mentioned, HART uses a modulated audio frequency carrier signal superimposed upon a 4-20 mA current signalling line. We will now look at the function of the component parts of the data packet, shown above.

- The 'Preamble' part of the HART packet consists of five to twenty hexadecimal 'FF' characters (binary, all logic '1'). Its purpose is to permit the analogue modem receiver circuitry to adapt itself to the incoming signal (for example, through automatic gain setting). We have already noted that, for simplicity, HART uses an asynchronous scheme to transmit its data. In other, base-band, synchronous, transmission schemes, the preamble would be used to permit the receiver clock to become synchronised to the coming transmission.

- The 'Start' character (one byte long) in a HART transmission can have several values according to the type of transmission (for example: Master-to-Slave, Slave-to-Master, or Burst Mode). In synchronous schemes, the start character is usually a unique bit pattern that indicates the start of the packet proper to the receiver.

- The 'Address' field in the HART data packet can be one or five data bytes long (according to the particular variant of HART). It contains both the Master and Slave addresses (HART permits up to two masters on a single loop).

- Next comes the 'Command' byte. This defines the action required of the slave by the master node. It is commonly one byte long (giving potentially up to 256 commands), but the use of a special code '254' indicates that a further byte will follow, giving the option of additional commands being defined.

- Next is the 'Byte Count', a single byte value indicating the length of the rest of the packet.

- Slave HART nodes replying to masters will next send two 'Status' bytes which include such information as any communications errors that may have occurred, and status information (for example, 'busy' or 'command not understood') from the slave.

- The next section of the packet is the 'Data' field. This is used to convey data to and from master and slave nodes, and the data may be in any appropriate format. Data can be variable in length from zero (no data required by that particular command) or up to 24 bytes.

- Finally, in the HART packet we have the 'Checksum'. As already noted in this chapter, this is a calculated value based on the contents of the rest of the packet. In HART it is a single byte value resulting from logically 'exclusive-or'-ing all of the rest of the bytes making up the packet together, beginning with the 'Start' character. The receiver will recalculate the checksum and compare it with the received value. If a difference is found, then there must be a corruption of the packet, and a retransmission will be requested. Up to three corrupted bits within a single message may be detected reliably in this fashion, with some chance of detecting additional errors. It must also be remembered that, in the case of HART, there is also the individual parity bit check that applies to each individual byte making up the packet).

That concludes our look at data packet structure. We will not dwell on protocols any further in this Thesis, as we are concentrating in our experimental work on the performance of the physical layers. However, protocols will form an important part of the follow-up work that will lead on from this initial study. We will look at exactly how, and consider the future direction of this research, at the end of the Thesis.

Next, though, we will look at the typical data rates required for the kind of industrial control applications envisaged.

6.7 Data Rate Requirements for Industrial Control

If PLC is to be suitable for industrial control, we must ensure that the system is capable of responding sufficiently fast to meet the need of the process. The author has already published a joint paper [7] that addresses some of these issues.

If we again use the HART system as a typical example, we can calculate the length of 'typical' message packets. To start with, we will consider a 'worst case' scenario, assuming maximum field lengths.

The packet will then consist of:

- 20 preamble bytes +
- 1 start byte +
- 5 address bytes +
- 1 command byte +
- 1 count byte +
- 2 status bytes + (NB. In slave response mode only)
- 25 data bytes +
- 1 checksum byte = 56 bytes in total

We already know that HART utilises an asynchronous framing scheme for each byte consisting of:

- 1 start bit +
- 8 data bits +
- 1 parity bit +
- 1 stop bit = 11 bits in total

Therefore, we can determine that the packet length for the worst case example above will be 616 bits (11 x 56).

If we consider a 'best case' scenario, with minimum field lengths we come up with:

- 5 preamble bytes +
- 1 start byte +
- 1 address byte +
- 1 command byte +
- 1 count byte +
- (0 data bytes) +
- 1 checksum byte = 10 bytes in total

Which gives a total packet length of 110 bits. We already know that HART operates at a rate of 1200 baud (signalling states per second). Therefore, we can state that the worst case packet will take just over 0.5 seconds to transmit, and the best case packet just under 0.1 seconds.

Of course, in reality, the passing of a message will consist of two packets - one sent, and an acknowledgement returned, so in a worst case scenario we are looking at around one second, or around 0.2 seconds best case.

A signalling rate of 1200 baud is a typical value for the power line modems that we will be looking at so these figures represent good 'ball-park' figures.

Within industrial control, there are many functions that require a very rapid response time (of the order of milliseconds). An example might be the control of fast moving machinery. High speed Fieldbus networks may be able to achieve such rates, but Fieldbusses such as HART, and our proposed PLC system, will not be suitable for such use. However, there are a great many other applications where responses of a second (or even longer), are quite acceptable, and it is on these that we hope to apply our system.

It is worth noting that manufacturers are beginning to propose high-speed PLC solutions, based on sophisticated electronics and transmission schemes. These are primarily aimed at home networking or internet access, but (if reliable) could offer a future potential for PLC technology to move into the realm of high-speed Fieldbus.

Such systems are beyond the scope of this Thesis, but we will discuss them briefly in our conclusions section.

Before moving on to a detailed description of the experimental work, in the next chapter, we will conclude this chapter by expanding on the 'Power Bus' concept, proposed by the author for industrial control applications.

6.8 The 'Power Bus' Concept

The term 'Power Bus' was coined to convey the idea of the power line forming a 'backbone', connecting all of the sensors, actuators, and controllers to be found within a typical industrial control application.

6.8.1 The Basic Application of the 'Power Bus'

Referring back to the discussion of MAP in a previous chapter, the area in which we propose that 'Power Bus' would operate represents the bottom level of the MAP hierarchy. Controllers utilising power bus would communicate with higher levels in the automation scheme (if required) using (perhaps) PLC or other Fieldbus techniques.

As we have already discussed, response times for our PLC system are likely to be of the order of a second or so, and this is perfectly adequate for many industrial control scenarios. We will now give an example, from an area in which the author is experienced.

6.8.2 A Burner Control Example Suitable for 'Power Bus'

The lighting-up of a large industrial burner plant must follow a set sequence of operations to ensure safety - there are going to be (potentially) large quantities of explosive fuel/air mixture present. Typically, such plant is operated by a discrete 'controller' which might be electromechanical in nature, utilising relay logic (as described in an earlier chapter), or increasingly, might be solid state, or incorporated into a distributed control system (DCS). Whatever technology is used, great care must be taken to avoid the possibility of a failure of the controller producing a hazardous condition.

A typical (simplified) sequence of operation would be as follows.

- *The controller is requested to light burner by an external signal (for example, a thermostat, or maybe a signal from a DCS).*
- *The controller starts an electrical fan, passing air into the burner.*
- *Within (say) five seconds, an airflow sensor must indicate to the controller that air is in fact flowing (i.e. the fan is operating correctly).*
- *The controller the drives the fan to its maximum airflow rate, and the achievement of this state is signalled to the controller by a sensor.*
- *This maximum flow is maintained by the controller for, typically, 30 seconds to expel residual fuel/air mixture from within the burner.*
- *The controller then drives the fan to a lower air flow rate prior to lighting the burner, and the achievement of this state is signalled to the controller by a sensor.*
- *The controller then operates a valve, supplying fuel to a small 'pilot' burner, and operates an electrical ignition spark to ignite the fuel.*
- *A flame sensor signals to the controller that the pilot flame has lit.*
- *After allowing a few seconds for the pilot flame to establish itself, the controller opens another valve, initially at a low flow rate, permitting fuel to reach the 'main' burner, which is lit by the pilot burner.*
- *When the flame detector indicates to the controller that the main burner has lit, it turns off the pilot burner and permits the main burner to establish.*

- *Once the main burner has been allowed to establish itself for a few seconds, the controller permits the main fuel valve to be controlled by a 'modulator' system. This varies the heat output of the burner to meet the heat demands of the system.*

- *Throughout the operation of the burner, the flame and airflow condition are monitored by the controller, and in the event of a loss of either, the controller causes the system to go to an alarm state.*

- *When the demand for heat is satisfied, signalled to the controller from external sources (e.g. a thermostat), the controller shuts down the burner in an orderly and safe fashion.*

As can be seen from this description, there are a number of 'sensors' and 'actuators' involved in this process, all of which must be connected to the controller by a mass of discrete wiring. (NB. A diagram showing the typical wiring arrangement for a burner control application is given in the transcript of the authors' joint paper, reproduced as an appendix of this thesis).

The time interval from start to 'running' is typically some 90 seconds, with individual timings rarely less than a second or so. Therefore, the time-scales involved are within the capabilities of our PLC application and the existing complicated wiring scheme could be replaced by a single 'Power Bus' supplying both power and switching instructions to the system.

It is also worth noting that applications such as the above are, in effect, isolated systems – they are practically self-contained, and separated from the main plant power distribution network via the controller itself.

By the judicious use of power line filtering techniques (as already discussed in a previous chapter) we can potentially overcome many of the noise and attenuation problems associated with PLC.

Finally, it must be noted that applications such as burner control are 'safety critical'. Even with a tradition hard-wired arrangement, it must be ensured that any potential fault conditions in the controller must not result in a dangerous state on the plant being controlled.

Such precautions would equally have to extend to the power bus itself, if used. This is beyond the scope of this Thesis, but would form an important separate line of research in its own right.

Having looked at using the power bus to replace existing wiring schemes, it must be remembered that it also has the potential to offer 'value added' benefits.

6.8.3 The Power Bus and 'Value-Added' Services

The 'Power Bus' concept may be applied at several levels. The most complex, as described above would involve the complete replacement of a traditional field wiring scheme with the power bus, whereby the only interconnections between the various sensors/actuators and the control elements is the mains power supply line.

This concept would of course need to be implemented at the design stage in the construction of plant, or at least retrofitted during a plant refurbishment.

An alternative power bus application would provide 'value added' services to an existing plant control system. Here, with the addition of PLC nodes, extra features could be added without the need for additional wiring to be installed hence the description 'value-added'.

Consider our previous burner control example, utilising the standard wiring:

- As already noted, the fan is simply switched on and off by the controller. Add a PLC node at the controller and another at the fan motor itself. It would now be possible for the fan node to report back to the controller parameters such as the fan running speed, or the fan motor operating temperature, both of which could give early warning of upcoming problems.

- The flame sensor is traditionally an on/off device, simply signalling if the flame is lit by way of a relay contact. By adding a PLC node, the flame sensor could report actual values of flame signal, providing useful information to an operator, or again warning of upcoming problems.

There would be numerous other such potential 'value-added' services possible within an industrial control scenario.

That concludes our look at the 'Power Bus', and indeed of the entire background sections of this Thesis. We will discuss the future directions in which this research (and the entire power bus concept) might be continued in our conclusions section at the end of the Thesis.

Meanwhile we will move on to the experimental work proper, starting with background information and the decision to create a specialised item of test equipment for the experiments.

Chapter 7 : Introduction to the Experimental Work

The author considers himself, primarily, a 'hands-on' engineer and it was intended that this would be reflected in the experimental work for this Thesis. We have already discussed the extremely variable nature of the power line medium in a previous chapter, and this could pose problems if we wish to make meaningful comparisons between different PLC solutions. What is required are some quantitative and repeatable 'standards' for noise and interference.

It was decided, therefore, that artificially generated noise and interference, meeting the requirements laid down in the EMC immunity standards, would be used to provide such a comparison.

In order to gauge the performance of the PLC systems under test, we will measure the bit-error-rate (BER) of the communications link. BER is defined as the ratio of bits corrupted over a communications link, to the total number of bits received. BER can be expressed as a percentage or as a power of 10 i.e. 1 in 10^{+9}. In the latter example, for instance, one bit in 1,000,000,000 is corrupted. This in fact represents an extremely low figure, as will be seen as the experiments proceed.

The authors' working situation precluded the availability of commercial test instrumentation to perform this task. It was therefore decided that a bit error rate test set would be designed and built from scratch, specifically for this application.

This development will be described in a later section, but next we will look at details of the actual experimental work undertaken.

7.1 A Brief Outline of the Experiments

It was the aim of the experimental work in this research to provide practical comparisons of the performance of PLC systems suitable for industrial use. The experimental strategy was to test the systems under conditions of simulated (and repeatable) interference. The nature and characteristics of this interference was based on the immunity requirements laid down in international standard EN 50082.

As has already been discussed, power line noise can be of a number of types, including Background, White, Synchronous, Non-Synchronous, or Impulse. From the point of view of EMC testing, however, the standards bodies have defined a 'generic' noise waveform. This waveform is referred to as a 'Fast Transient Burst' (FTB).

7.1.1 The Fast Transient Burst (FTB) Tests

The structure of the FTB waveform is shown in the diagram below.

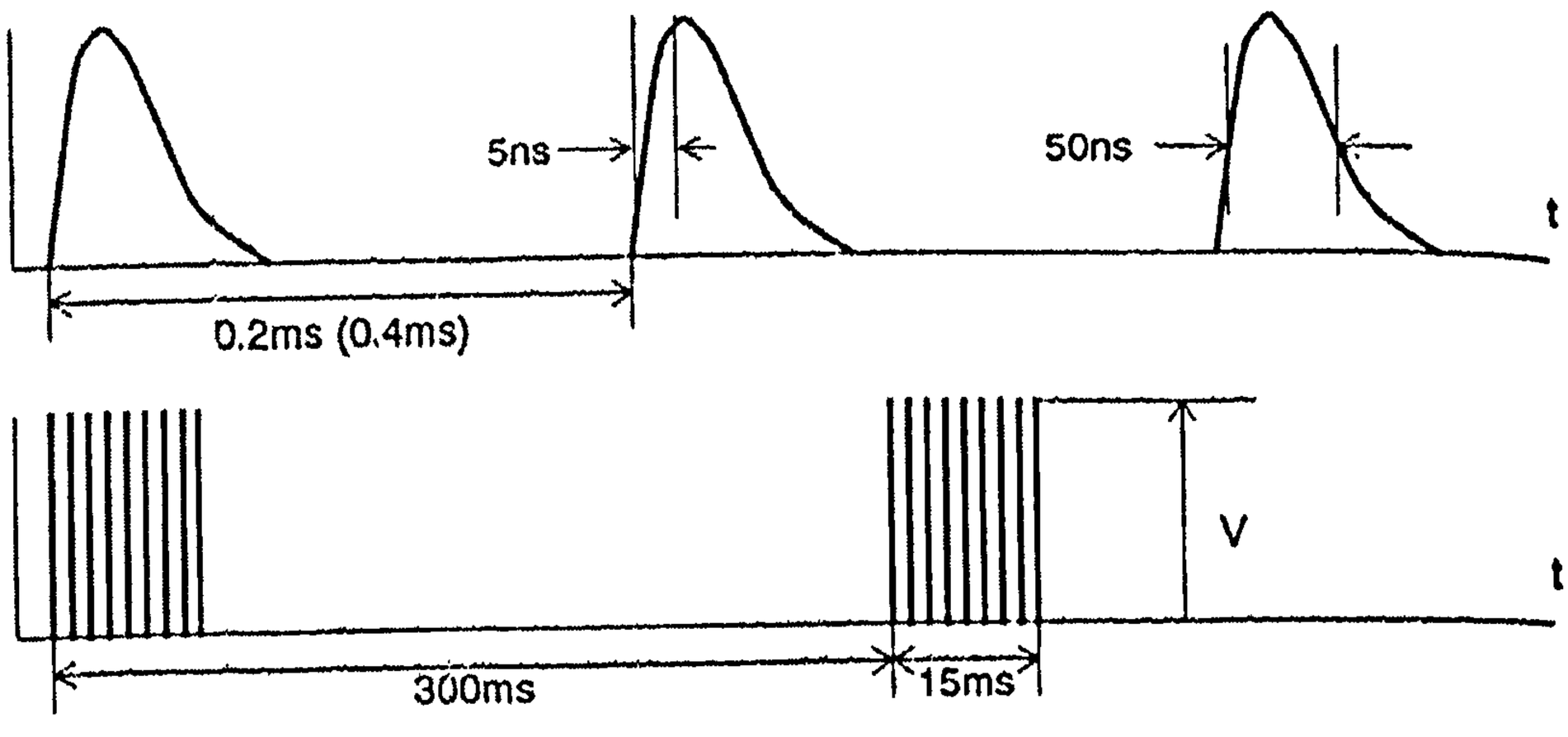


Figure 44: Fast Transient Burst Waveform

It can be seen that the individual pulses that go to make up the FTB waveform, shown in the top part of the diagram, have a fast rising edge (5 ns) and a narrow width (50 ns). The pulses are spaced at either 0.2 ms or 0.4 ms (giving a pulse repetition rate of either 5 kHz or 2.5 kHz). The commonest repetition rate is 5 kHz, with 2.5 kHz only being used for the most stringent (4 kV) test.

The pulses are generated in 15 ms bursts, at intervals of 300 ms (as shown in the lower part of the diagram). The amplitude of the FTB pulses may be 500 V, 1 kV, 2 kV, or 4 kV, depending on the stringency level of the test applied. The pulse stream in our experiments will be supplied by a commercial FTB generator, intended for EMC immunity tests.

7.1.2 The Spot Frequency and Swept Frequency Noise Tests

In addition to the FTB tests, tests were carried out to evaluate the performance of the PL modems in response to spot and swept frequency noise.

These tests are not actually a part of the relevant immunity standards. In some respects, they are akin to the RF common mode immunity tests, however these operate over a frequency range of 0.15 to 80 MHz, outside of the PL communication bands. They were included because the equipment was available, and the author felt that some knowledge was to be gained.

A signal generator was used to generate this sine-wave interference at various frequencies around the operational frequencies of the PL modems. Additionally, the sine wave frequency was also swept across the operational frequency of the PL modems, and the performance under these conditions logged.

As a finale to the above 'laboratory' experiments, a series of 'real world' tests were performed. Here the PLC modems and BERT equipment were set up in a 'typical' light industrial environment (the authors workplace), and left running continuously.

We will describe these 'real world' experiments in greater detail at the end of this chapter. Meanwhile, before describing the development of the bit error rate test equipment, we will look at the choice of power line modems suitable for our experiments, then describe the operation and physical circuitry of those chosen.

7.2 The Choice of Power Line Modem for the Experiments

The nature of the proposed experiments, as outlined in the previous section, means that it is necessary to have modems where we can access the 'pure' bit streams at the receive and transmit ends of the communications link.

Unfortunately, many PLC modems integrate an actual communications protocol into a single integrated circuit (IC) or set of integrated circuits (a 'Chip Set'). Consequently, such modems are unsuitable for our experiments. However, in later experimental work, where we will be considering the effectiveness of the communications protocol used, we will be able to make use of such modems.

However, for these experiments, simplicity is a virtue, and we have available examples of modems for two of the more straightforward modulation schemes, ASK and FSK.

We will discuss these modems, their principle of operation, and their circuitry, in detail in the next section.

7.3 A Description of the ST7537 FSK Modem

The first modem to be evaluated is based around the ST7537 IC [16]. This device is an FSK modem, manufactured by the SGS-Thomson Company. It is designed to comply with EN 50065, working at carrier frequencies of 133.05 kHz (representing logic '0') and 131.85 kHz (representing logic '1'). This arrangement neatly complies with the EN 50065 access protocol arrangement, since it is (roughly) symmetrical about the centre frequency of 132.5 kHz, and both frequencies fall within the pass-band required (131.5 - 133.5 kHz). The ST7537 is rated by the manufacturer for operation at a nominal signalling rate of 2400 baud.

A block diagram of the device is shown below.

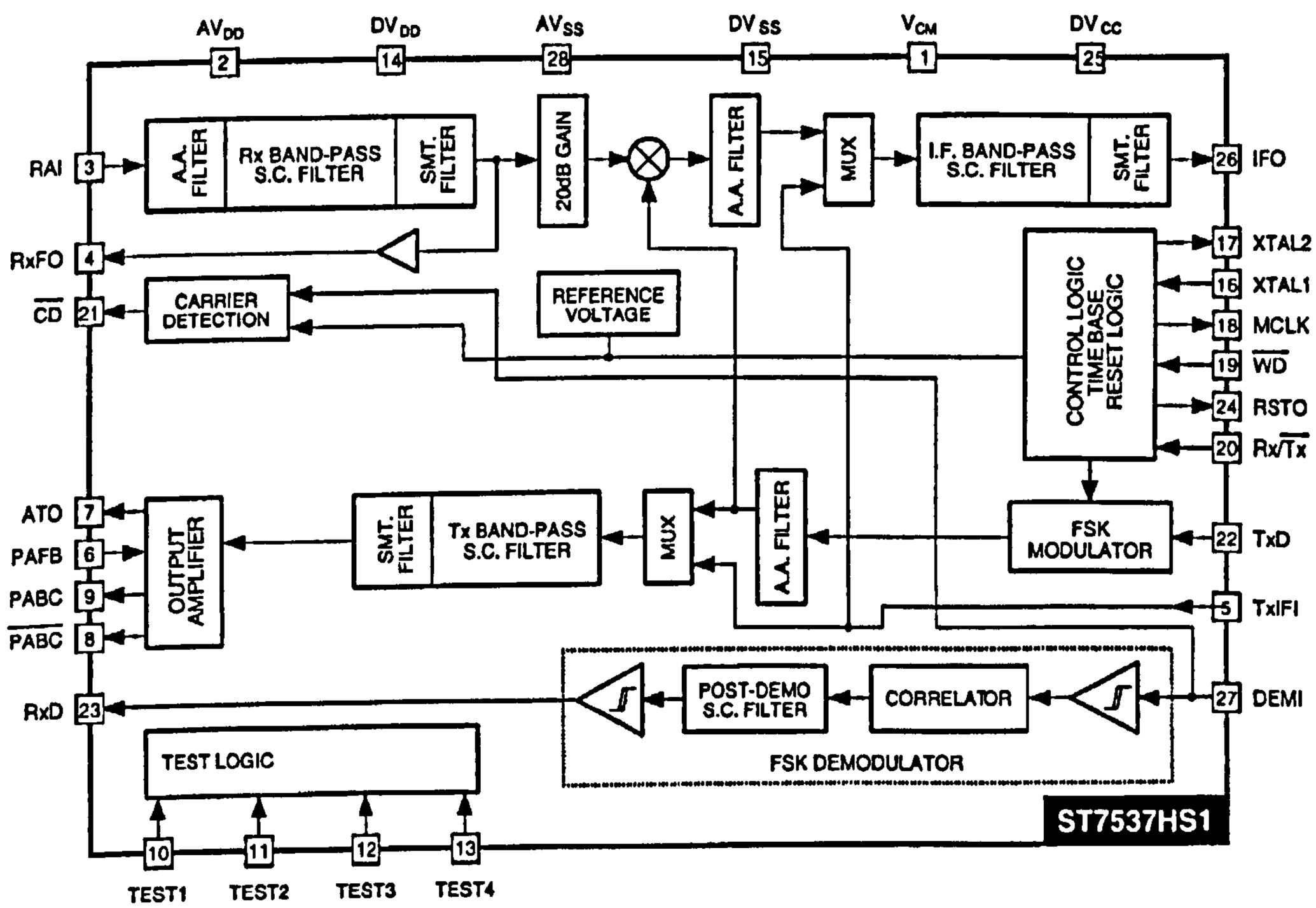


Figure 45: Block Diagram of the ST7537 PL Modem IC

7.3.1 The ST7537 Transmit Path

The carrier frequencies in the ST7537 are derived from a master clock of 11.0592 MHz, by a process of division and sine wave table synthesis. The appropriate frequency is selected and filtered in a switched-capacitor digital filter, before being applied to the output amplifier driver stage. The ST7537 requires an external power amplifier stage, which will be discussed later. The device also provides enable outputs for the purpose of de-activating this PA stage when the device is in the receive mode. In addition, there is a watchdog system, which will disable the transmitter after an interval of one second, to prevent a faulty network node from blocking the network (again, in keeping with the requirements of EN 50065).

7.3.2 The ST7537 Receive Path

On the receive side, the input signal from the power line firstly passes through a band-pass filter with a bandwidth of about 12 kHz. After subsequent amplification, the signal is mixed with another locally derived signal and passed to an intermediate frequency (IF) band-pass stage with a centre frequency of 5.4 kHz. The output from this stage is passed (via an external capacitor) to a correlator stage that discriminates between the two resultant intermediate frequencies.

Switching between transmit and receive mode is achieved by setting the logic level on pin 20 of the ST7537 device. A logic '0' is transmit mode and a logic '1' receive.

7.3.3 The ST7537 Support Circuitry

In order to create a working PL Modem, certain support circuitry outside of the modem IC itself is required. The modem design utilised in these experiments was based upon the manufacturers recommended application circuit, and is shown in the following diagram. It was supplied as a kit by a Swedish Company, High-Tech Horizons, who have also developed a communications protocol called SNAP [54], proposed for use in PLC applications.

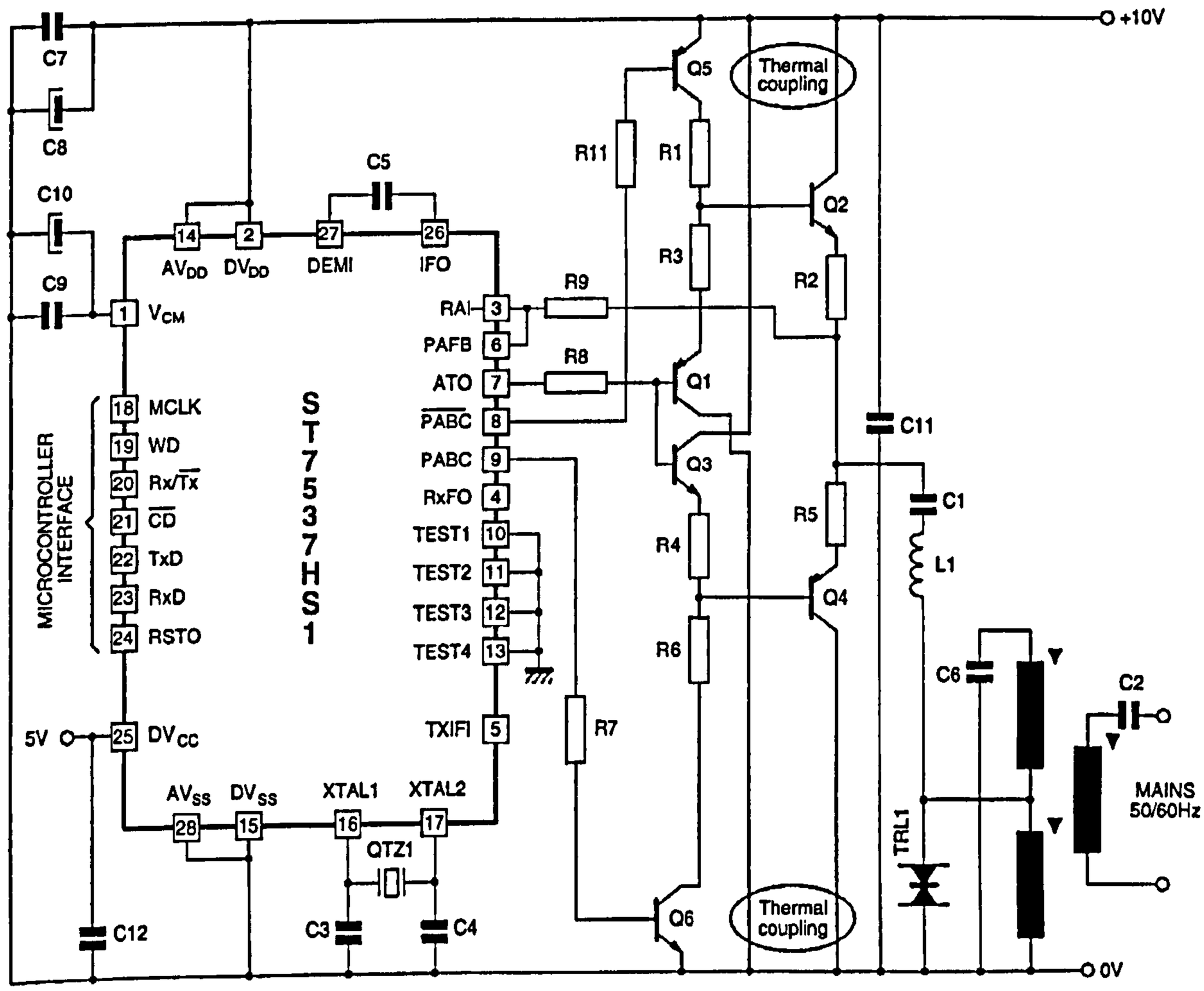


Figure 46: Circuit of the ST7537-based Modem

It can be seen that there is a significant amount of support circuitry required for this device. Most noticeable is the power amplifier stages, consisting of transistors Q1 - Q6 and associated resistors R1 - R8 and R11. The transmit output from pin ATO operates a push-pull driver stage consisting of Q1 and Q3, which in turn drives the output stage Q2 and Q4. Transistors Q5 and Q6 serve to disable the output stages when the device is in receive mode, preventing them from loading the receive signal input, which is taken from the junction of R2 and R5, via R9, to the receive input RAI (and also to PAFB, which is the power amplifier feedback input). The device is coupled to the power line via C1 and L1 (forming a simple band-pass filter) to the tuned isolating transformer, from whence it is coupled to the power line via the transformer secondary, and C2. TRL1 is a transient voltage suppressor, designed to protect the device from high voltage noise spikes on the power line. The master clock frequency is derived from quartz crystal QTZ1 and capacitor C3 and C4.

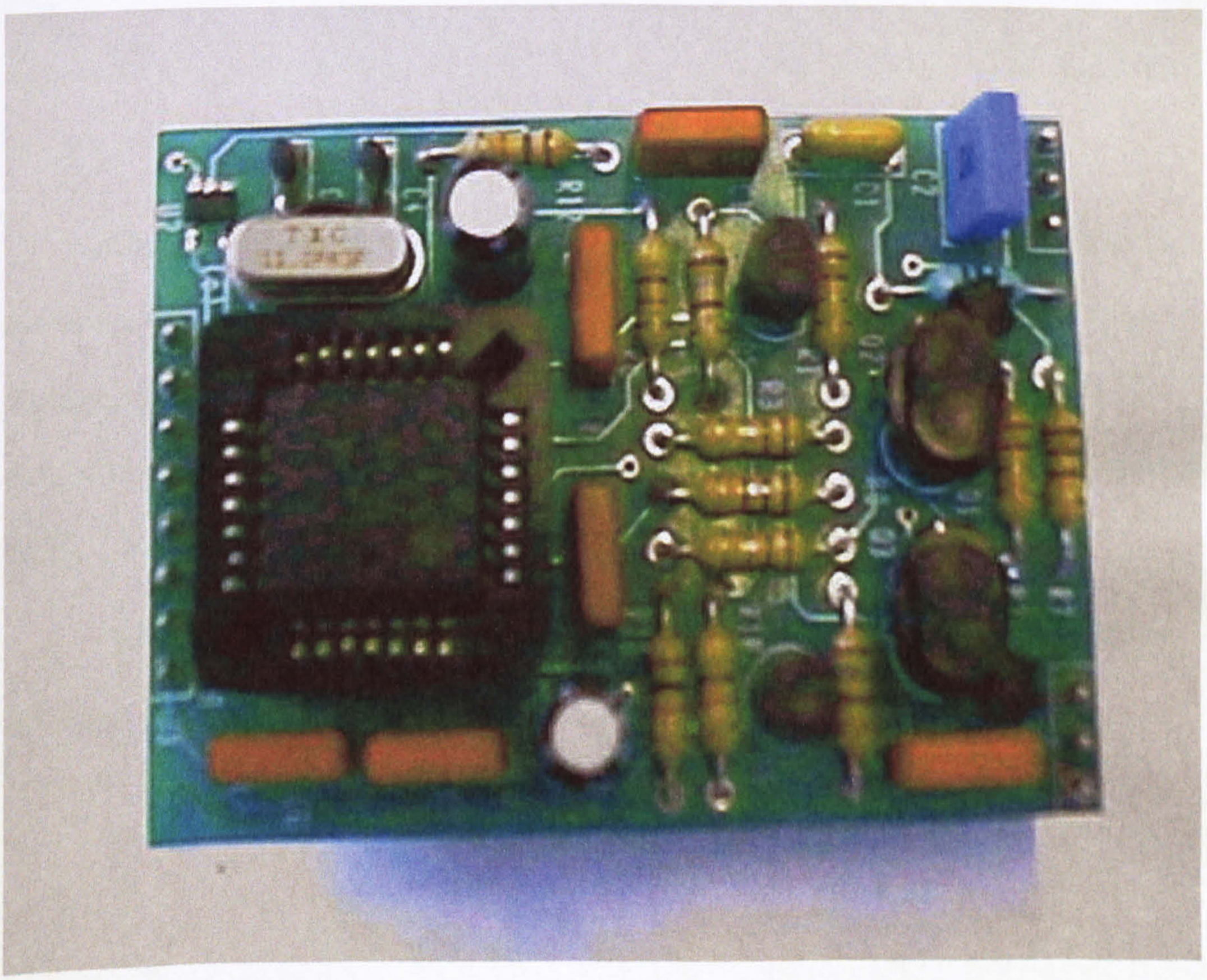


Figure 47: The ST7537 Power Line Modem PCB

The completed modem PCB is shown in the previous image. The modem IC can clearly be seen (on the left-hand side), along with the master clock crystal above it. The power amplifier stage transistors and associated components can be seen on the right.

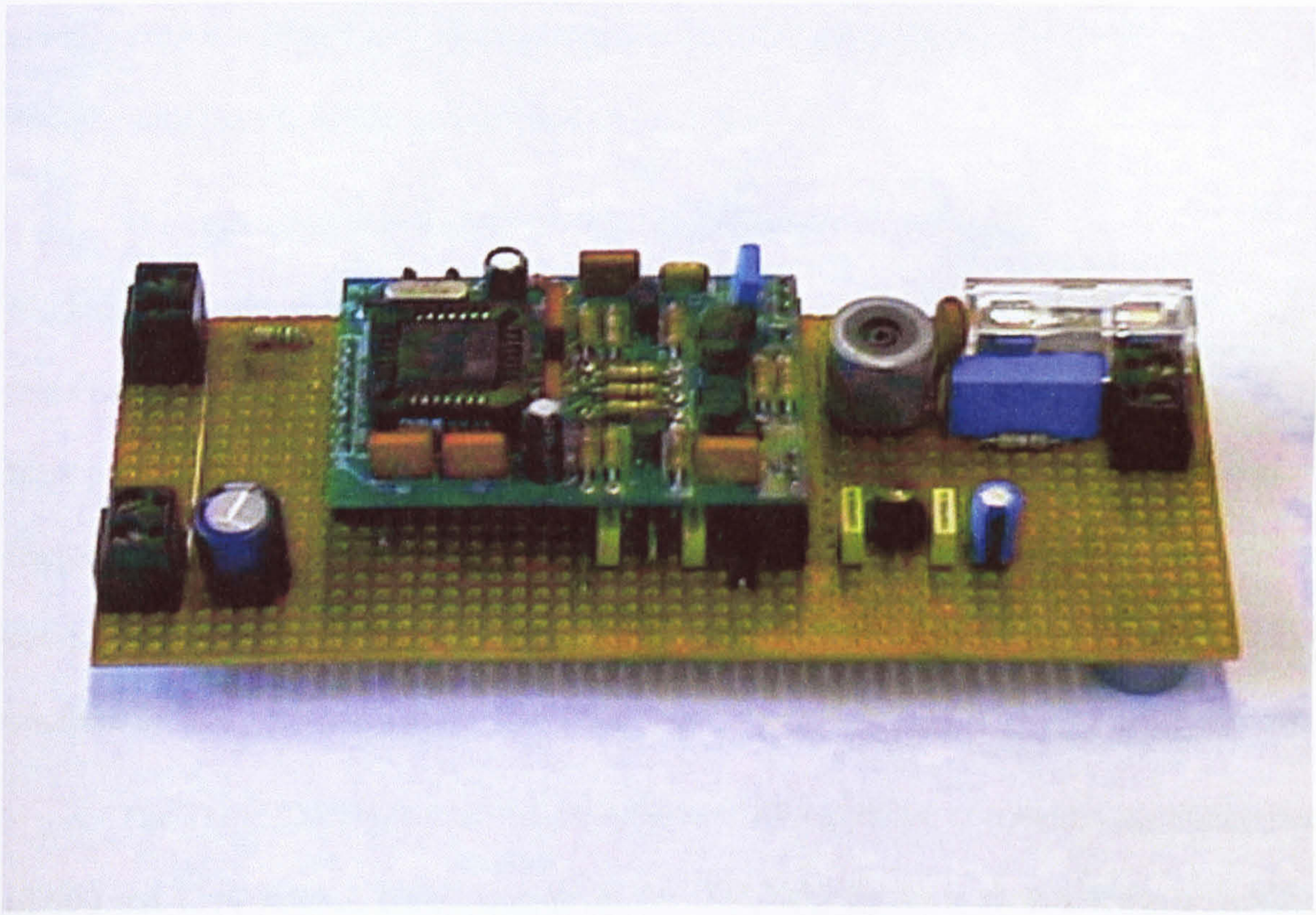


Figure 48: The ST7537 Assembly

The above image shows the modem PCB on its 'motherboard'. This board carries the power line isolation transformer and coupling capacitors (visible top right) and also voltage regulators and associated capacitors to provide the +10 V and +5 V supplies required by the modem circuit (these are visible to the right of, and underneath, the modem PCB).

Two of these motherboard assemblies were built, one configured as a transmitter, the other a receiver.

7.4 A Description of the TDA5051 ASK Modem

The second modem to be evaluated is based on the Philips TDA5051 IC [44]. This device is an ASK modem, manufactured by the Philips company. It too is designed to comply with EN 50065, and when working at a carrier frequency of 132.5 kHz would comply with the EN 50065 access band arrangement.

The evaluation boards used for this PL modem were supplied by Michat Electronique, in France [55]. It should be noted, however, that the boards utilised in these experiments operate, as supplied, at a carrier frequency of 115 kHz. It would have been possible to shift the frequency to 132.5 kHz by utilising a different master oscillator frequency (8.48 MHz instead of 7.37 MHz). However, it was decided by the author that the results obtained would not be likely to vary significantly, and so the modems were left unaltered.

The TDA5051 is rated by the manufacturer for operation at nominal signalling rates of 600 and 1200 baud. A block diagram of the TDA5051 device is shown in the following figure.

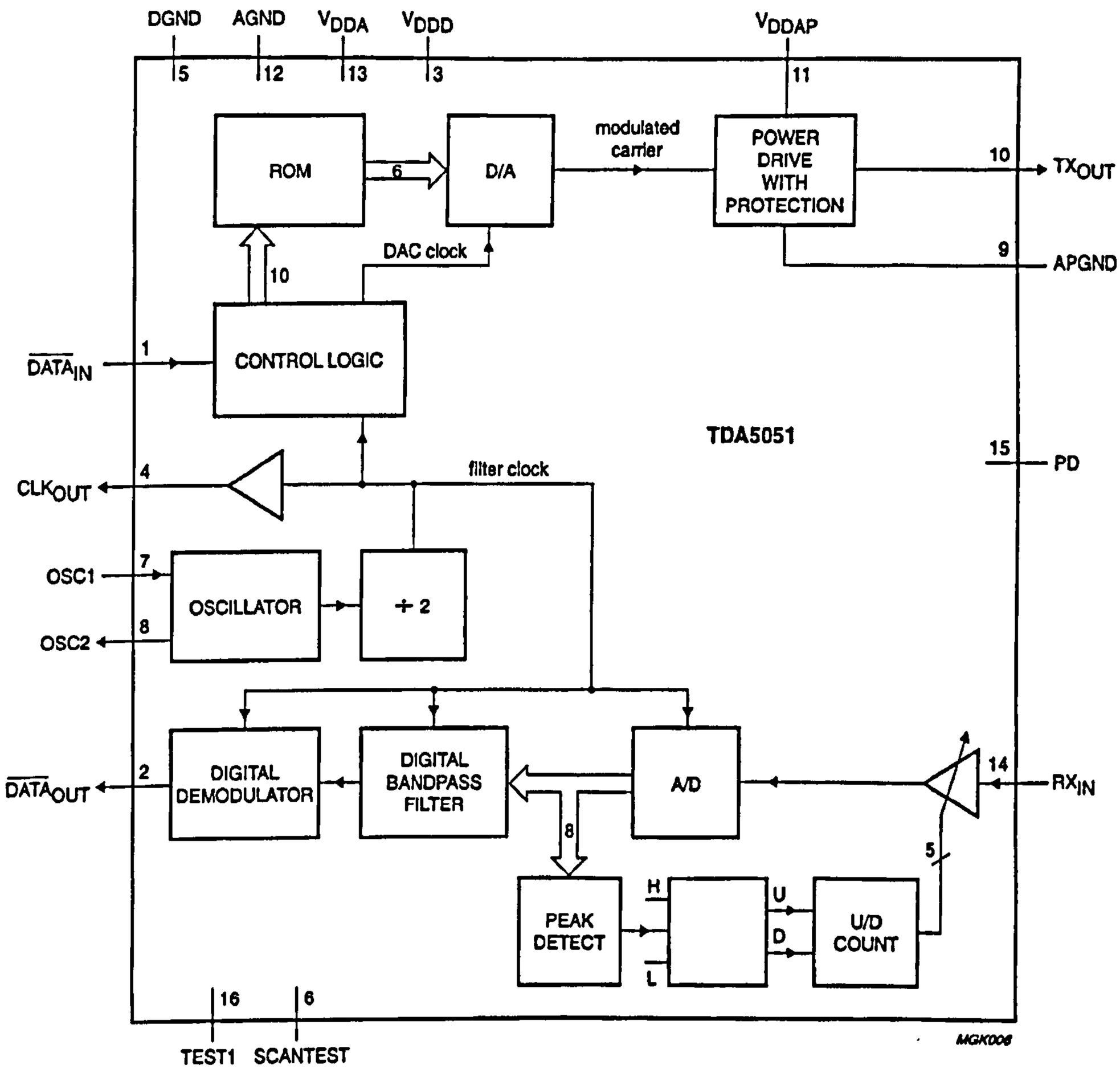


Figure 49: Block Diagram of the TDA5051 PL Modem IC

7.4.1 The TDA5051 Transmit Path

The carrier frequency in the TDA5051 is derived from a master clock of 7.37 MHz, by a process of sine wave table synthesis, to produce a carrier frequency of 115.16 kHz. The output from the sine-wave look-up table passes to a D-A converter and is then amplified by the on-board PA stage. Keying of the transmit carrier is carried out at the wave table synthesis stage, and permits precise control of the waveform attack and decay characteristics, to minimise the risk of out-of-band harmonic generation.

7.4.2 The TDA5051 Receive Path

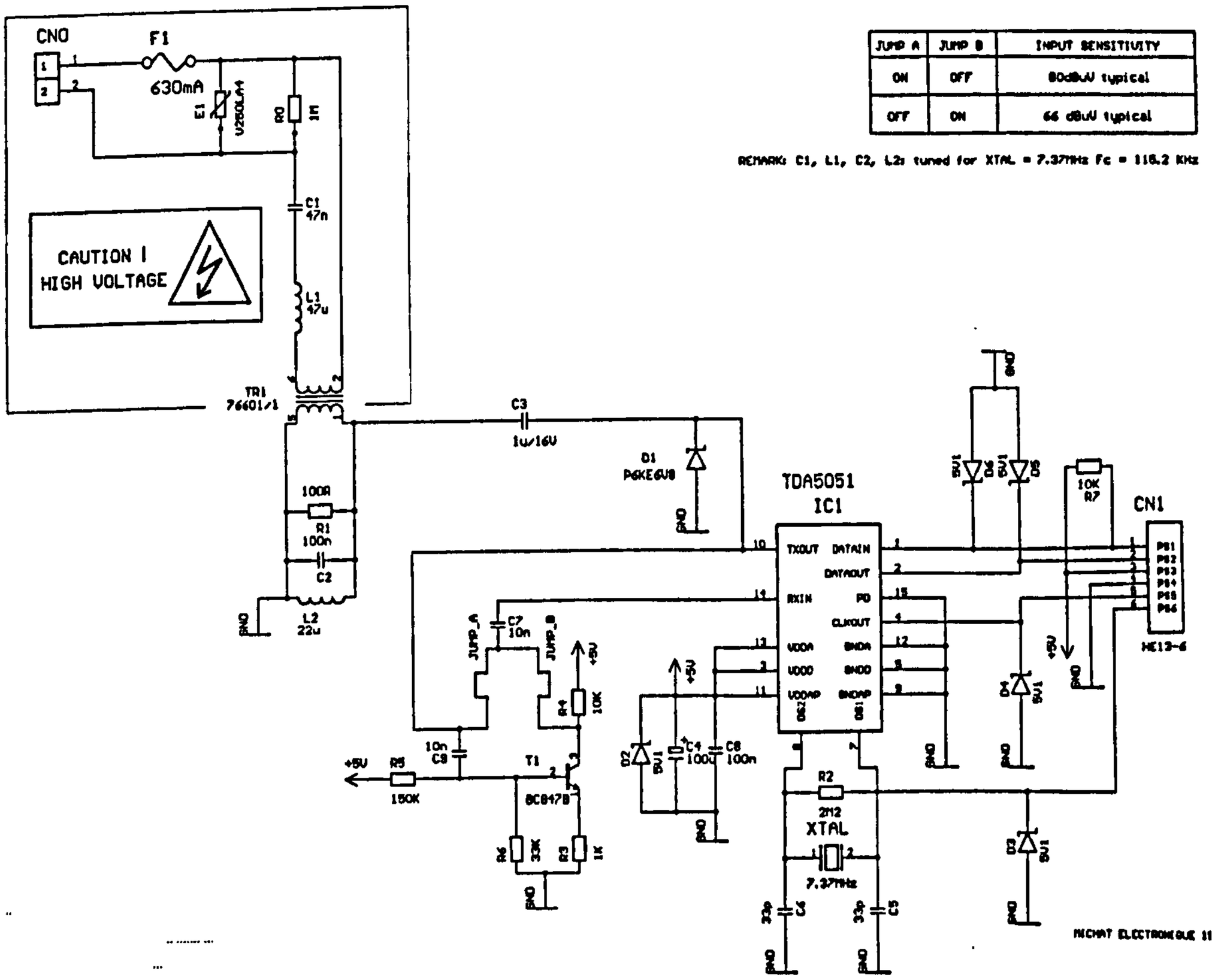
The receive path of the TDA5051 is also largely based upon digital techniques. After passing through a variable gain pre-amplifier stage, the signal is digitised in an A-D converter. This is filtered in a digital band-pass filter and detected by a digital demodulator. There is also a peak detector driven off the A-D output, which is used to set the gain of the pre-amplifier stage, termed 'automatic gain control' (AGC).

The receive stage is active, even when the device is transmitting. Therefore, in order to prevent the pre-amplifier AGC system from responding to the high level transmit signal, the TDA5051 stores the last set gain value before transmission starts, and restores it after transmission is finished.

Since this is an ASK device, switching between transmit and receive mode is achieved by setting the $DATA_{in}$ pin (pin 1) to a logic '1' (representing the 'no carrier' state for the transmitter).

7.4.3 The TDA5051 Support Circuitry

The modem design utilised in these experiments is also based on the manufacturers recommended application circuit, and is shown in the following diagram.



JUMP A	JUMP B	INPUT SENSITIVITY
ON	OFF	80dBuV typical
OFF	ON	66 dBuV typical

REMARK: C1, L1, C2, L2: tuned for XTAL = 7.37MHz Fc = 115.2 KHz

Figure 50: Circuit of the TDA5051-based Modem

It can be seen that this design requires somewhat fewer support components than the ST7537, largely due to the integrated power amplifier stage. The crystal master oscillator can be seen, as can the power line isolation circuitry. Where mains voltage isolation is not a requirement, the TDA5051 can be directly connected to the power line using a simple combination of L and C coupling components.

This design is also provided with an optional external pre-amplifier stage, consisting of T1 and its associated components.

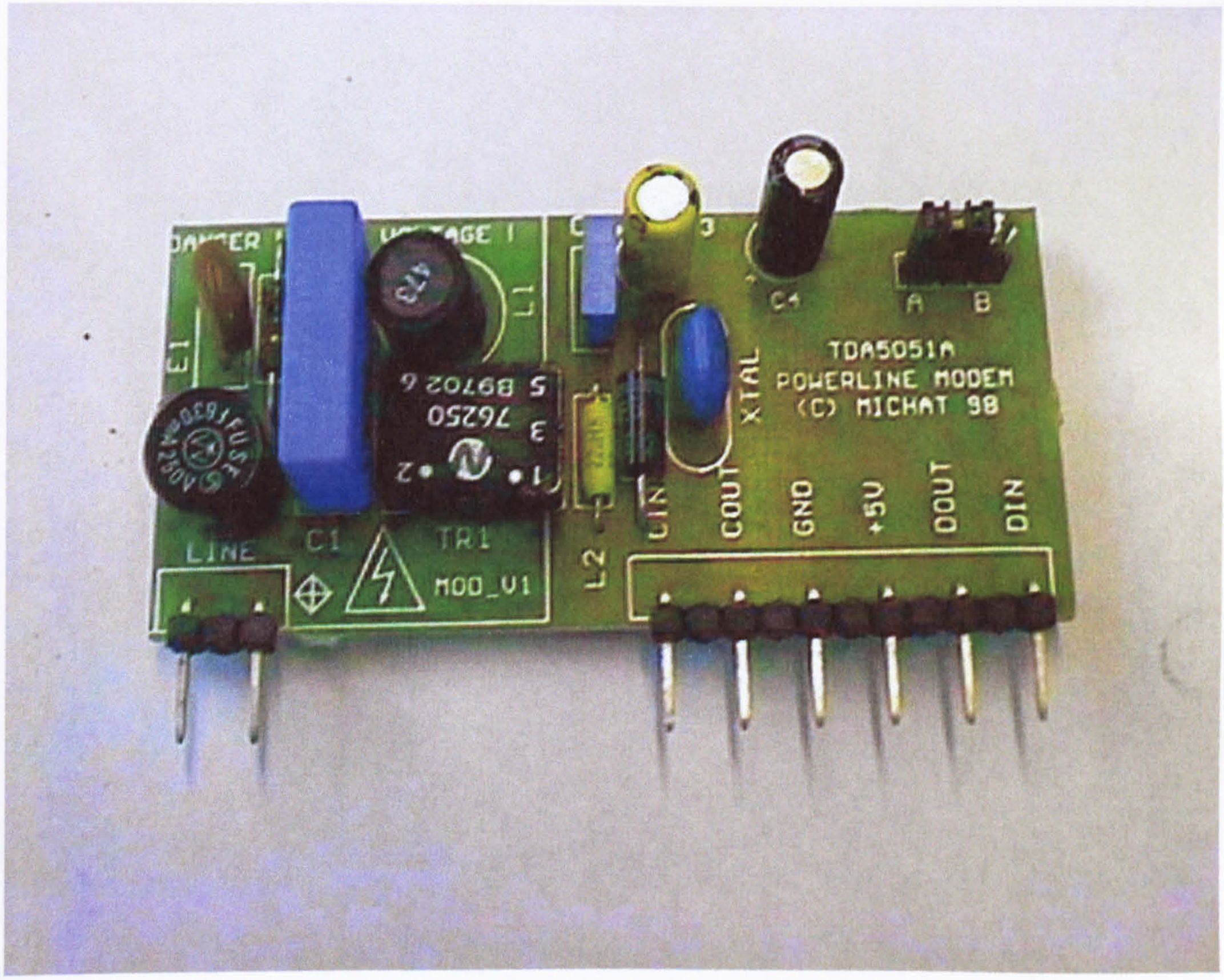


Figure 51: The TDA5051 Power Line Modem PCB (front view)

The above photograph shows the complete PL modem assembly. Clearly visible is the isolation transformer (TR1) and associated power line coupling components, the master clock crystal (XTAL), and the links ('A' - 'B') which permit the external pre-amplifier to be selected.

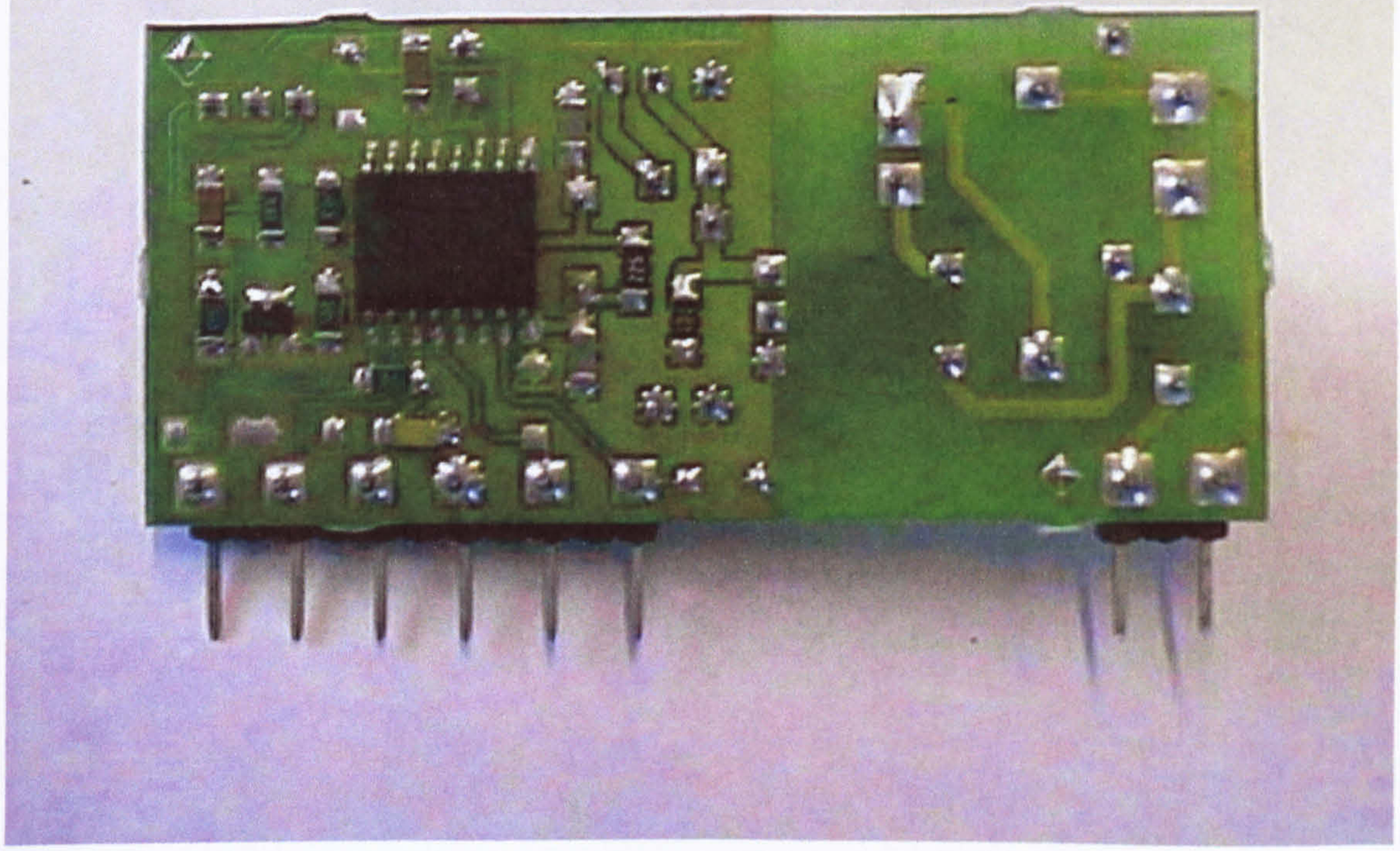


Figure 52: The TDA5051 Power Line Modem PCB (rear view)

Here we have the rear view of the same modem PCB. This time the surface-mounted TDA5051 IC itself can be seen, as well as various surface mounted support devices. The external pre-amplifier transistor (T1) can just be seen as the small three-pin device to the lower left side of the TDA5051.

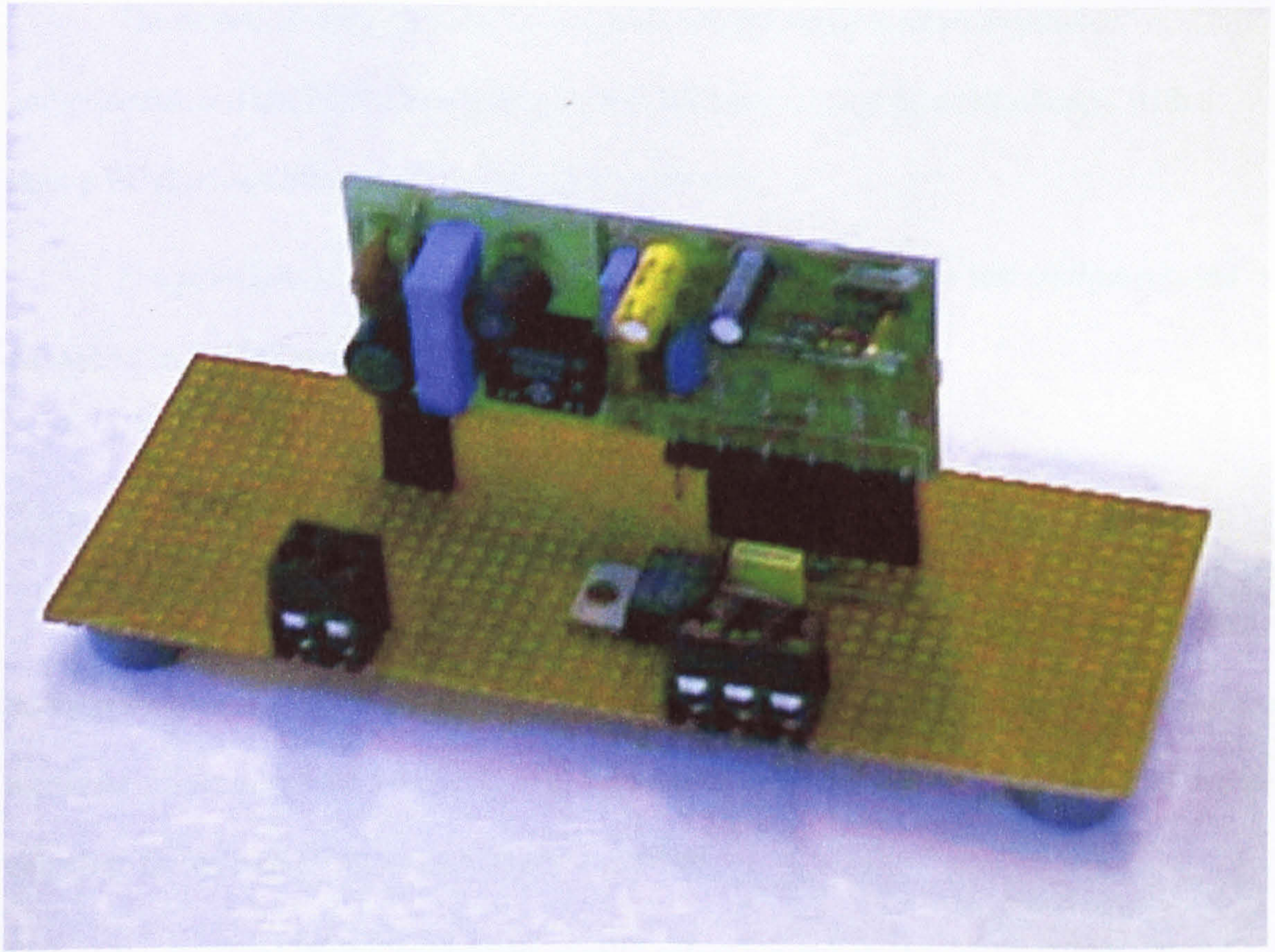


Figure 53: The TDA5051 Assembly

The above image shows the modem PCB on its 'motherboard'. It can immediately be seen that this is much simpler than the assembly for the ST7537. The only external components are a voltage regulator and associated capacitors, to provide the single +5 V supply required by the modem circuit. Again, two of these were built, one configured as a transmitter, the other a receiver.

Having introduced the PL modems that we will be evaluating in these experiments, we will next describe the development of the bit-error-rate test equipment itself.

7.5 Development of the Bit-Error-Rate Test (BERT) Equipment

Whilst BER test equipment is available in commercial form, such equipment was not available to the author. It was therefore decided to generate a custom-built item specifically geared up to performing the experiments in this thesis.

The author is familiar with the use and programming of microcontroller components, and the BER test equipment will be based around this technology, with a laptop PC used to collect and store the data generated.

The principle of operation and hardware development of this test equipment will be described in the following sections:

7.5.1 Principle of Operation of the BERT

The principle of a bit error rate tester (BERT) is to generate a test bit stream, pass this stream over the communications medium (whatever form it may take) and monitor the received bit-stream at the other end. Any incorrectly received bits will be noted and use to calculate the overall BER, as previously described.

Commercial BERT equipment usually offers a number of options as regards the structure of the test data stream. These, for example, might simulate data packets for a particular protocol. Another common option is a random bit stream (or more usually 'pseudo random' - this distinction will be described shortly). This will simulate the operation of a generalised communications link with its unpredictable data.

To generate genuinely random data in an electronic circuit is not always simple. Such effects as electrical noise or radioactive decay are natural random events, but additional (and unnecessary) complexity is involved in using them in this context. In practice, what are called 'pseudo-random' data streams are usually acceptable.

The definition of pseudo-random can be stated as 'random, when sampled over a small to medium-sized interval, but ultimately repeatable'. A common means for the generation of pseudo-random data electronically is the 'shift-register with feedback' approach. Essentially, a serial digital shift-register of a certain length has 'taps' at several points along its length. The data present at these taps is combined in a gate arrangement to provide the source data for the shift register input. The pseudo-random data is read from the shift register contents. It is a simple task to implement such a generator as an algorithm within a microcontroller [56], and this is the approach which we have employed here.

A test bit-stream, as we require, can be obtained from the above arrangement by sampling one bit from any point within the shift register. A data stream at a particular signalling rate is simply derived by clocking the shift register at that rate.

Having generated our bit stream, we must feed it to one of the PL modems under test, configured as a transmitter. A simple 5 V logic level is all that is required, and this can be achieved simply from an output pin on the microcontroller.

The output from a second PL modem, this time configured as a receiver, feeds into an input pin on the microcontroller. The microcontroller firmware is then able to compare the transmitted and received bit-streams and ascertain if an error has occurred. The resultant data can be appropriately processed by the microcontroller, and then output to a laptop PC for storage.

We will now describe the actual hardware used in the BERT equipment.

7.5.2 The BERT Hardware

The BERT has two main components:

a) A microcontroller-based data generation/recovery unit, the function of which has already been described.

b) A laptop PC, running a specially written logging program, used for storage of the BERT data, prior to subsequent processing.

The first item is based around a member of the Arizona Microchip 'PIC' family of single chip microcontrollers, specifically the PIC16F84-04 [57].

This is a reduced instruction set computer ('RISC'), which means that it has a small, but fast set of internal operations. The 16F84 has 1024 14-bit words of flash program memory, in which our operating software is stored, 36 bytes of general-purpose registers, and 64 bytes of EEPROM data memory (not used in our application). The –04 version of the device operates at a maximum clock frequency of 4 MHz [57]. This particular part was chosen as the author has had previous experience in its programming and application.

The circuit of the data generation / recovery unit is shown in the next figure, and it can be seen that the final design is comparatively simple.

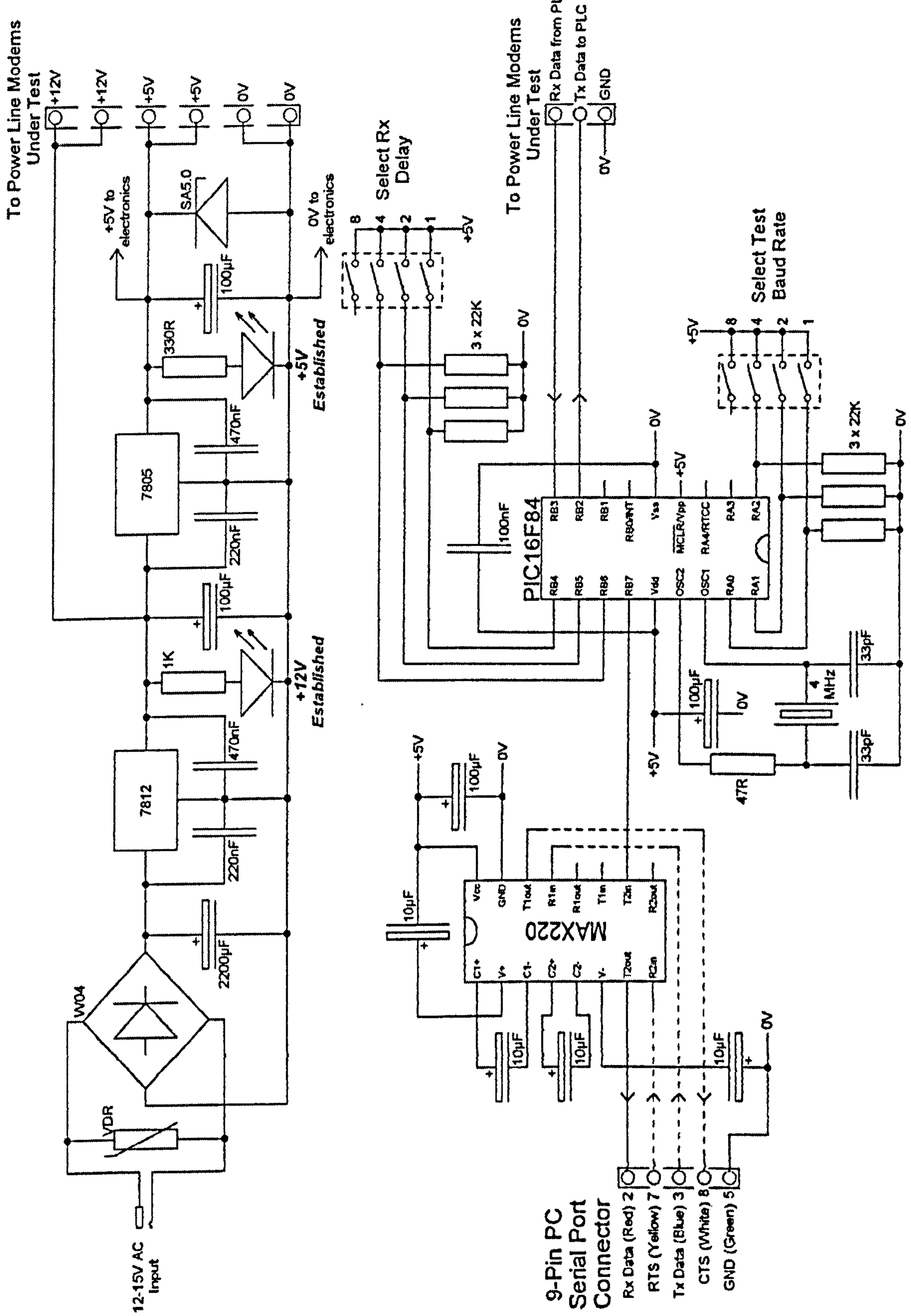


Figure 54: BERT Main Assembly Circuit Diagram

The PIC16F84 interfaces to two rotary BCD switches (SW1 & SW2) connected to I/O ports on the device. These are used to input two parameters pertinent to the BER test - the signalling rate for the test bit-stream, and the receiver delay (the purpose of this last parameter will be discussed in detail later).

The PIC16F84 outputs a bit-stream of pseudo-random data on pin 8. This is used to drive the power line modem transmitter under test via an opto-isolated interface (again, the reason for, and purpose of this extra circuit element will be described in detail later).

After the signal has passed through the transmission line, the corresponding power line modem receiver inputs data to pin 9 of the PIC16F84, again via an opto-isolated interface.

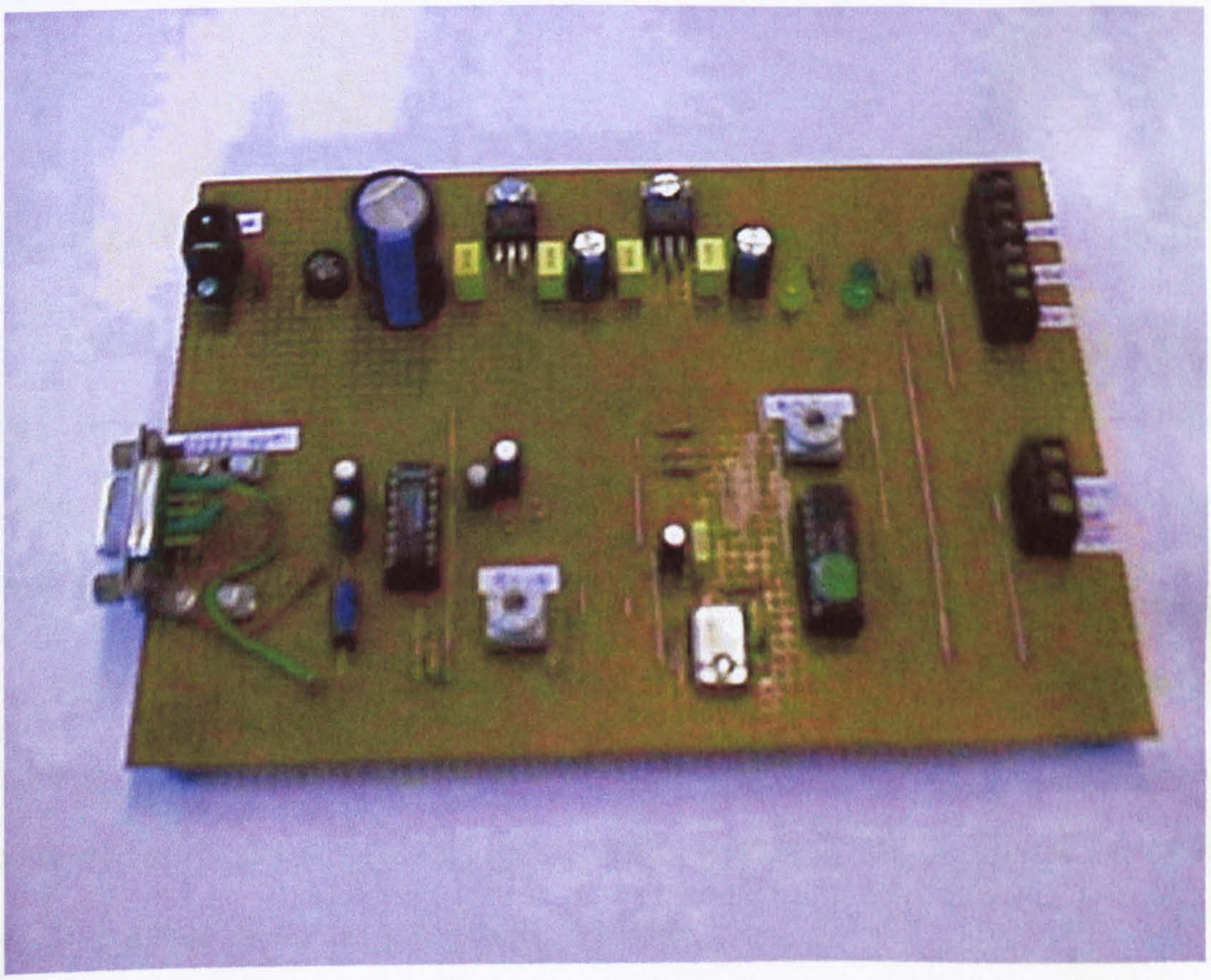


Figure 55: The BERT Hardware

The previous figure shows the actual BERT hardware, as built by the author. At the top of the circuit board can be seen the power supply components. The PIC16F84 microcontroller is in the lower right-hand side of the circuit board and the two BCD switches can be seen, one above, and one to the left of the PIC. The nine-way plug at the bottom left of the board, and the associated components to the right of it, is the RS-232 interface to the logging computer. The set of terminal blocks on the right hand side are the power and data connections to the opto-isolator circuits, which proved to be needed in practice, and the which will be described in the next section.

The rest of the circuit simply consists of ancillary components such the power supplies and interference suppression circuitry. The main circuit requires 5V DC, plus additional isolated 5V supplies are required for the isolation circuits and PL modems themselves.

7.5.3 The Need for Signal Isolation

Early proving tests with the BERT showed that the main control circuitry was prone to be itself affected by the FTB pulse train, causing the front-end circuit to 'lock-up' and cease to send its data. This behaviour is ironic and in itself emphasises the importance of EMC immunity in modern electronic equipment.

Because of this, it was found necessary to electrically isolate the digital signal paths to and from the BERT device and the PL Modems under test, and circuits were developed to achieve this. The use of these isolators greatly decreased the effect. The circuits of the isolators, and their operation, will now be described.

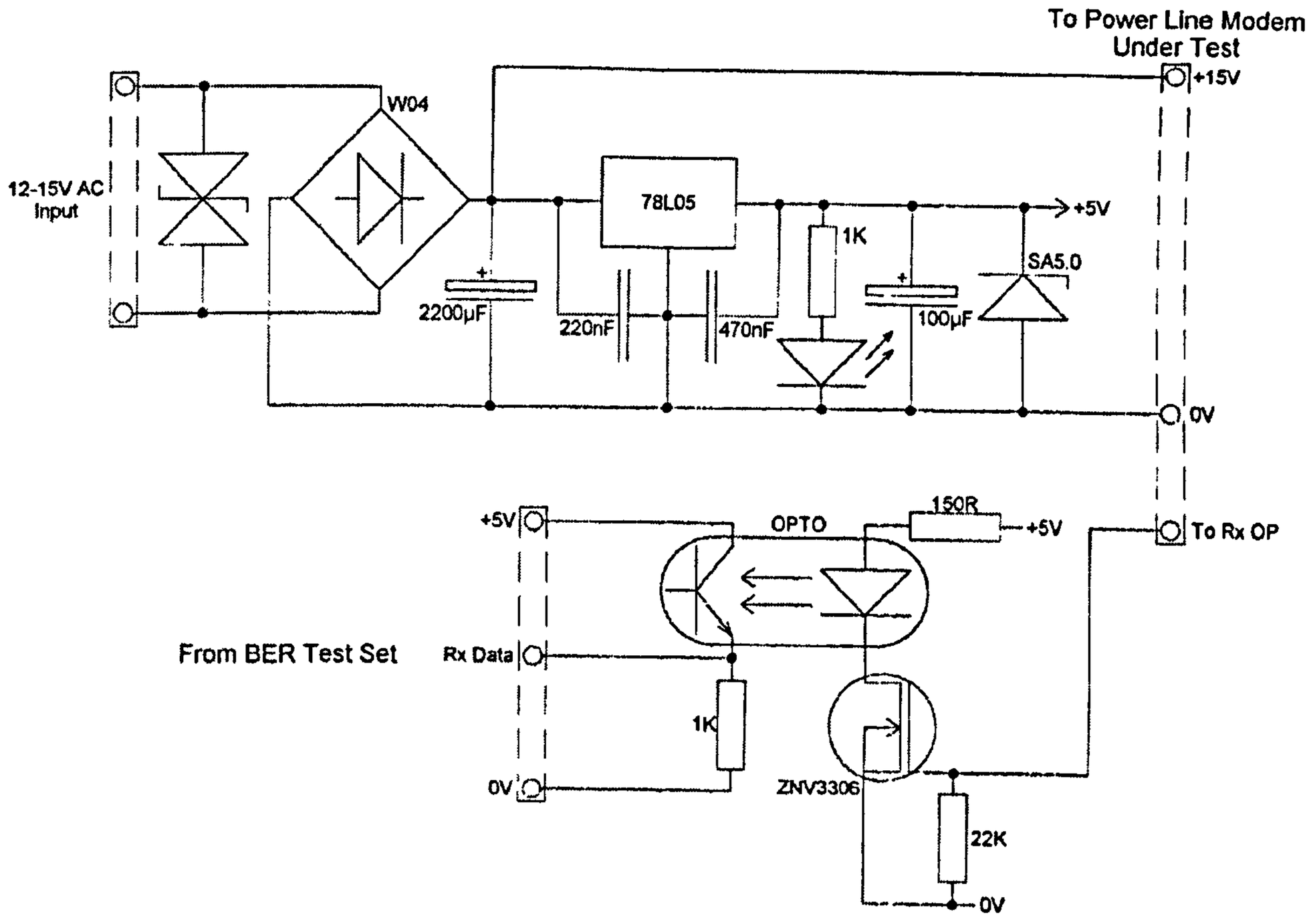


Figure 56: Receiver Isolator Circuit

The receiver isolator is simply based around a solid-state opto-isolator device (designated 'OPTO' in the circuit above). The output from the PL modem receiver operates the ZVN3306 transistor and switches current to the light emitting diode (LED) in the isolator. Power for this side of the circuit, including the receive PL modem, is provided by the voltage regulator and associated components at the top of the figure. The output of the isolator, in this case a phototransistor, switches an isolated 5V supply, provided from the main BERT equipment, across a 1K resistor, to provide a matching output logic bit-stream which is fed to the BERT.

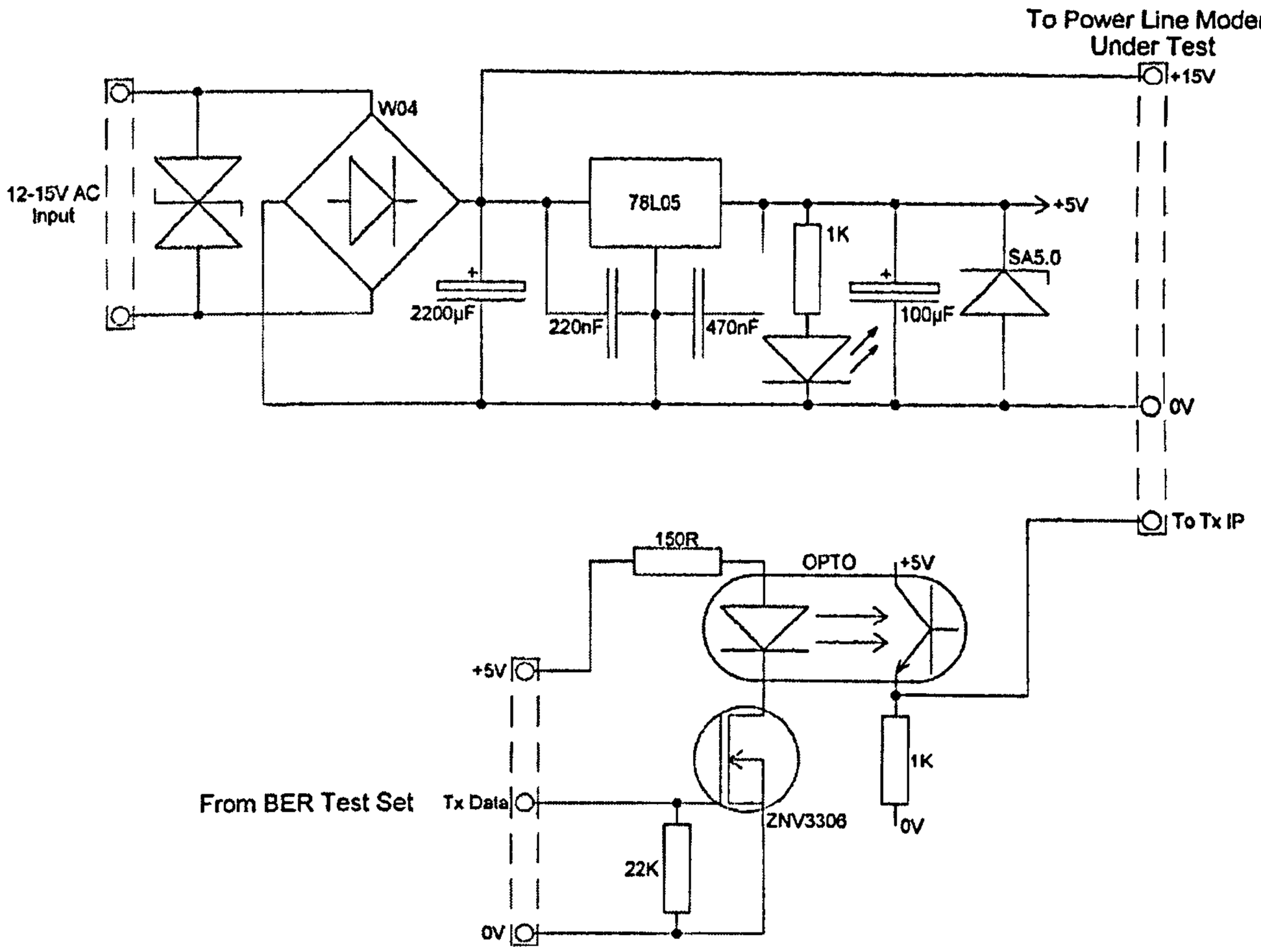


Figure 57: Transmitter Isolator Circuit

The transmitter isolator is virtually identical to the receiver, except that this time the transmit bit stream from the BERT operates the isolator LED, and the output from the phototransistor feeds the transmit PL modem

The processed data from the tester is output as a serial data stream, in RS-232 format, from pin 13 of the PIC16F84. This data is passed to a MAX232 voltage converter, which translates it to the standard RS-232 voltage levels of +12 V and -12 V.

This data is passed to the data-logging laptop PC over a serial cable, for storage and subsequent processing.

That ends our description of the front-end hardware. However, the heart of the front-end functionality is the internal firmware of the PIC16F84, the structure of which we will now describe.

7.6 The Structure of the BERT Front-End Software

The front-end software (listed in appendix 2) is split into two sections - the main body and the interrupt service routine. The interrupt service routine is driven off of the PIC16F84 internal hardware timer, set up to be clocked by the system clock. The timer is programmed to generate an interrupt signal at an interval of 208 µs. This period corresponds to a signalling rate of 4800 baud, and is the fundamental timing interval used within the entire controller.

7.6.1 The Interrupt Service Routine (ISR)

One of the tasks of the ISR is to handle the transmission of test results from the BERT equipment to the logging PC. There are hardware solutions to sending RS-232 asynchronous serial data, generally called 'Universal Asynchronous Receiver / Transmitters' (UARTs). Many microcontrollers integrate UART hardware onto the chip itself, however the PIC16F84 is not one of them.

Therefore, it was decided to utilise a 'software UART' to perform the transmission function. When the main routine (described later) wishes to transmit a data byte over the RS-232 link, it signals the fact to the ISR and passes the data by storing it in a register. The ISR processes this data, adding start and stop bits, at a rate of one bit per interrupt call, giving the overall transmission signalling rate of 4800 baud.

In addition, the BER test data is generated and processed by the ISR. By the use of a software prescaler, effectively dividing the interrupt rate still further, lower signalling rates than the fundamental 4800 baud can be easily obtained. In this instance we have the option of generating signalling rates of 4800, 2400, 1200, 600 and 300 baud, easily encompassing the specifications of the particular PLC modems under evaluation.

When the prescaler indicates that it is time for a new bit to be generated, a pseudo-random number generator routine is called. The least significant bit of the output word of this routine is used to determine the new state of the BER test output. The reasons for using a pseudo-random bit stream have been discussed earlier in this chapter.

Next, it is necessary to save the current BER test state for subsequent comparison with the received data. It was originally the intention to simply compare the input data with the output just prior to the output data being updated, however, after some early evaluation checks, a problem was noted.

7.6.2 Problems caused by Receiver 'Lag'

During early proving tests the ST7537 modem was observed to give high error rates above a certain signalling rate (600 baud), even under ideal link conditions. After some investigation, it was observed that there was a finite delay after a signal was received, before the receiver output changed state to reflect this. This delay was found by experiment to be about 800 µs. Only signalling rates of 600 baud or lower gave the receiver time to change state before the BER tester was sampling the output.

The cure for the problem was to introduce a delay function within the PIC16F84 software, storing the test output, waiting for the set time, then sampling the input state and comparing it against the stored state.

In practice, this was achieved by allocating a series of counters and bit stores within the PICs internal registers. Whenever the BER test routine was invoked, and the output bit changed, the software would look for a free counter. The selected delay value (read from input switches) would then be stored in the counter register, and the value of the output bit saved in the corresponding bit store.

7.6.3 Bit Error Rate Logging

At every pass through the interrupt routine, each counter in use would be decremented. When a counter reached zero, the stored output state (effectively delayed by 208 μs times the set delay value) would be compared with the current input state from the PLC receiver.

If the bit originally sent was a logic '1', but was incorrectly received as a '0', a 'high error' counter was incremented. If the bit originally sent was a logic '0', but was incorrectly received as '1', a 'low error' counter was incremented. In addition, counts were maintained of the total number of logic '1's and logic '0's sent.

NB. It should be noted that the delay routine as described is not ideal. The relatively large (208 μs) timing increments may mean that there is a risk of not sampling the input signal from the PLC receiver at the optimum point. This is especially true when the test signalling rate is set to its maximum value of 4800 baud. This could have been improved by increasing the interrupt rate, or by using an additional timer for this function. However, PIC16F84 only has a single timer available, and the speed of the processor used (4 MHz) does not allow accurate timing to be achieved at a higher rate. However the fact that, in practice, the particular PLC modems evaluated did not operate at rates above 2400 baud lessened the extent of this problem, so it was considered to be a reasonable compromise.

That ends our description of the operation of the interrupt routine. We will now describe the action of the main routine.

7.6.4 The Main Software Routine

After performing housekeeping jobs, such as initialising variables, hardware etc. the main program loop waits until one thousand BER test bits have been sent by the interrupt routine. It then saves the current value of the bit counts and error counts, before re-initialising the counters for another run (this means that a test bit stream is continuously generated, with no gaps). The main routine then proceeds to transmit the test data, at a signalling rate of 4800 baud, over the RS-232 link, to the host PC, whilst the generation of test data continues.

The data is transmitted as a stream of 16-bit binary values in the following format:

Data word #1	MSB	The binary word value representing the total number of low (0) bits sent in the last run.
	LSB	
Data word #2	MSB	The binary word value representing the total number of high (1) bits sent in the last run.
	LSB	
Data word #3	MSB	The binary word value representing the total number of low (0) bit errors detected in the last run.
	LSB	
Data word #4	MSB	The binary word value representing the total number of high (1) bit errors detected in the last run
	LSB	
Delimiter bytes	13 (decimal)	(see text for a description of the function of the delimiter bytes)
	10 (decimal)	

Figure 58: Structure of a Data Packet sent from the BERT

The two byte 'delimiter' values of 13 and 10 (decimal) are equivalent to the 'carriage return' / 'line feed' (CR/LF) pair of ASCII control characters. The purpose of these delimiter characters is to indicate the gap between two sets of data. The use of CR/LF is arbitrary - the only requirement should be that the characters chosen should not normally appear in the experimental data. The maximum value of any of the four data items being sent is going to be around 500 (decimal). The binary MSB values should therefore not exceed one, so CR/LF (with both values significantly greater than one, fits this bill (but equally there are many other suitable pairs!).

When the task of sending the data packet is complete, the main software routine then waits for the end of the next 1000 bits of test data, before repeating the above actions.

That concludes our description of the PIC16F84 firmware used in the BERT equipment. We will next describe the logging software used to collect the data.

7.7 The PC Logging Software

The software used to process and save the output from the BERT equipment was written in the High Level Language 'PASCAL', using the Borland Turbo PASCAL 5.0 Compiler. This language was chosen because the author already had some experience with it over the years.

The primary function of the logging software is to receive the data packets sent from the BERT equipment, as described above, and to store them onto a floppy disk.

At the same time, it was decided that the software should perform a certain amount of 'pre-processing' of the data, to facilitate later analysis of the data. This pre-processing was as follows:

- The binary data words sent from the BERT would be converted to their decimal equivalents, and sent in this form as ASCII numbers.
- Individual numeric values would be delimited by commas.
- Complete sets of four data words would be delimited by a CR/LF pair.
- Every ten sets of data, a time stamp would be added, to facilitate the identification of the extent of individual experimental runs within a single large block of results data.

The above formatted data is then in a suitable form for easy integration into word processing or spreadsheet programs for subsequent analysis.

In order to accept the data from the BERT equipment, the logging software must capture the data as it is received by the asynchronous serial port on the PC and write it to the floppy disk. This action must occur in real time, and concurrently. Therefore, whilst the action of writing a block of received data to the floppy disk is taking place, the software must continue to accept the serial data, saving it in a 'buffer' store until the previous disk write operation has finished.

In order to simplify the programming, and prevent 're-inventing the wheel!', the author made use of a ready made Turbo Pascal 'unit' (a collection of software routines which can be called by a user program) called 'Async4' [58]. This set of routines is 'freeware' and made available to users at no cost.

'Async4' provided all of the facilities required to handle the reception and buffering of data from the serial port. The rest of the logging program was mainly concerned with reading this data from the buffer, writing it to the floppy disk, and echoing it to the PC screen. Finally, a basic user interface, allowing the operator to start and stop the logging of the data, was provided. A listing of the main body of the logging software is provided in Appendix 3 of this Thesis.

In use, the BERT hardware was set up and started, then the logging software run on the PC. A series of experimental runs could then be carried out, with the operator noting the start and finish times of each using the on-screen time-stamps that form part of the saved data. When later analysing the results, the time stamps were used to identify the start and end of the data block for each experiment.

We will discuss the subsequent analysis of the data in a later section, next, though we will look at the actual experimental set-up.

7.8 The Experimental Setup

The experimental set-up used is shown in the following diagram. It should be noted that the set-up is not energised at mains voltages. This is not necessary as the characteristics of the mains supply are simulated by the use of a network, which we will describe later. Also, the need to measure our low level PLC signals against a high level (even if appropriate filters are used to attenuate it) 50 or 60 Hz signal are alleviated.

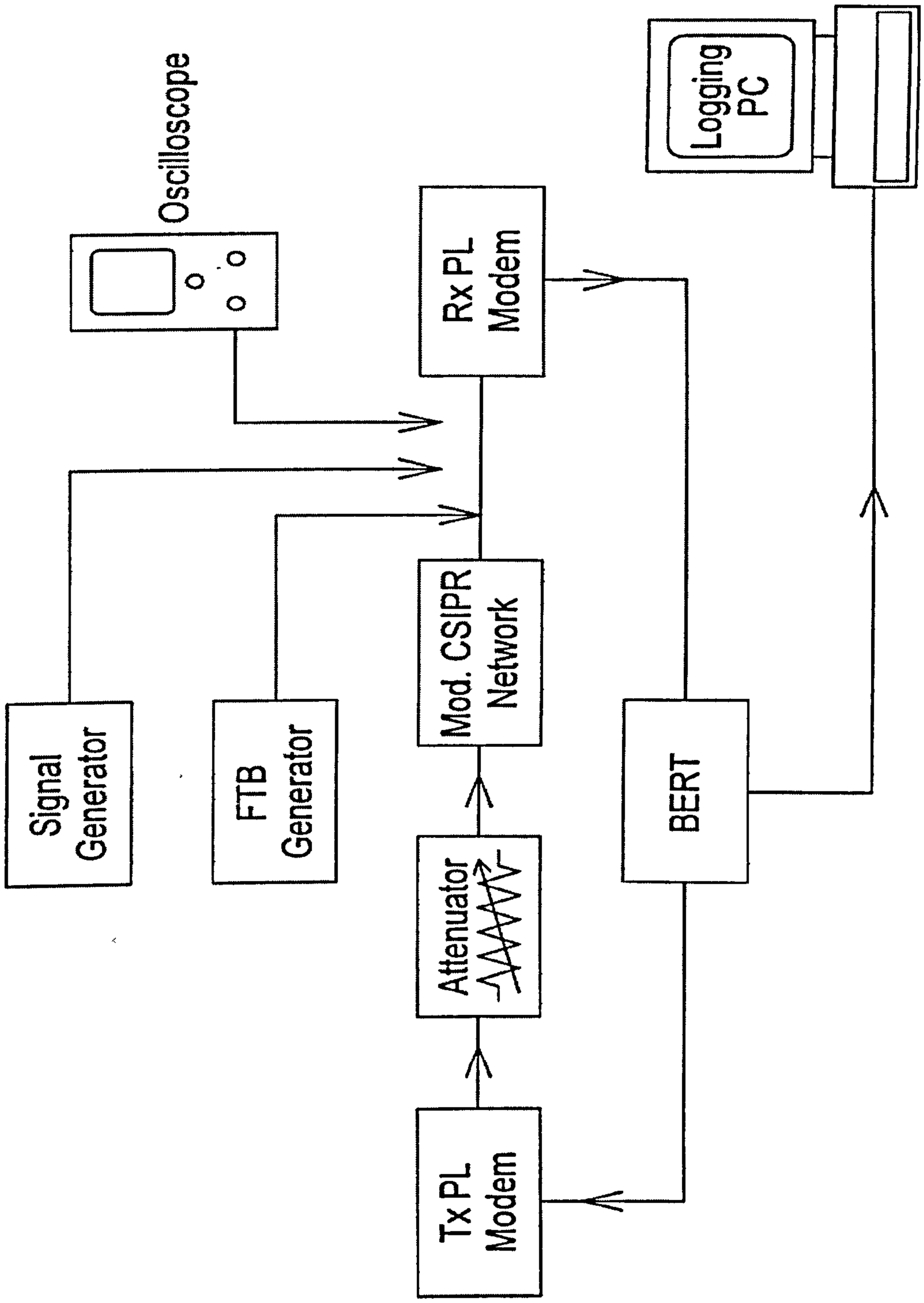


Figure 59: Block Diagram of the Experimental Set-up

The signals to and from the BERT equipment have already been described. We will now look at the purpose of the various components in the PLC signal path between the Transmit (Tx) modem and the Receive (Rx) modem.

7.8.1 The Signal Attenuator

The output bit stream from the BERT passes to the transmitter PL Modem. The output from this modem passes via a simple resistive attenuator, to allow the signal amplitude at the receiver to be varied, into the modified CISPR network (which will be described next).

The attenuator acts as a series element, in line with the impedance of the network itself, to form a potential divider. The actual magnitude of the resultant signal across the network is monitored using the oscilloscope. Although the impedance of the modified CISPR network varies with frequency, the relatively narrow bandwidth of the PL modem signals means that this will not cause problems. The arrangement therefore represents a good compromise and a simple means of varying the effective amplitude of the transmitted signal for our tests.

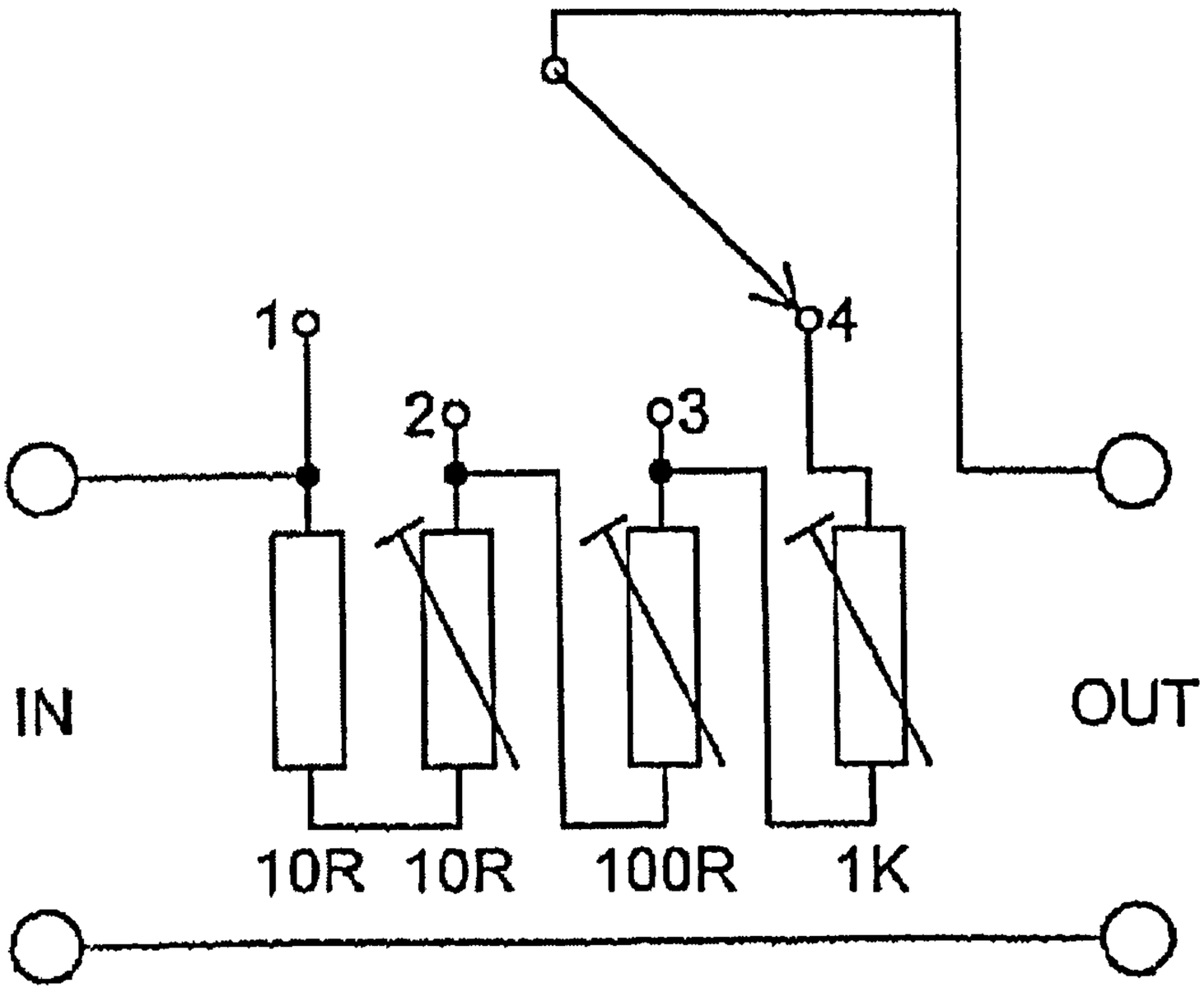


Figure 60: Circuit of the Attenuator Assembly

The actual circuit of the attenuator is shown in the previous figure. By selection of the appropriate switch position, and adjustment of the variable resistors, resistances of from zero ohms up to some 1120 ohms can be achieved.

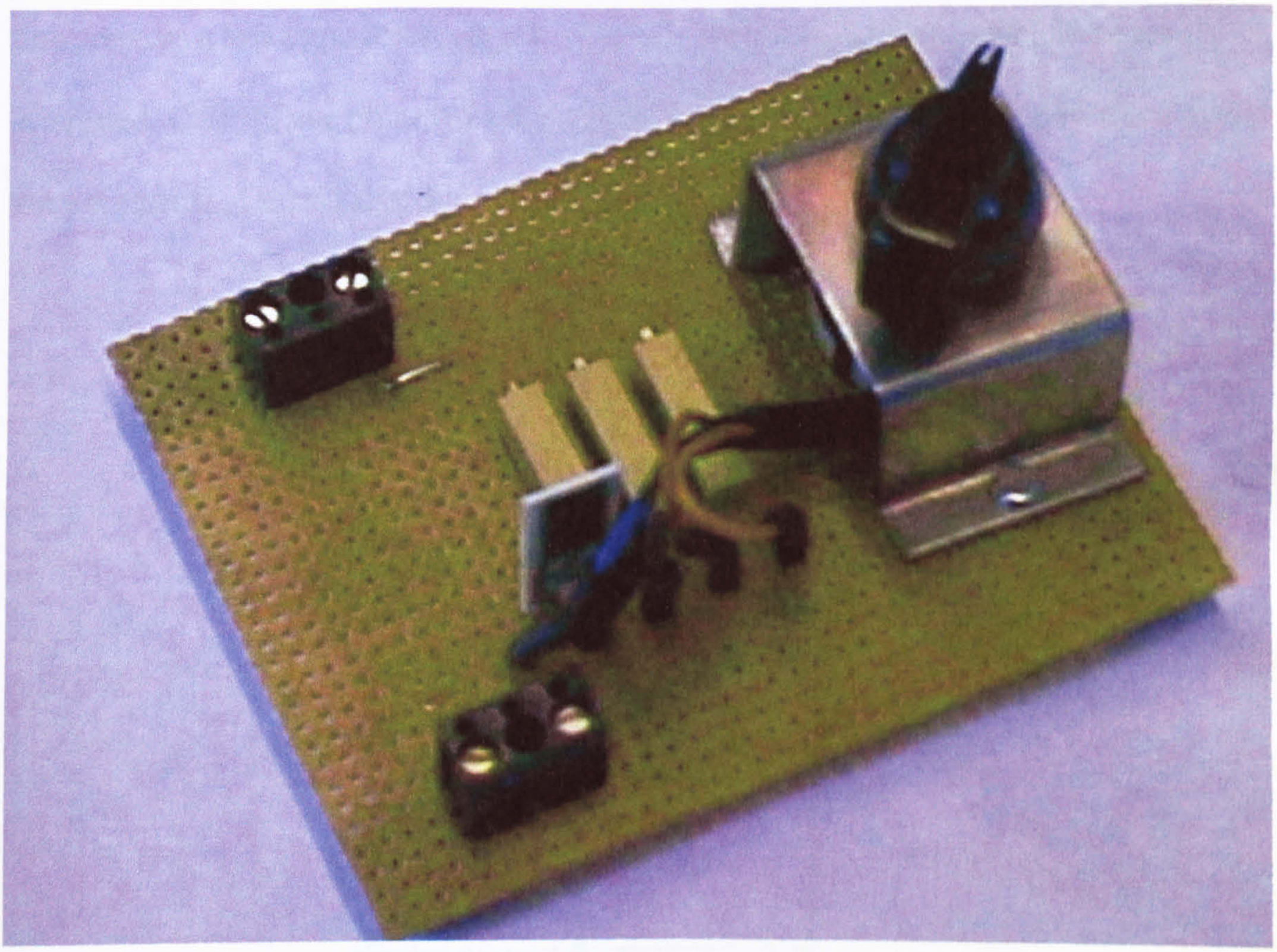


Figure 61: The Attenuator Assembly

The physical realisation of the attenuator is shown above. Clearly visible are the variable resistors and the thick film fixed resistor. Thick film resistors and linear element variable resistors were chosen so that the attenuator would present a pure resistive load with a minimum of inductive or capacitive effects, in deference to the frequencies of the PL modem signals.

The attenuator then feeds the mains simulation network, the structure of which we will describe next.

7.8.2 The Mains Simulation Network

This network is intended to simulate the actual impedance conditions found on a power line. We have already commented in a previous chapter on the fact that the power line presents a low impedance, especially at the carrier frequencies in which we are interested. CISPR have proposed a standards line impedance network for use when making measurements of mains signalling systems, which is shown below.

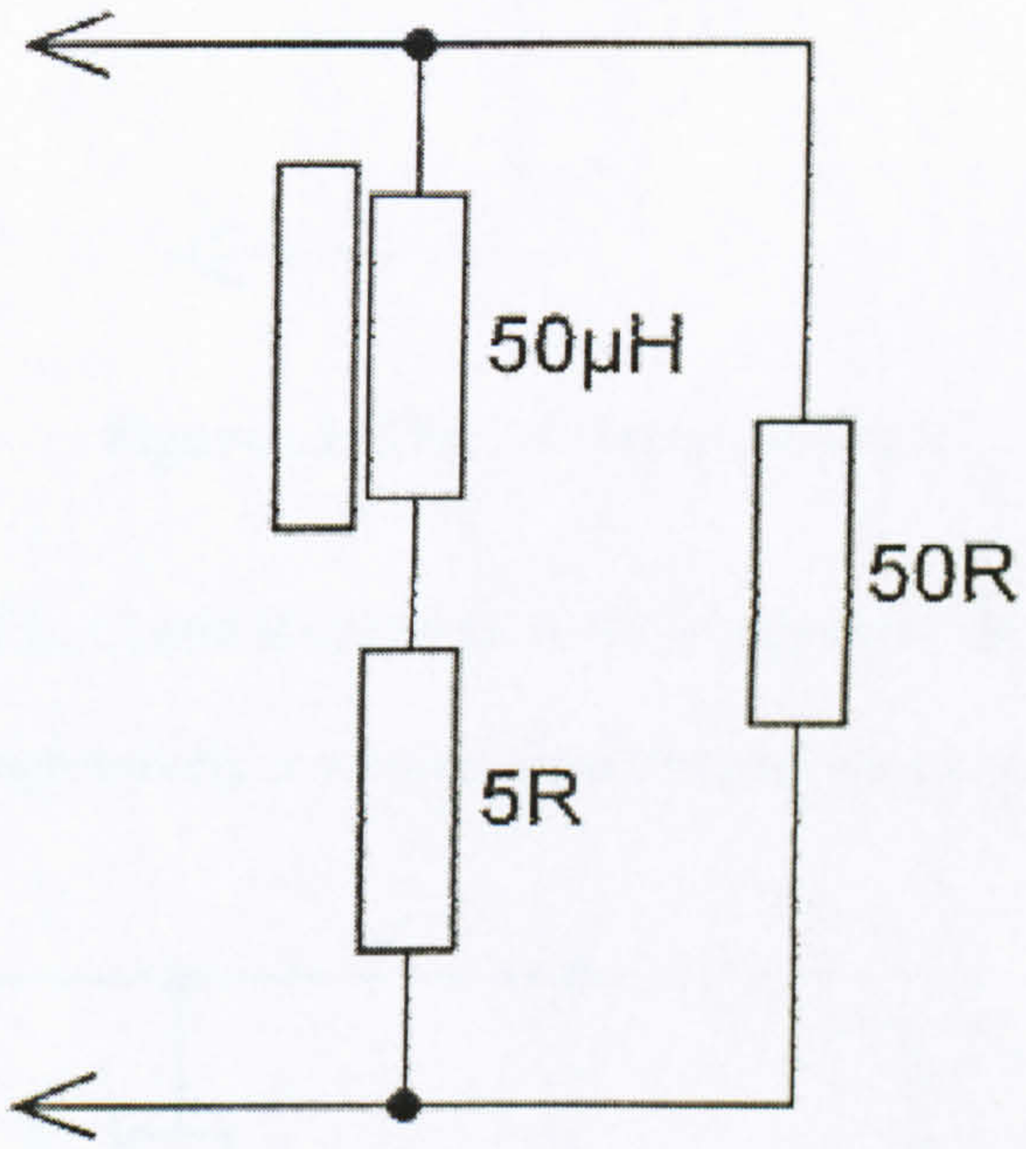


Figure 62: The CISPR Network

It can be seen that the above network is purely resistive/inductive in nature. Having an impedance at DC of a little below 5 ohms, the impedance will progressively rise as the frequency increases. At the frequencies that we are interested in, the network will have a relatively high impedance (approx. 32 ohms at 132.5 kHz), which will therefore not closely mimic 'real life'.

The French Company Moulinex have carried out work evaluating the potential of PLC applications [59], and CENELEC standard EN 50065, and have proposed a modification to the basic CISPR network to more closely approximate to a real mains power line. This modification is shown in the next diagram.

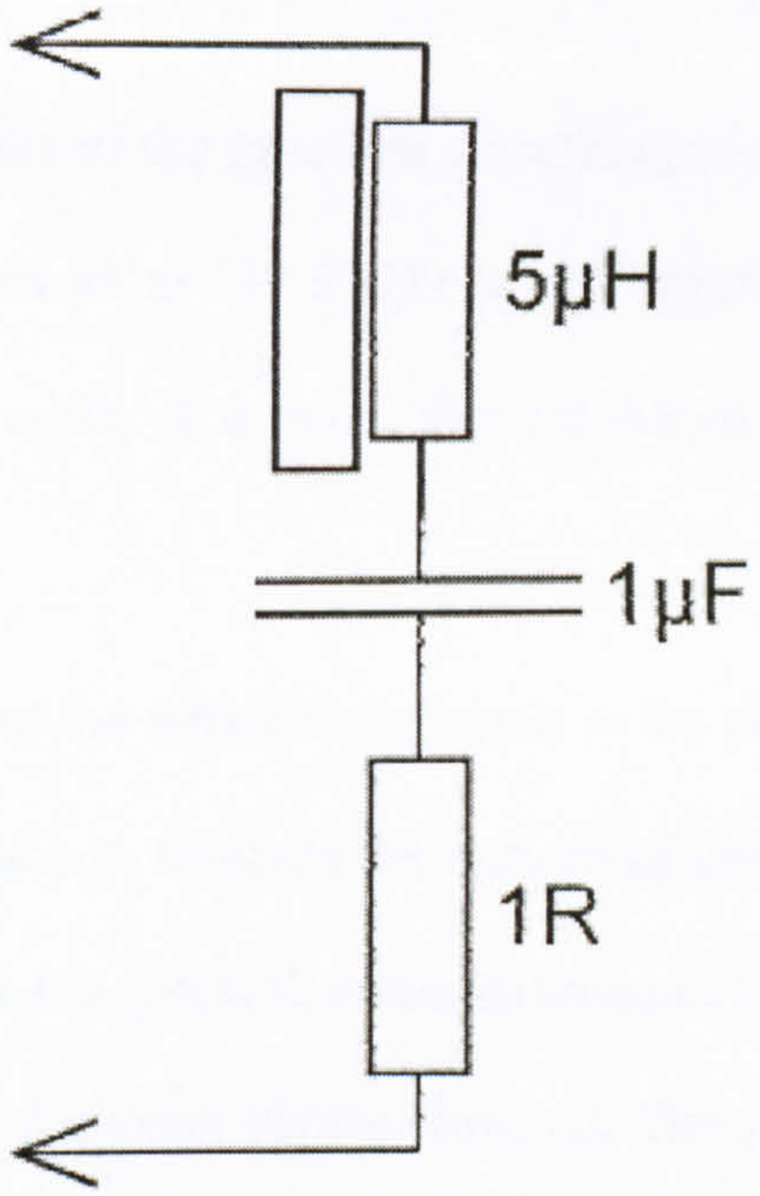


Figure 63: The Adaptive Network

The inclusion of L, C, and R elements in this adaptive network result in both a resonant peak, and a progressively lowering impedance as the frequency increases.

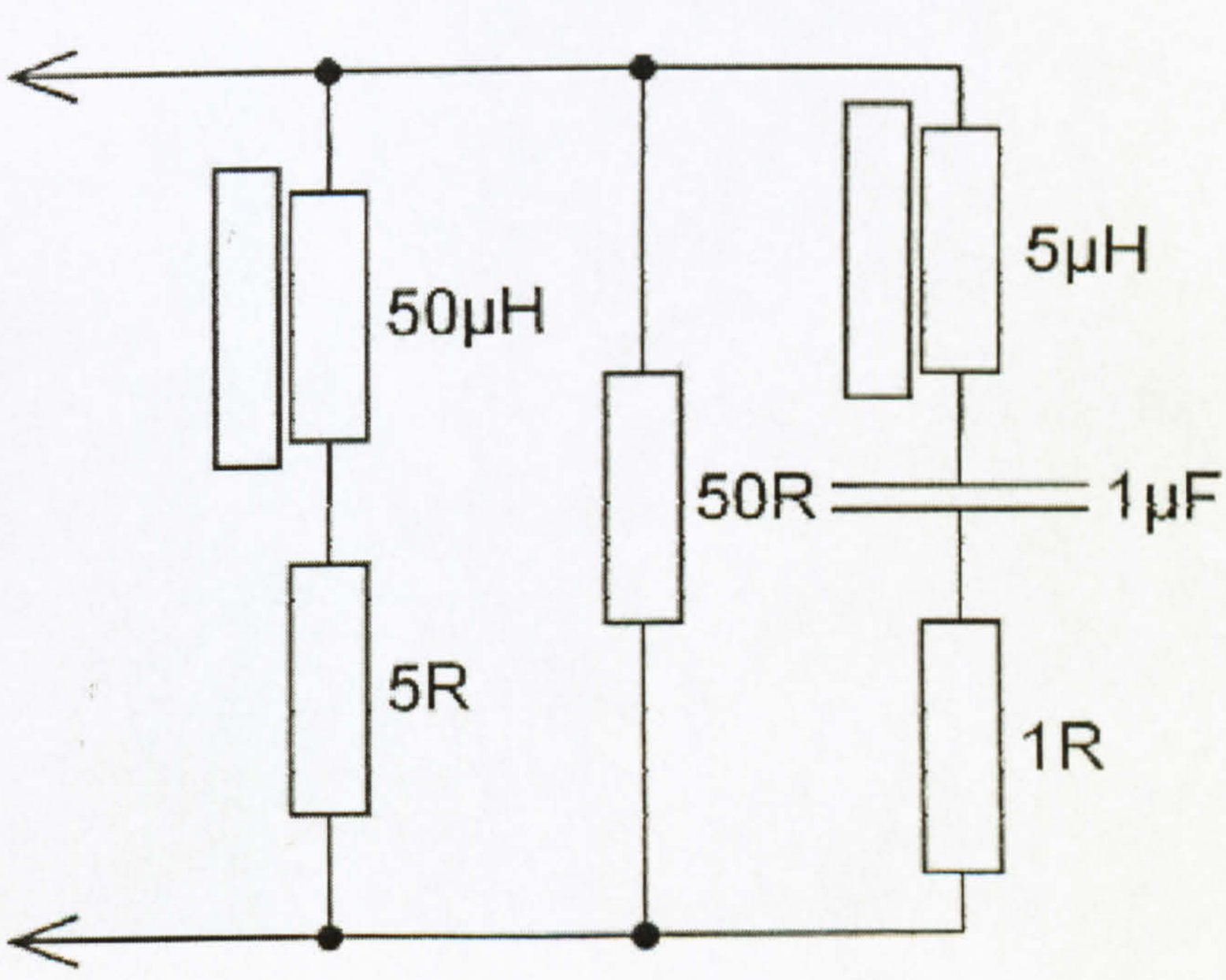


Figure 64: The Combined Network

The combined network, shown in the previous figure has an impedance curve that quite closely matches the results of the practical experiments carried out by Moulinex. The effective impedance of the network at 132.5 kHz is now approximately 3 ohms. Based on the findings of Moulinex, it was decided to use this combined network in the experimental work carried out in this thesis.

The actual realisation of the network is shown in the photograph below. The CISPR network consists of the components towards the bottom of the photo and the adaptive network the components at the top (NOTE: some inductances and resistances were placed in series or parallel to provide the exact values required. The switches visible enabled each part of the network to be disconnected if required.

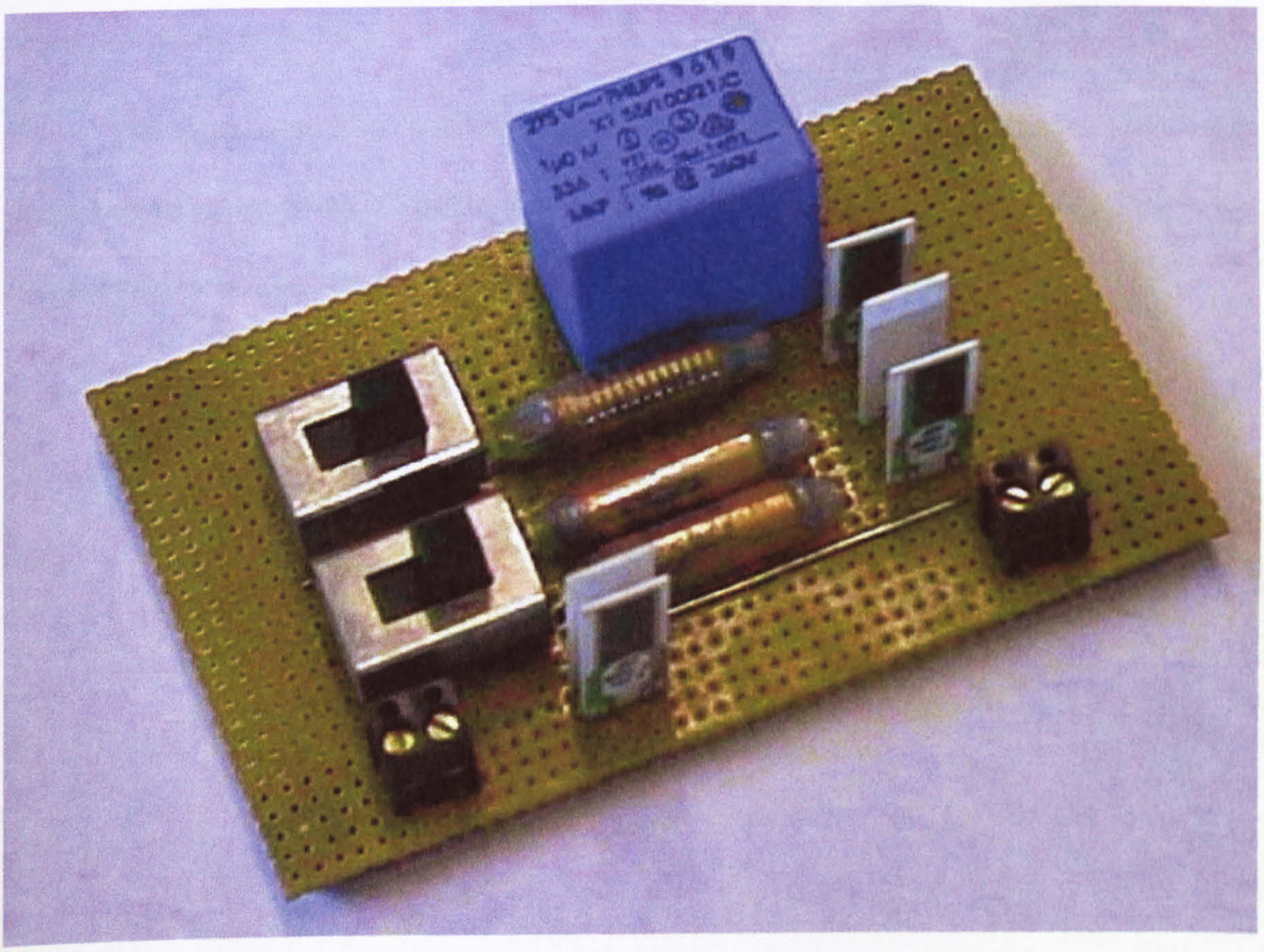


Figure 65: The Mains Impedance Simulation Network

The receiver PL Modem is connected across this network. The demodulated bit stream from the receiver is then passed back to the BERT. The RS-232 output from the BERT carrying the test results, as already described, passes to the logging PC.

7.8.3 The Fast Transient Burst Generator and Signal Generator

The FTB pulse train was provided by an item of commercial EMC test equipment - called a 'MACE', manufactured by Seaward Electronics in the UK. This equipment provides for other types of EMC-related test, such as mains drop-out and electrostatic discharge (ESD), but it was only the FTB facility that were used in these experiments. The MACE provides an FTB output either onto a mains supply, used when testing equipment immunity through the 'mains' port, or on an isolated output. This is for use with a 'capacitive clamp', for coupling the FTB onto signal lines from the equipment under test (EUT).

In our experiments, we used the latter output to feed the FTB signal into our simulated mains network.

The signal generator, used for spot frequency tests that we will describe later, was simply a general-purpose laboratory instrument, having a frequency range extending beyond the operational frequencies of the PL modems.

Photographs of the actual experimental set-up are shown next.

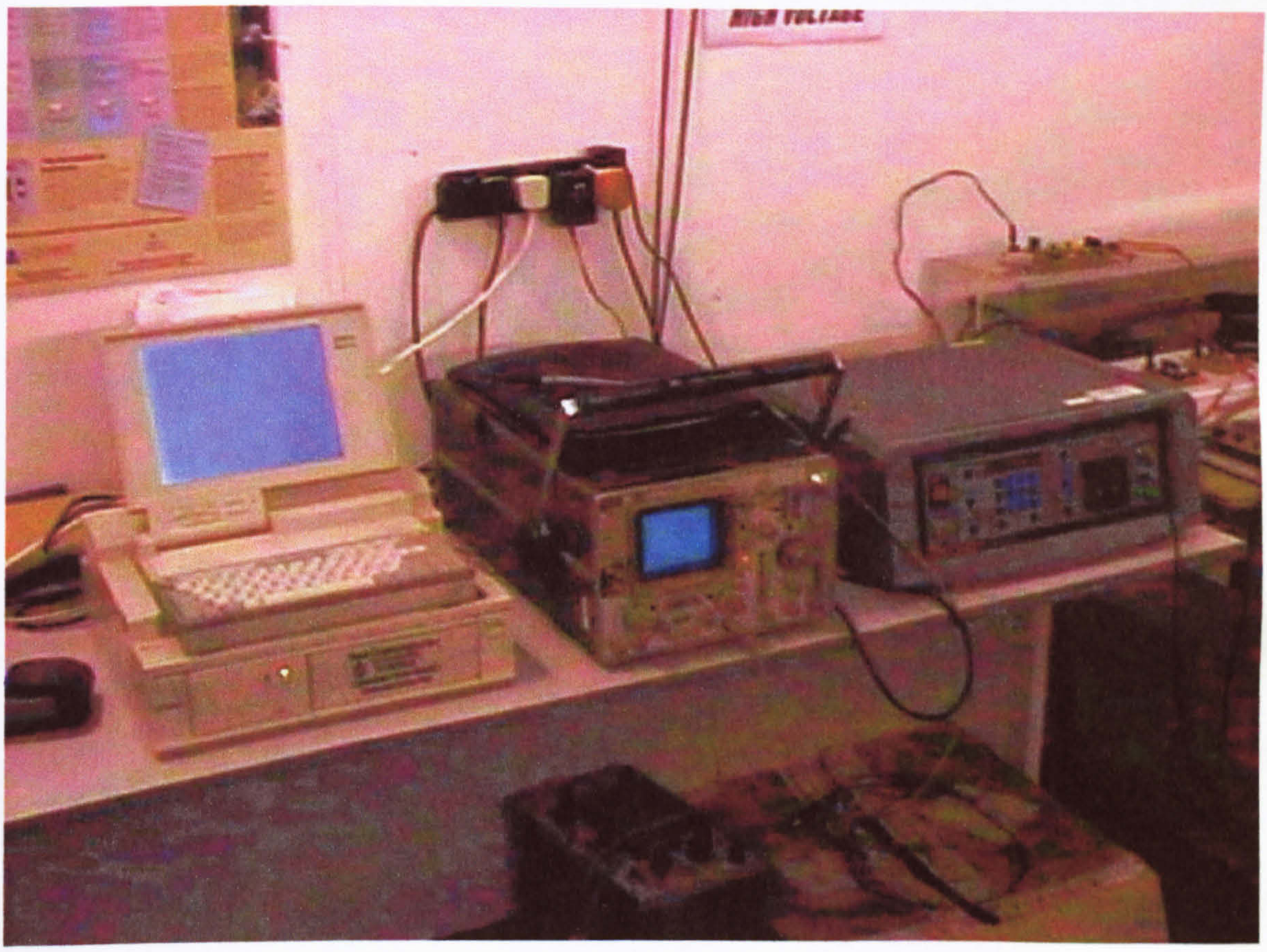


Figure 66: The Experimental Set-up in Real Life (#1)

On the left of the photograph the laptop PC used for initial data logging can be seen, next to it is the oscilloscope, used to measure waveform amplitudes, and on the right is the MACE Fast Transient Burst Generator.

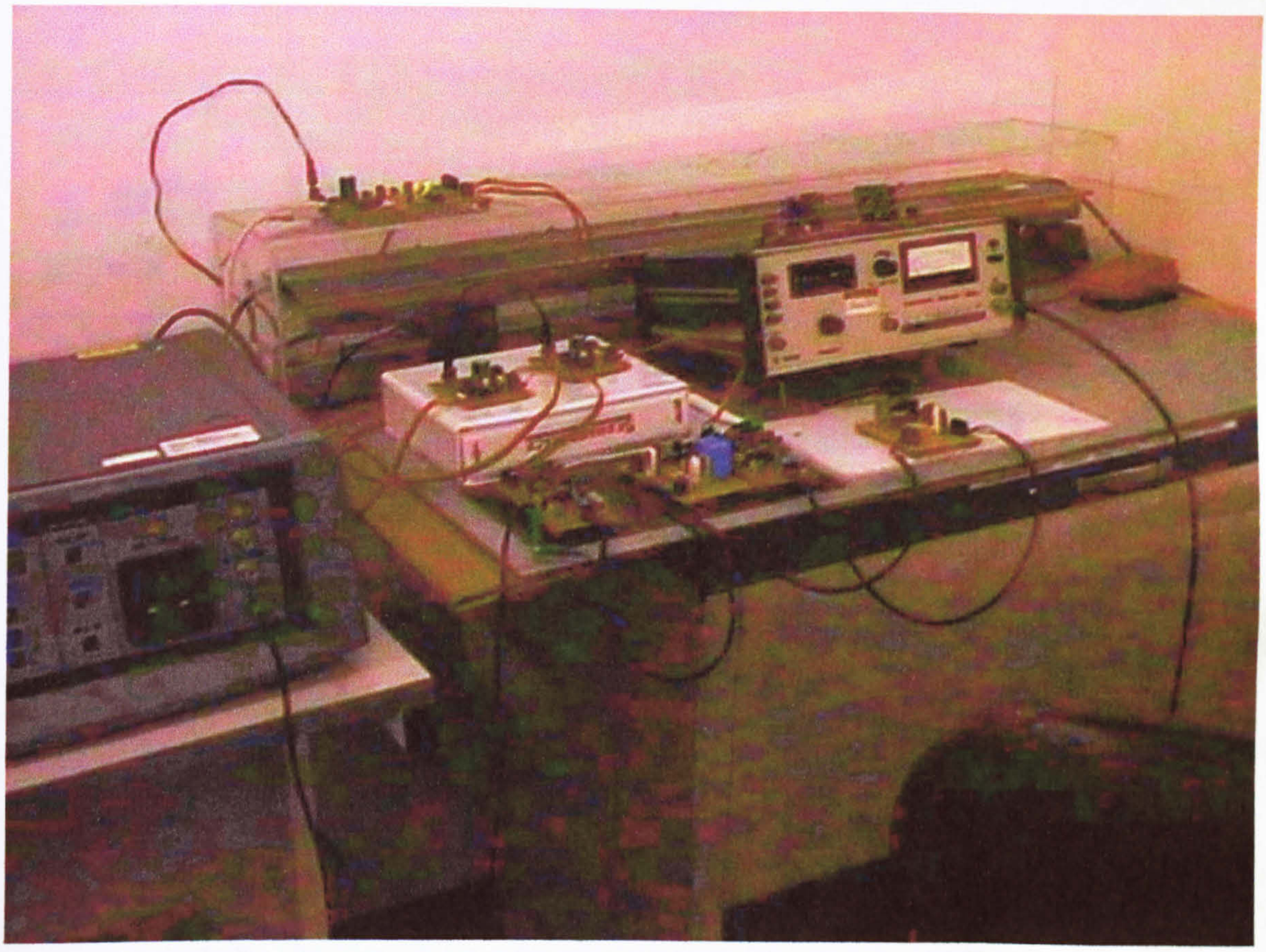


Figure 67: The Experimental Set-up in Real Life (#2)

Photograph #2 shows the rest of the experimental set-up. To the right of the MACE FTB generator can be seen the PL modems, the mains simulation network, and the attenuator unit. Behind these items are the isolator units, and at the back is the BERT assembly itself.

Having described the experimental set-up, we will move on to look at how a typical test run was organised.

7.9 Collecting the FTB Experimental Data

After connecting a PL Modem in the experimental set-up, as shown above, some initial tests were made without the application of an FTB signal:

- The maximum output signal level from the transmit modem was measured, both unloaded and with the mains simulation network in circuit.
- Using the attenuator, and with the BERT equipment running, the transmitter signal was reduced until errors started to be observed on the logging PC screen, giving a measure of the lowest signal capable of being reliably detected by the receiver.
- Next, a series of runs were carried out with FTB interference applied to the system. The Mace FTB generator was programmed to the appropriate value of burst amplitude, polarity, and duration (a standard duration of 120 seconds was used for these tests).
- Test runs were carried out at the various interference levels and signalling rates.
- In order to keep track of the experimental runs, the start and finish time stamp values on the screen of the logging PC were written down, plus (especially for low signalling rates) a count of the number of lines after the last time-stamp, before the test ended.

Overall, FTB tests were carried out at the following amplitudes:

- *500 V bursts, positive polarity*
- *500 V bursts, negative polarity*
- *1 kV bursts, positive polarity*
- *1 kV burst, negative polarity*
- *2 kV bursts, positive polarity*
- *2 kV burst, negative polarity*

At each amplitude value, tests were carried out at the following signalling rates:

- *2400 baud*
- *1200 baud*
- *600 baud*
- *300 baud*

It should be noted that some of these signalling rates are outside of the manufacturers nominal ranges, either below (300, 600 and 1200 baud for the ST7537, 300 baud for the TDA5051), or above (2400 baud for the TDA5051).

Nevertheless, it was decided that tests would be carried out at all of these rates, and due allowance made when analysing the results. In any case, it would be reasonable to expect that the modems will operate satisfactorily at lower than nominal rates.

7.10 Initial Processing of the 'Raw' Data

One a complete set of runs was finished the logging PC software was stopped. The 'raw' data was then loaded onto another PC by the simple expedient of taking the floppy disk (on which the data was recorded) to the PC, and copying it over! Once on the master PC, the 'raw' data file was then further processed using a simple text processor.

With the list of start and stop times created during the experimental runs, each block of experimental data was identified and isolated, and surplus, unnecessary, data deleted. A heading line was added to the top of each block of data indicating the conditions for that particular test (PL modem type, FTB voltage, polarity, and signalling rate).

The data saved by the logging software is already in what is known as comma-separated-value (CSV) format, which is a standard import format for most spreadsheet software. This permitted the processed data to easily be imported into Lotus 1-2-3, the spreadsheet software chosen.

Once within the spreadsheet, the data could easily be processed further and informative charts or graphs produced.

```
507,493,0,0
494,506,0,0
517,483,4,0
490,510,6,0
499,501,4,0
499,501,4,0,13:59:4
496,504,1,0
489,511,7,0
496,504,3,0
485,515,4,0
510,490,8,0
515,485,2,0
502,498,0,0
507,493,6,0
495,505,1,0
551,449,4,0,13:59:10
481,519,1,0
482,518,2,0
542,458,5,0
499,501,1,0
488,512,2,0
472,528,2,0
```

Figure 68: An Example of Saved Data from the BERT

As already described, the format of the data is as follows (with each line representing a single test block of 1000 bits):

- The total number of '0' bits sent in the test block.
- The total number of '1' bits sent in the test block.
- The total number of '0' bit errors ('0' bit received as '1') in the test block.
- The total number of '1' bit errors ('1' bit received as '0'), in the test block.
- Finally, every ten blocks, there is a time stamp.

Theoretically, the first two items should each equal 500, showing an even spread of '1's and '0's in the pseudo-random bit stream. In fact, there is a deviation either side of 500, due to the nature of the pseudo-random generator and the relatively low number of bits sampled in each block. Over a longer time scale, the 50:50 ratio will be more accurately maintained.

Before going on to analyse the experimental results in the next chapter, we will conclude this chapter by taking a more detailed look at the real world tests.

7.11 The 'Real World' Tests

As already mentioned, as a finale to the experimental work, some practical tests were run utilising the PL Modems in a 'real world' set-up. It was decided to pass the PL modem signal over the electrical distribution network, in an industrial (factory) environment, and monitor the performance over the course of several working days, using the BERT equipment to record the bit-error rates.

A route was chosen, within the premises of Elcontrol Limited (the authors workplace), which was as long as was reasonably achievable. The following diagram shows the arrangement:

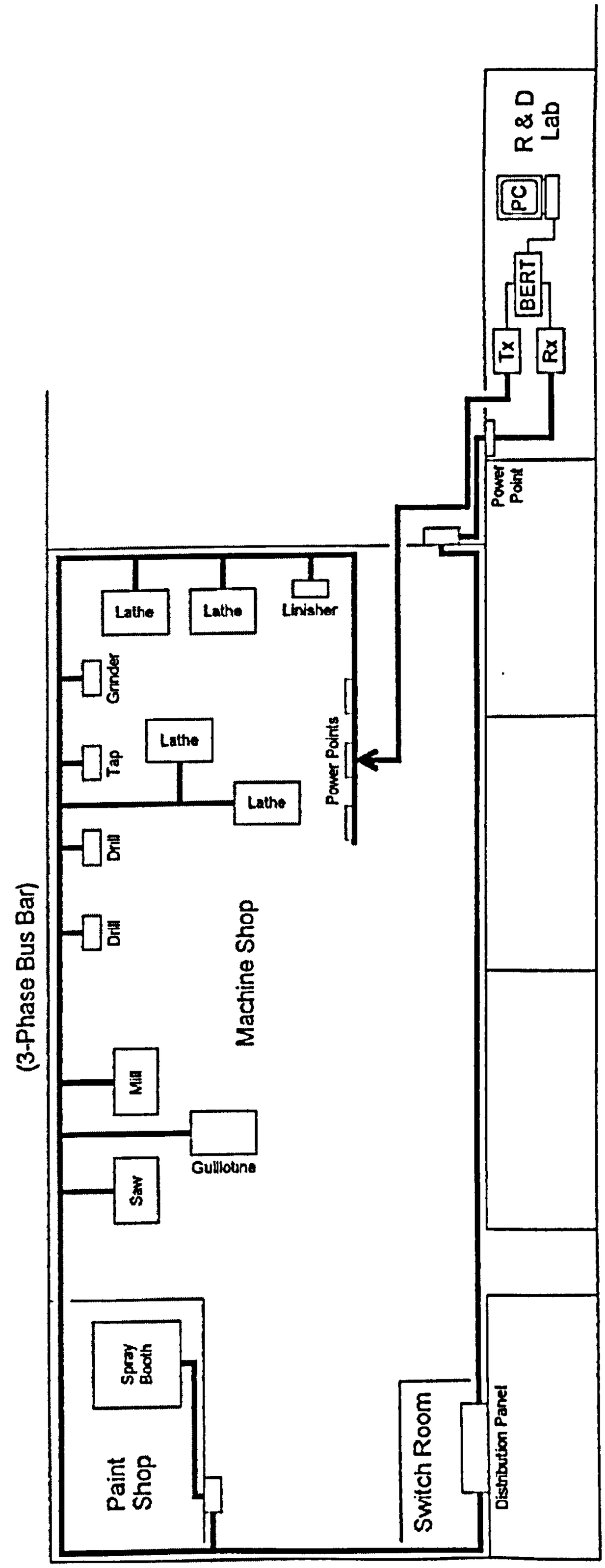


Figure 69: The 'Real World' Experimental Set-up

The transmitter PL Modem was connected via a flying lead of approximately 6 metres length, to a standard 13 A single-phase socket located within the machine shop of the company. This socket was at the far end of the main 3-phase bus-bar system from which all of the heavy workshop machinery is powered.

It can be seen from the diagram that this bus-bar passes around the periphery of the workshop. From it, a number of machine tools are powered, either directly, or via spur lines. The supply runs past the paint shop, where it is used to feed heating elements and fume extraction fans, to the main distribution panel in the switch room, a further distance of approximately 46 metres.

From the distribution panel, a spur line passes down the length of the factory to a small distribution box, from which the main single phase power feed to the R & D Lab is derived. The receive PL Modem was connected to a 13 A socked located in the R & D Lab. This leg of the set-up was some 20 metres in length, giving a total run between transmitter and receiver of approximately 72 metres. The entire loop was on the same phase.

Experimentally, the set-up was tried across phases, relying on intrinsic coupling effects, but in practice, this resulted in insufficient signal transfer. Further experiments would be feasible to investigate the effect of introducing purpose-built coupling networks to pass the PLC signal between phases, but this is considered beyond the scope of the present experimental work.

The BERT equipment and associated logging PC were set up as shown in the previous diagram. The data logging commenced at approximately 08:45 am each morning, and ceased at approximately 16:45 pm each afternoon, over a period of five working days, from Monday to Friday. The procedure was carried out for each power line modem in turn.

Obviously, these tests are non-quantitative, as we had no means of measuring the actual levels of noise present in the workshop environment. Nevertheless, they were worthwhile as they provided an idea of the modem performance in an actual environment.

We will discuss the results of the real world tests at the end of the next chapter, once we have finished analysing the results from our main experimental work.

Chapter 8 : Experimental Results, Analysis and Conclusions

In this chapter we will present and analyse our experimental results. We will begin with the Fast Transient Burst tests, as these constitute the most significant component of the experiments overall.

8.1 Initial PL Modem Performance Tests

As discussed in the previous chapter, before the FTB tests proper started, measurements were made to determine the amplitude of the carrier frequency waveforms generated by the PL modems. We will present these results first.

8.1.1 Modem Output Waveform Amplitudes

With the BERT equipment set up and running, simply to generate an arbitrary data stream, the oscilloscope was used to measure the transmitter output amplitude under various loading conditions viz:

- *Unloaded*
- *Loaded by the CISPR 16 network solely*
- *Loaded by the adaptive network solely*
- *Loaded by the combined CISPR 16 and adaptive network*

These measurements were repeated with the receiver PL modem in circuit to gauge what additional loading effect that had. The results are presented in the following tables:

TDA5051 Power Line Modem:	Measured Output (unloaded):		Measured Output (loaded by receiver):	
State:	Pk-to-pk	RMS	Pk-to-pk	RMS
No line loading:	3.4 V	1.21 V	2.8 V	0.99 V
Loaded by CISPR 16 network:	2.8 V	0.99 V	1.8 V	0.64 V
Loaded by adaptive network:	0.92 V	0.33 V	0.92 V	0.33 V
Loaded by CISPR 16 + adaptive network:	0.62 V	0.22 V	0.62 V	0.22 V

Figure 70: Measured Transmit Signal Levels for TDA5051

ST7537 Power Line Modem:	Measured Output (unloaded):		Measured Output (loaded by receiver):	
State:	Pk-to-pk	RMS	Pk-to-pk	RMS
No line loading:	8.4 V	2.98 V	5.8 V	2.06 V
Loaded by CISPR 16 network:	2.4 V	0.85 V	2.3 V	0.82 V
Loaded by adaptive network:	0.96 V	0.34 V	1.0 V	0.35 V
Loaded by CISPR 16 + adaptive network:	0.64 V	0.23 V	0.64 V	0.23 V

Figure 71: Measured Transmit Signal Levels for ST7537

We can make the following observations from these results:

- With the modems in an unloaded condition, they each gave notably different outputs, which fell significantly even when loaded only by the receive modem.
- As the mains simulation network elements are placed in circuit, the results begin to fall into line. With the full network (CISPR 16 + adaptive), the measured outputs are very close, with the receiver loading making no discernible difference (0.22 V RMS for the TDA5051, and 0.23 V RMS for the ST7537).

Referring to EN 50065-1, we know that the maximum permitted signal level for general use is 630 mV, meaning both modems are well within that limit. Indeed, for industrial use (maximum signal level 5 V) we could in theory increase the output magnitude some 20-fold, although this would require a much increased drive power to operate into the low impedance of the mains simulation network!

Next, measurements were made of the minimum signal amplitude from the transmitter that would be reliably detected by the receiver.

8.1.2 Modem Receiver Sensitivity

Using the attenuator network, and observing the display on the BERT equipment, the transmission signal level was reduced until errors started to be observed on the BERT display. This signal level was measured using the oscilloscope.

In both cases, the modems reliably operated at about 20 mV peak-to-peak input (the TDA5051 with the pre-amplifier out of circuit). This is equivalent to an RMS value of approximately 7 mV. With the TDA5051 pre-amplifier in circuit, the input requirement dropped to a level too low to reliably measure on the oscilloscope (well below 5 mV peak-to-peak). This means that both modems comply with the access band requirement of EN 50065 (which states that a signal level of 10 mV within the operational band must be detected).

In view of this 7 mV RMS minimum signal, and in deference to EN 50056, we decided to use a test level of 10 mV RMS (approximately 30 mV peak-to-peak) as the baseline, lowest, signal value for our experiments. It was further decided to disregard the pre-amplifier facility on the TDA5051 modem, in order to achieve an even comparison between the two modems.

We will now consider the actual results for the FTB noise experiments. The results presented here will be summary results for each modem and each FTB amplitude value.

8.2 BER Test Results for FTB Noise

As already mentioned, these tests were carried out at FTB amplitudes of 500 V, 1 kV, and 2 kV, and at signalling rates of 300, 600, 1200, and 2400 baud. The results presented on the following pages are summarised from the detailed results presented in Appendix 1 of this thesis. Specifically, the results for the ST7537 and TDA5051 are combined onto a single graph and the separate results for the positive (+ve) and negative (-ve) FTB pulse trains are averaged. It is noticeable (referring to Appendix 1) that the BER levels measured for the positive pulses often differ from those for negative pulses with, typically, the negative pulses producing slightly lower BER values. This was more noticeable with the ST7537 modem compared to the TDA5051. Without further research, the author can at present offer no explanation for this phenomenon.

The BER values calculated are expressed as a percentage value, i.e. bits corrupted per 100 sent bits. The first set of results are for a transmission signal of 30 mV peak-to-peak (10 mV RMS) which, as we mentioned, was chosen as our minimum working level.

8.2.1 FTB Results for 10 mV RMS Signal Amplitude

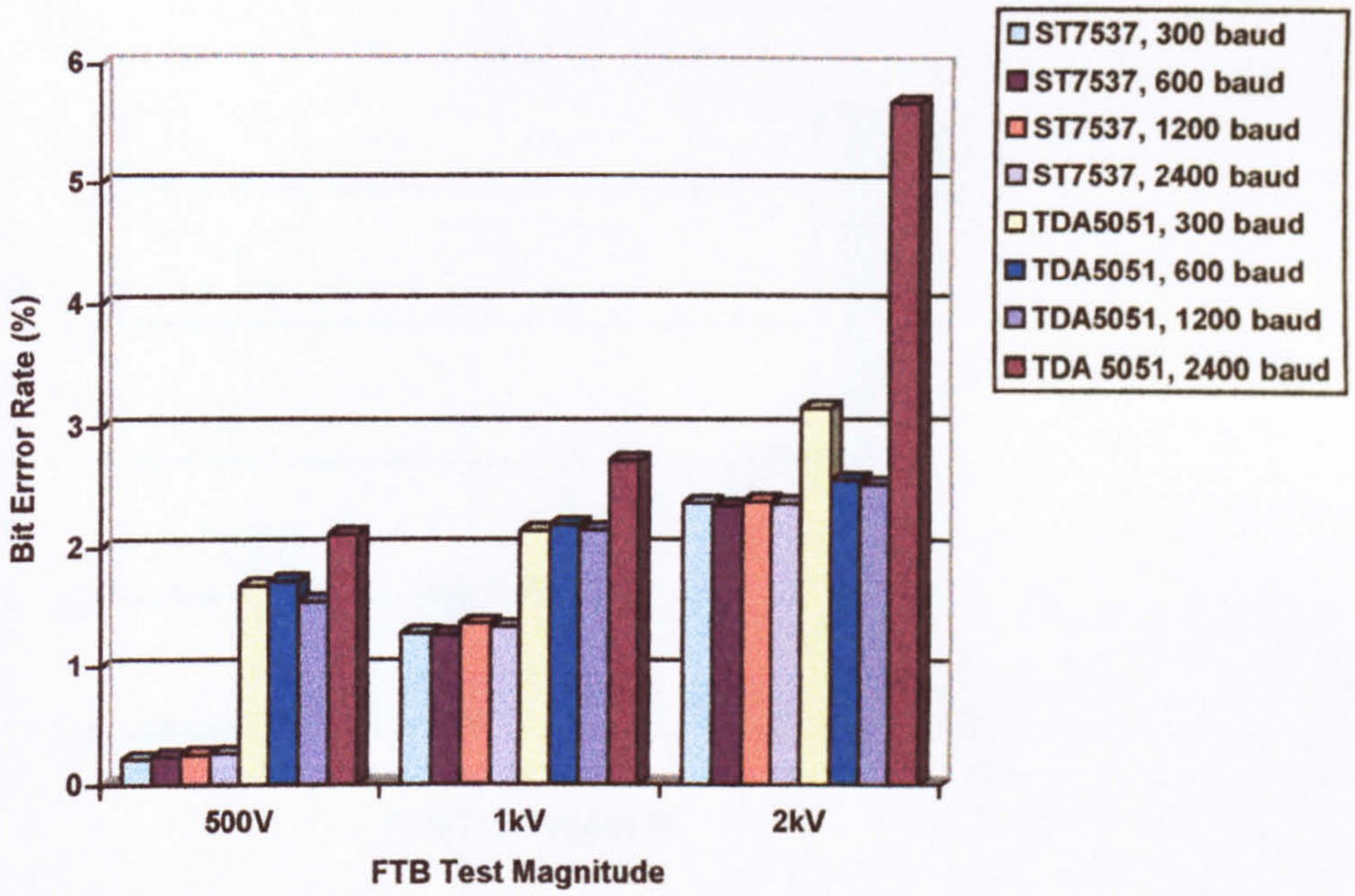


Figure 72: Summary FTB Results for 10 mV RMS Signal Level

Immediately evident from the above graph is the fact that, especially at lower FTB magnitudes, the BER results for the ST7537 are noticeably better than those for the TDA5051. At 500 V, the average BER (combining all signalling rates) is 0.23 % for the ST7537 and 1.8 % for the TDA5051. As the FTB amplitude increases, the difference drops - at 1 kV the BER is 1.3 % for the ST7537 and 2.3 % for the TDA5051. At 2 kV, the difference is much less pronounced, except at signalling rates of 300 and 2400 baud, both technically outside of the nominal operating range for the TDA5051. Disregarding these anomalies, the BER at 2 kV is around 2.4% for both modems.

We might postulate that at such relatively low carrier signal levels, the advantage of the FSK modulation scheme over the ASK is tending to be masked by the sheer magnitude of the FTB signal compared to the PLC signal.

8.2.2 FTB Results for 20 mV RMS Signal Amplitude

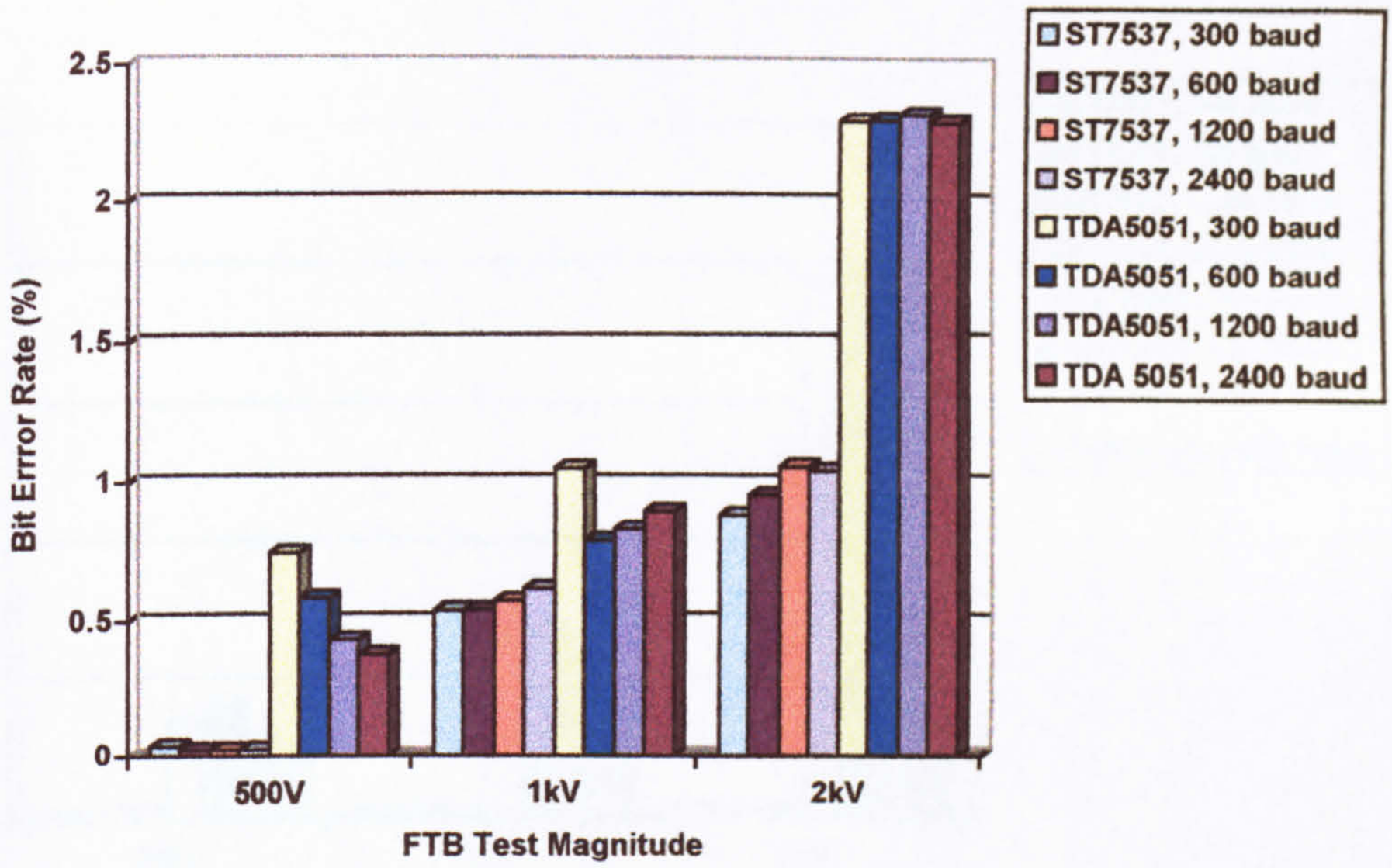


Figure 73: Summary FTB Results for 20 mV RMS Signal Level

The transmission signal level was next doubled to 60 mV peak-to-peak (20 mV RMS). The most obvious trend noticeable in these results is the overall lowering of BER for both modems, plus the notable increase in the differential at 2 kV FTB amplitude between the two modems.

At 500 V, the average BER is 0.03 % for the ST7537, a considerable drop from 0.23 %, and 0.5 % for the TDA5051, down from 1.8 %. At 1 kV the BER is 0.6 % for the ST7537 (from 1.3 %) and 0.9 % for the TDA5051 (from 2.3 %). At 2 kV the BER is 1.0 % for the ST7537 (from 2.4 %) and 2.3 % for the TDA5051 (only a little less than the 2.4 % value achieved if we disregard the anomalous value already mentioned).

8.2.3 FTB Results for 40 mV RMS Signal Amplitude

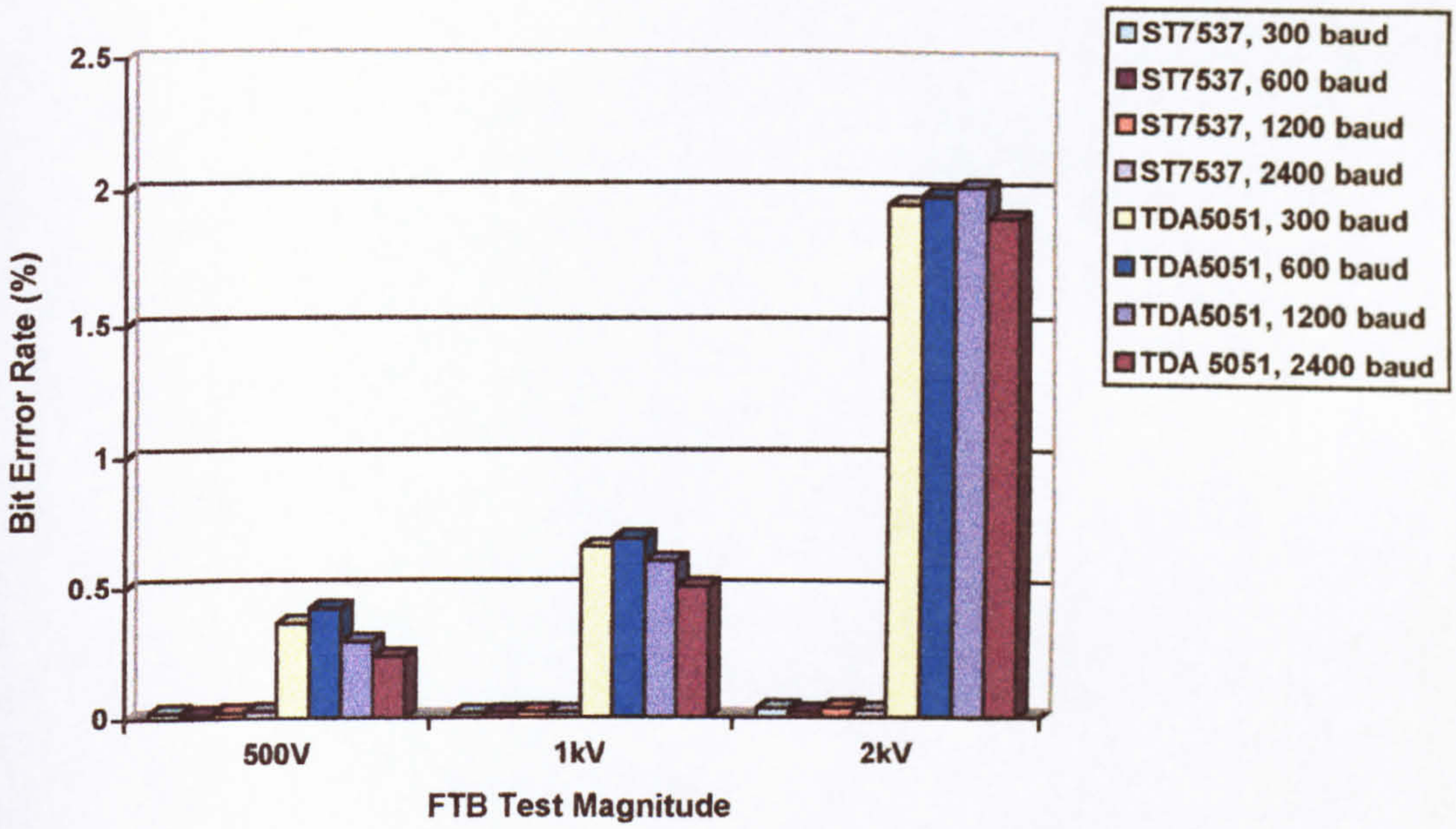


Figure 74: Summary FTB Results for 40 mV RMS Signal Level

The transmission signal level was again doubled to 120 mV peak-to-peak (40 mV RMS). The most obvious trend noticeable in these results is the dramatic reduction of BER for the ST7537.

At 500 V, the BER is 0.02 % for the ST7537 (from 0.03 %) and 0.32 % for the TDA5051 (from 0.5 %). At 1 kV the BER is still 0.02 % for the ST7537 (from 0.6 %) and 0.6 % for the TDA5051 (from 0.9 %). At 2 kV the BER is 0.03 % for the ST7537 (from 1.0 %) and 2.0 % for the TDA5051 (down from 2.3 %).

8.2.4 FTB Results for 80 mV RMS Signal Amplitude

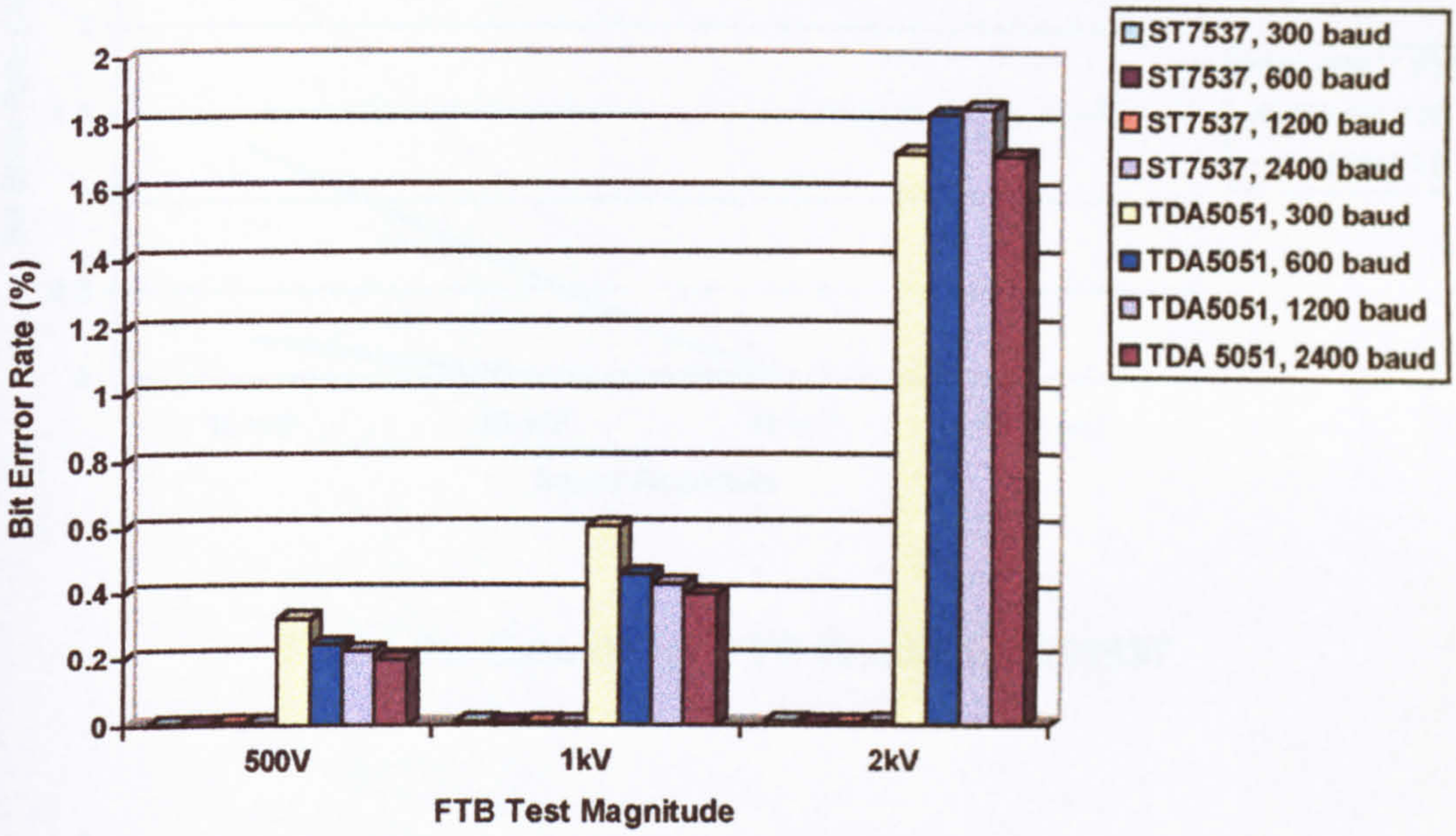


Figure 75: Summary FTB Results for 80 mV RMS Signal Level

Finally, the transmission signal level was doubled to 240 mV peak-to-peak (80 mV RMS). Again, the most obvious trend noticeable in these results is the low BER for the ST7537. Since the results for the ST7537 are now so low, no higher signal amplitudes were tested.

At 500 V, the average BER is 0.003 % for the ST7537 (from 0.02 %) and 0.25 % for the TDA5051 (from 0.32 %). At 1 kV the BER is still only 0.007 % for the ST7537 (from 0.02 %) and 0.47 % for the TDA5051 (from 0.6 %). At 2 kV the BER is 0.008 % for the ST7537 (from 0.03 %) and 1.8 % for the TDA5051 (down from 2.0 %).

8.2.5 FTB Test Conclusions

In order to sum up the previous findings we have amalgamated the BER values for all signalling rates, for a given value of signal amplitude and FTB voltage level. The next two graphs show these amalgamated results.

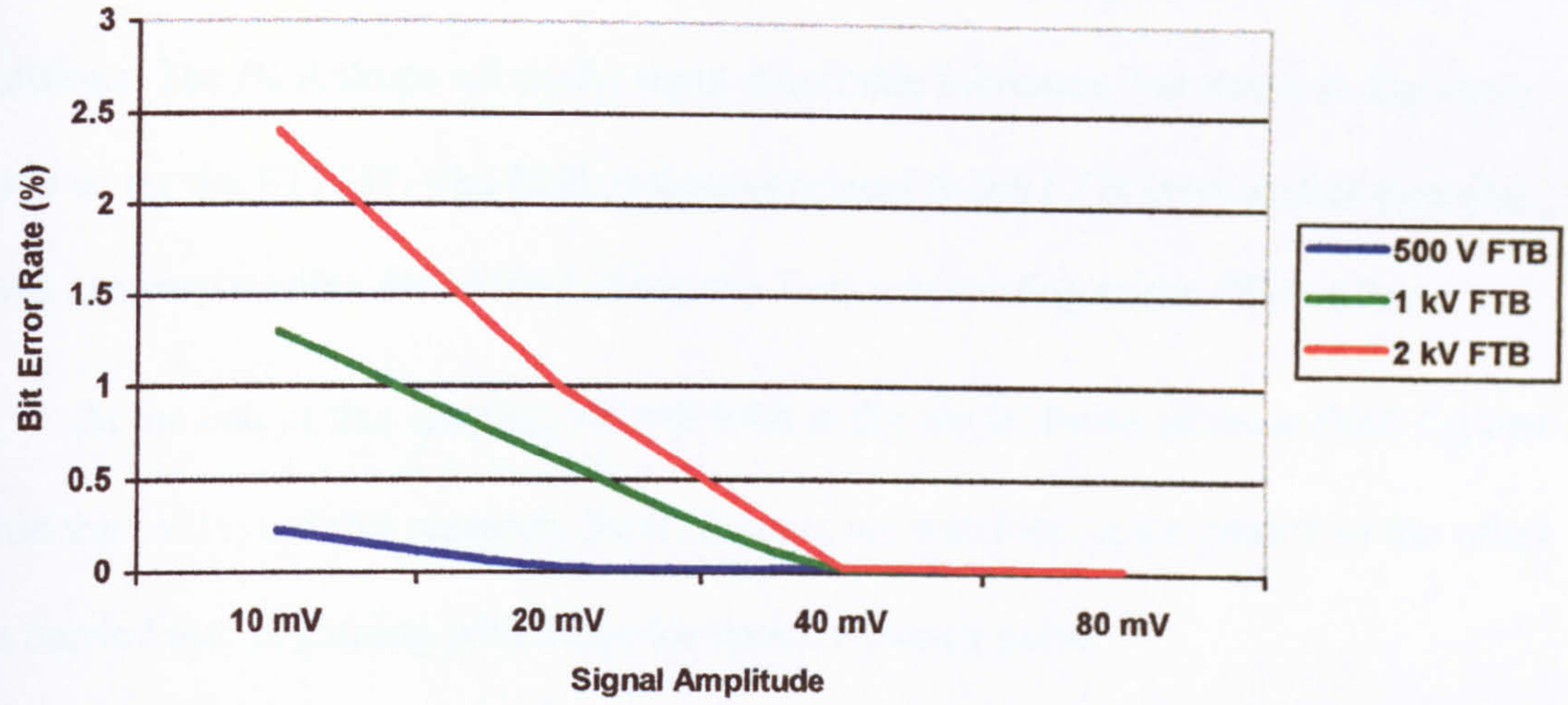


Figure 76: Cumulative FTB Results for ST7537

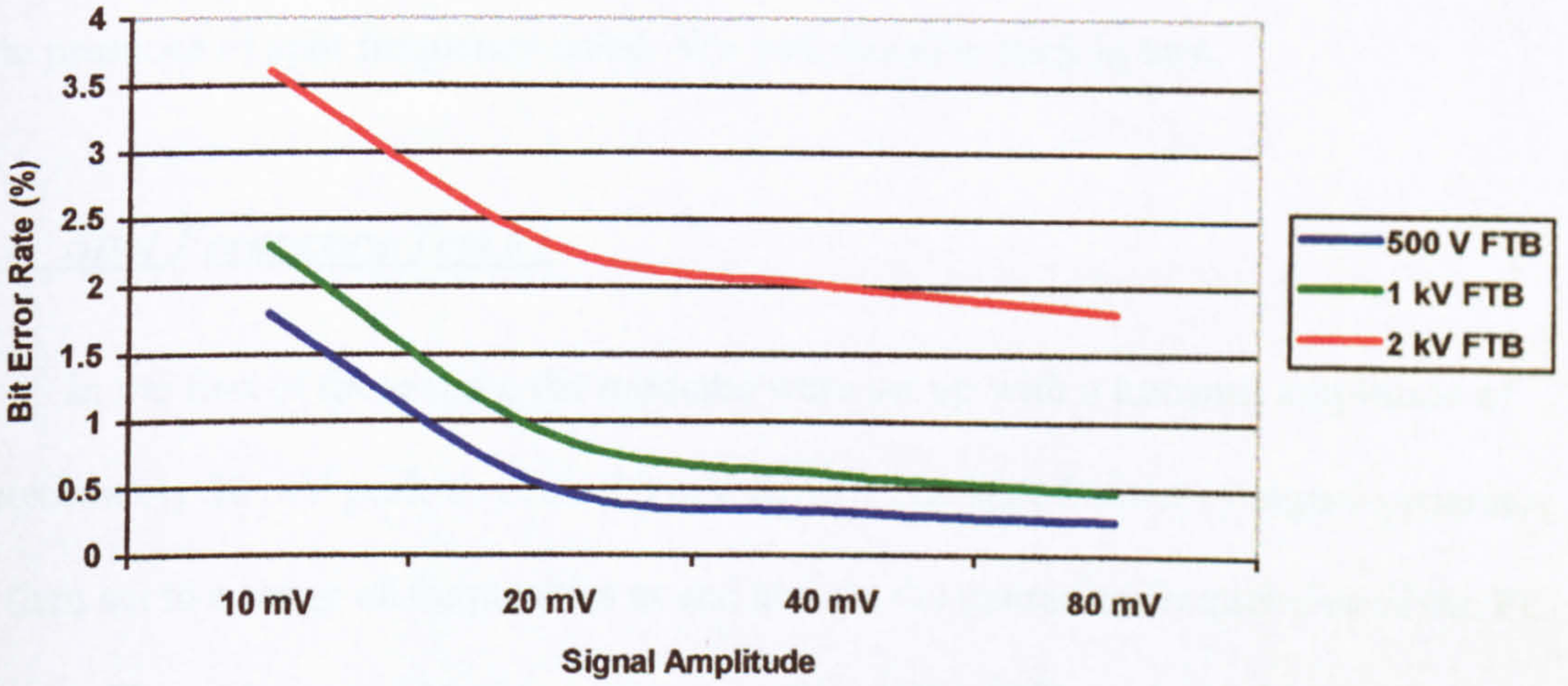


Figure 77: Cumulative FTB Results for TDA5051

Looking at the first graph it can be seen that the ST7537 exhibits a sharp drop in BER as the signal amplitude increases. By the time we reach a level of 40 mV, the BER has dropped to below 0.1 % (less than one corrupted bit in 1000) for all FTB levels. In fact, if we infer that we can extrapolate the sharp initial drop between 10 mV and 20 mV right down to the X-axis, this point would be achieved at less than 40 mV signal level.

The TDA5051, on the other hand, has a significantly higher BER under all conditions. The BER drops off as the input amplitude increases, but never to the same degree as for the ST7537. The BER is always related to the FTB level, notice how the curves are very similar, but shifted along the Y-axis according to the FTB voltage.

At the end of this chapter, we will look at the implications of these BER figures within the context of this research. Next, though, we will look at the results of the other tests carried out, beginning with those for spot frequency noise.

8.3 BER Test Results for Spot Frequency Noise

Three distinct tests were carried out to ascertain the performance of the PL modems in the presence of spot frequency noise. We will describe each in turn.

8.3.1 Spot Frequency Test #1

In the first of these tests, the modems were set up with a transmit amplitude of approximately 30 mV peak-to-peak (10 mV RMS). The spot frequency signal generator was then set to a range of frequencies at and around the operating frequencies of the PL modems. This value was 115 kHz in the case of the TDA5051, and 131.85 kHz and 133.05 kHz, in the case of the ST7537 (in addition, for the ST7537, the approximate median value of 132.5 kHz was also used). The noise output amplitude was increased until errors just started to appear on the BERT data readings. These results were noted and plotted as graphs. The results are shown on the following pages.

8.3.2 Results for ST7537

The following data shows the amplitude of noise frequency required to just cause errors in the received bit-stream, for a modem transmit signal amplitude of 10 mV RMS.

ST7537, 10 mV RMS received signal	
Noise Frequency, kHz	Noise level causing errors in received bit stream (mV RMS)
125	**150**
130	**9**
131.85	**2.7**
132.5	**2.7**
133.05	**2.7**
135	**53**

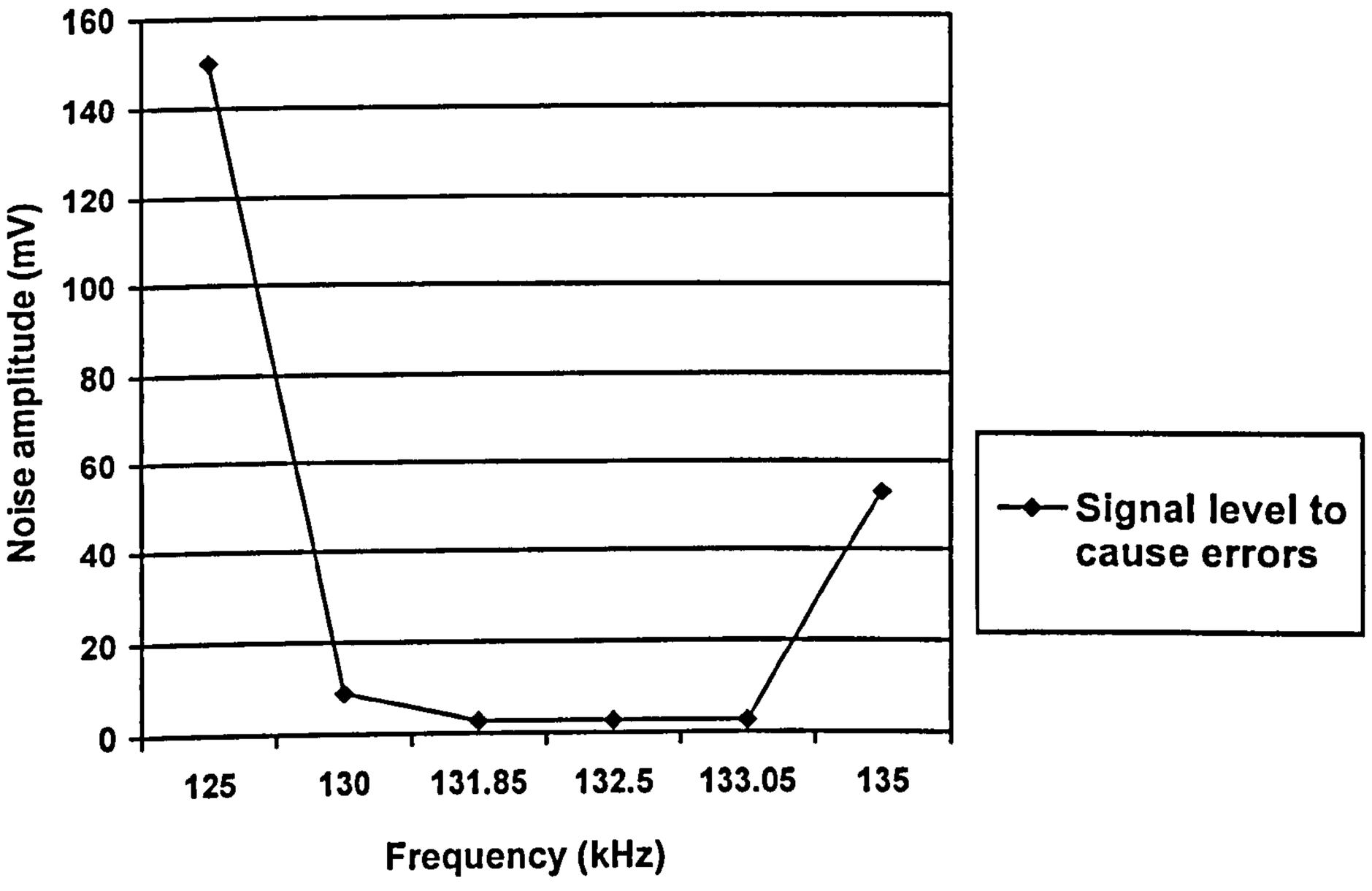


Figure 78: Results for ST7537 Spot Frequency Test #1

8.3.3 Results for TDA5051

The following data shows the amplitude of noise frequency required to just cause errors in the received bit-stream, for a modem transmit signal amplitude of 10 mV RMS.

TDA5051, 10 mV RMS received signal	
Noise Frequency, kHz	Noise level causing errors in received bit stream (mV RMS)
40	**320**
55	**127**
75	**37**
95	**29**
105	**32**
110	**35**
112.5	**32**
115	**7**
117.5	**27**
120	**32**
125	**29**
135	**23**
155	**19**
175	**35**
195	**70**

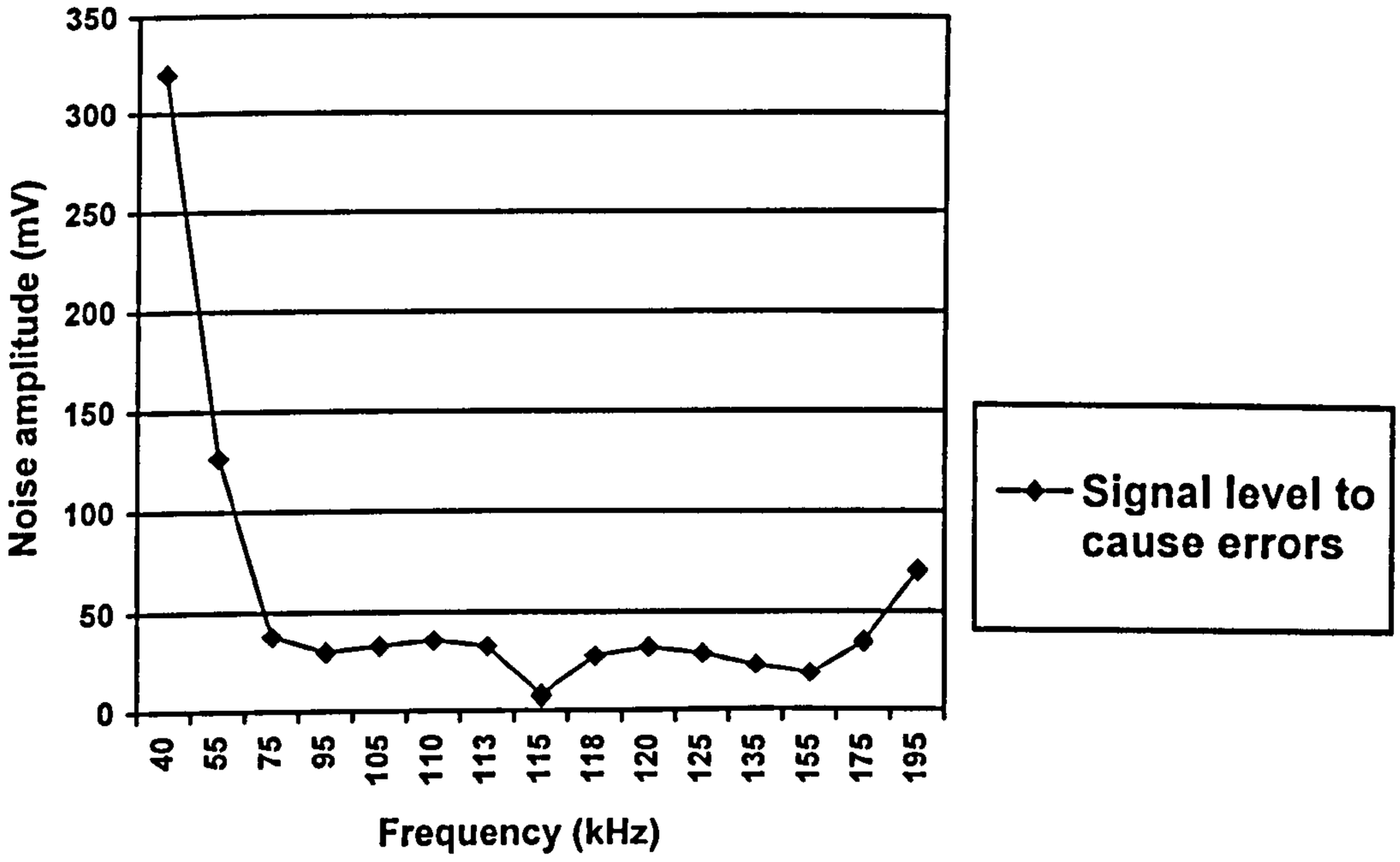


Figure 79: Results for TDA5051 Spot Frequency Test #1

8.3.4 Analysis of Results for Spot Frequency Test #1

It can be seen that at the operating and median frequencies, the ST7537 is susceptible to signals of some 2.7 mV, for a 10 mV signal level. Outside of these frequencies, there is a very noticeable band-pass effect. By the time we drop below a frequency of 130 kHz or exceed a frequency of 135 kHz, more than 10 times that noise level is needed to cause errors.

The TDA5051, on the other hand, is less susceptible noise at its operational frequency (7 mV for a 10 mV signal level). However, the band beyond which the noise level rises dramatically is much wider - from approximately 75 kHz to 175 kHz. Referring to the manufacturers data sheets for the two devices [16, 44] gives us a possible explanation. We can see that the ST7537 is equipped with an internal band-pass filter of 12 kHz bandwidth, early on in the receive signal path. In addition, the signal later passes through an intermediate frequency (IF) stage itself having a 5.4 kHz bandwidth.

The TDA5051 has no equivalent input filter, and no bandwidth limiting is applied until later in the signal path, after the receive signal has passed through the input wide-band automatic gain stage and been digitised in an A-D converter. At low input signal levels the gain of the front end will necessarily be high, which may further exacerbate the problem. Further tests would be worthwhile to determine if the TDA5051 performance could be improved by the use of additional front-end filtering.

We will next consider the second spot frequency test.

8.3.5 Spot Frequency Test #2

For the second spot frequency test, the modems were set up with a transmission amplitude of approximately 240 mV peak-to-peak (80 mV RMS). The spot frequency signal generator was also set to an amplitude of 80 mV RMS at various frequencies around the operational frequencies of the modems. At each frequency, the measured BER value was recorded. These results were noted and plotted as graphs. The results are shown on the following pages.

8.3.6 Results for ST7537

The following data represents the effect on BER of a spot frequency signal of 80 mV RMS, at various frequencies, against a PL modem signal amplitude of 80 mV RMS.

Frequency:	107.5 kHz	117.5 kHz	127.5 kHz	130.0 kHz	131.9 kHz
BER %	**0.00000**	**0.00000**	**0.01625**	**0.01125**	**50.34125**
Frequency:	132.5 kHz	133.1 kHz	135.0 kHz	137.5 kHz	147.5 kHz
BER %	**42.84125**	**49.69875**	**0.05000**	**0.00250**	**0.00375**

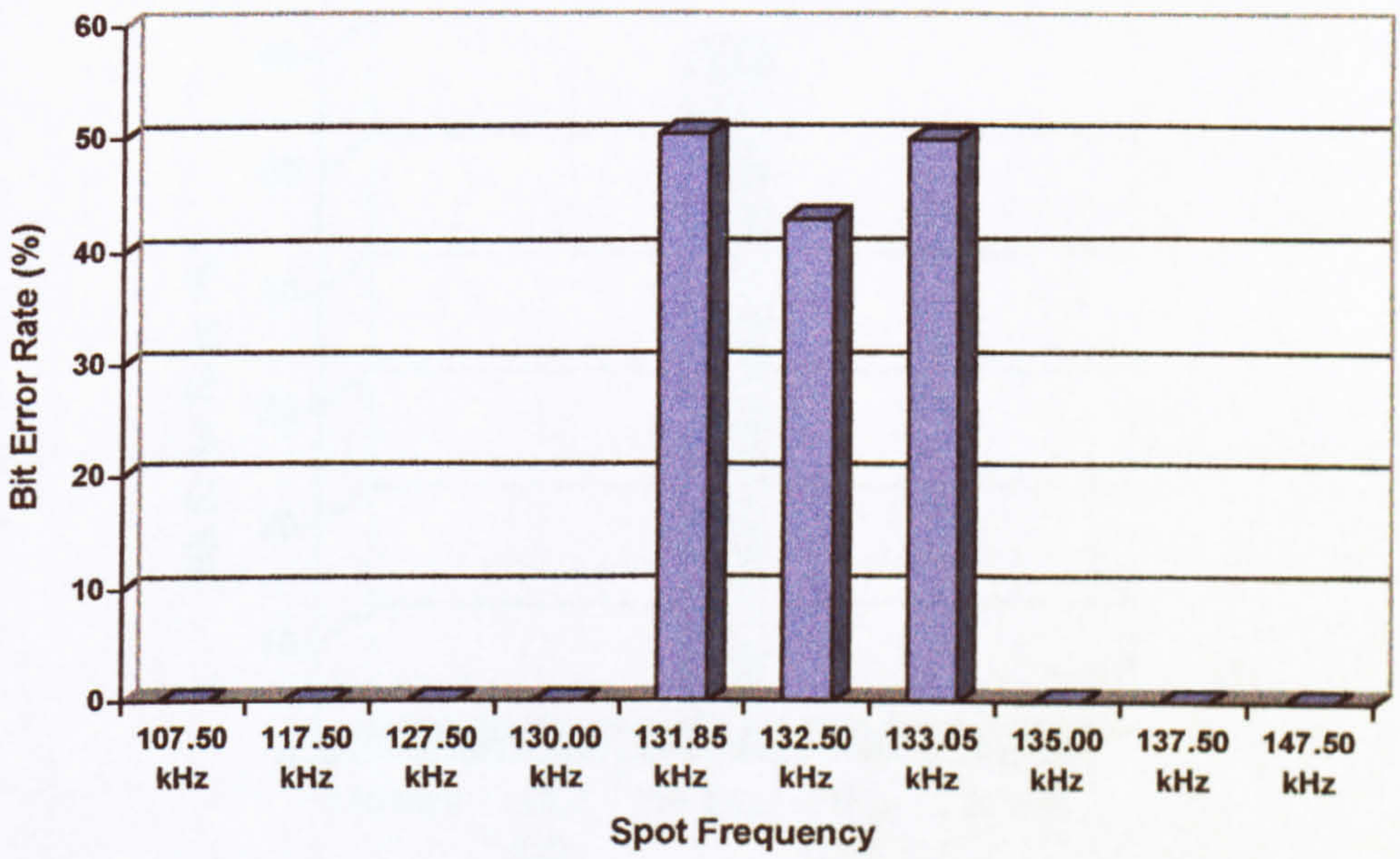


Figure 80: Results for ST7537 Spot Frequency Test #2

8.3.7 Results for TDA5051

The following data represents the effect on BER of a spot frequency signal of 80 mV RMS, at various frequencies, against a PL modem signal amplitude of 80 mV RMS.

	Spot Frequency				
Bit Error Rate (%)	110 kHz	112.5 kHz	115 kHz	117.5 kHz	120 kHz
	0.00000	**0.00000**	**59.22500**	**0.00000**	**0.00000**

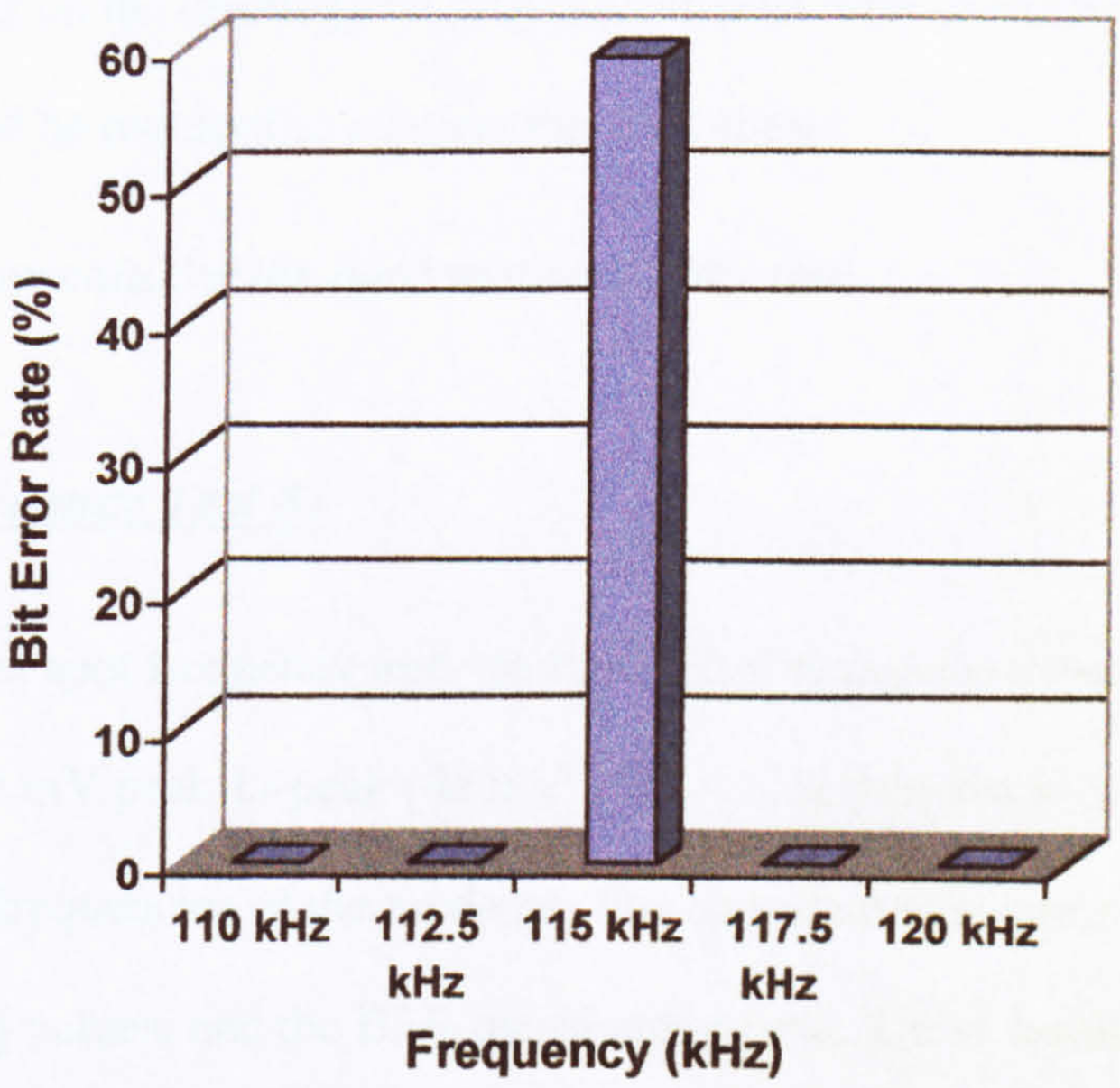


Figure 81: Results for TDA5051 Spot Frequency Test #2

8.3.8 Analysis of Results for Spot Frequency Test #2

It can be seen that for the ST7537 these results broadly follow those already noted in test #1. The device exhibits a narrow pass-band with good immunity outside of it.

For the TDA5051, the effects noted in test #1 seen to have been overcome, and the device also shows good immunity outside of a narrow band around its operating frequency. We can surmise that this is due to the input automatic gain stage now needing to operate at a much lower gain due to the larger input signal. The presence of the noise signal now has less spurious effect on the digital (post-ADC) band-pass filter present in this device. Further tests would be required to confirm this hypothesis.

We will now consider the third spot frequency test.

8.3.9 Spot Frequency Test #3

For the final spot frequency test, the transmission amplitude was again set to approximately 240 mV peak-to-peak (80 mV RMS). This time the signal generator was set to the operational frequencies of the modems. The spot frequency amplitude was set to a range of increasing values, and the BER measured at each. These results were noted and plotted as graphs. The results are shown on the following pages.

8.3.10 Results for ST7537

The following data represents the effect on BER of a spot frequency signal of variable amplitude, at certain spot frequencies at and between the modem operating frequencies, against a PL modem signal amplitude of 80 mV RMS.

Spot Freq.	Spot Frequency Amplitude (RMS)						
	20 mV	30 mV	40 mV	60 mV	80 mV	120 mV	160 mV
131.85 kHz	**0.005**	**0.0525**	**1.8**	**13.2**	**44.7**	**49.3**	**49.1**
132.50 kHz	**0.0125**	**0.00375**	**0.0**	**4.0**	**25.7**	**35.6**	**39.8**
133.05 kHz	**0.0025**	**0.0025**	**0.015**	**8.5**	**20.7**	**50.0**	**49.7**

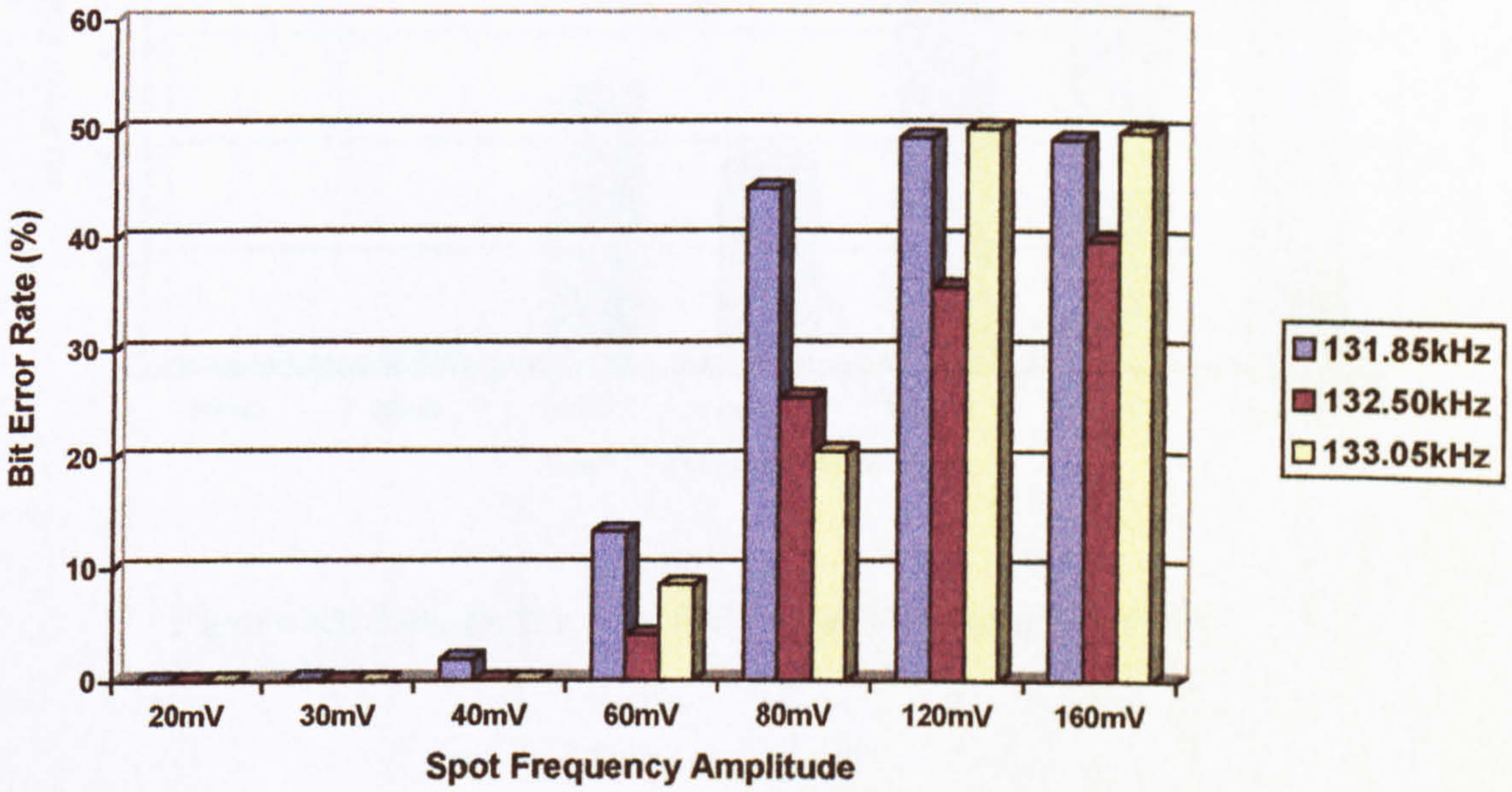


Figure 82: Results for ST7537 Spot Frequency Test #3

8.3.11 Results for TDA5051

The following data represents the effect on BER of a spot frequency signal of variable amplitude, at the modem centre frequency of 115 kHz, against a PL modem signal amplitude of 80 mV RMS.

	Spot Frequency Amplitude RMS						
Bit Error Rate (%)	7 mV	8 mV	10 mV	20 mV	40 mV	80 mV	160 mV
	0.0	**1.6**	**25.3**	**19.0**	**44.3**	**57.5**	**52.3**

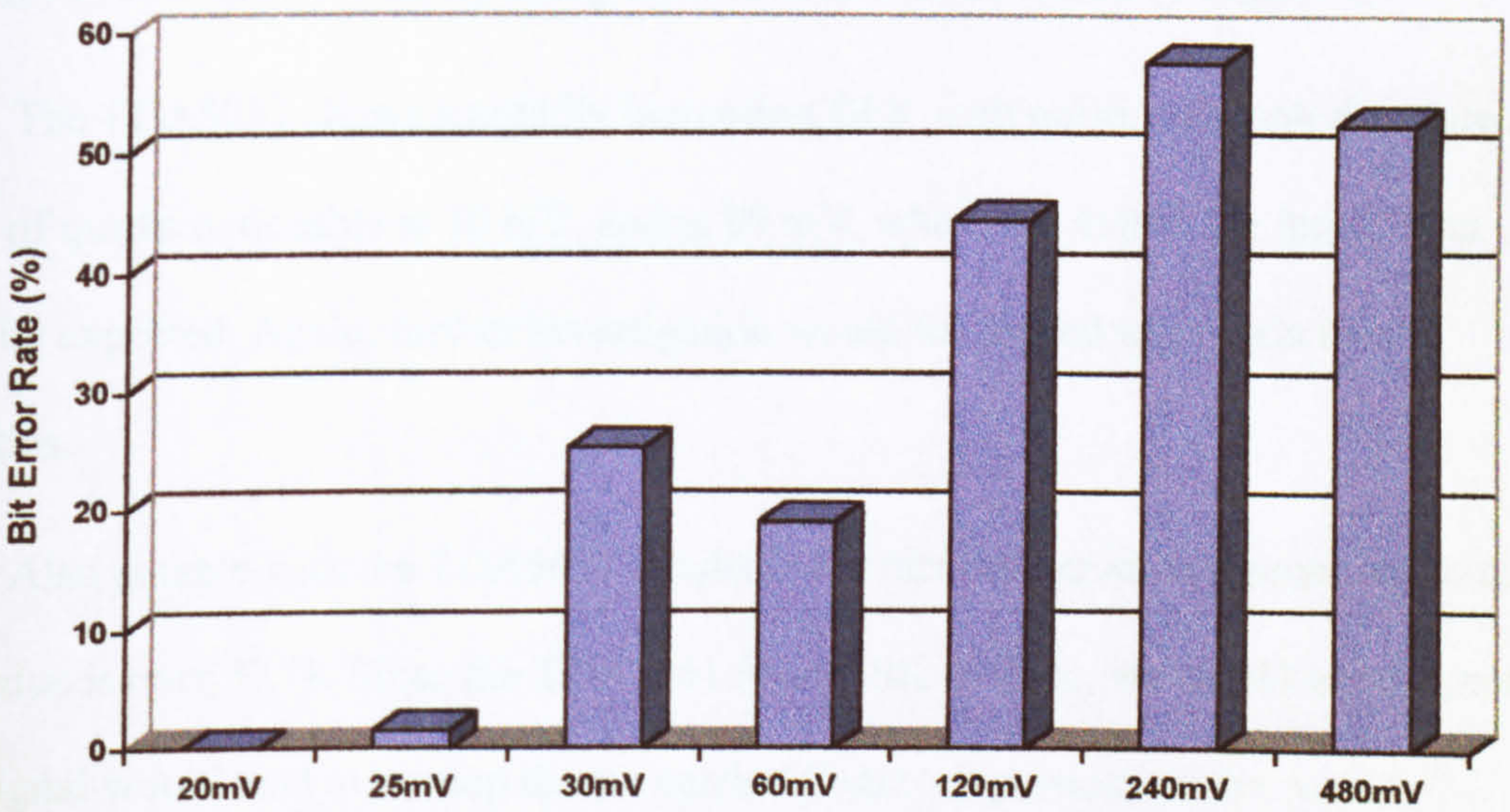


Figure 83: Results for TDA5051 Spot Frequency Test #3

8.3.12 Analysis of Results for Spot Frequency Test #3

The ST7537 results are broadly what one would expect. As the amplitude of the noise signal rises, so does the BER. Interestingly, it is evident, especially at lower amplitudes, that noise at the 131.85 kHz carrier frequency has a greater effect than noise at the other carrier frequency of 133.05 kHz. This may be a result of the demodulation technique utilised within the device, but would require further investigations to clarify. At noise amplitudes of 120 mV RMS and above, this effect disappears. At the median frequency (132.5 kHz) a steadily rising BER is achieved, as would be expected.

The TDA5051 shows a broadly increasing BER with noise, although there are a couple of quirks noticeable at 10 mV, and at 80 mV, where the values are larger than would be expected. Again, further investigation would be needed to explain these anomalies.

Also notable with the TDA5051 results is the fact that, at 80 mV noise level, the BER value is over 57 %. Since the TDA5051 is an ASK modem, we would expect that the noise signal would tend to swamp the 'no carrier' (logic '1') portions of the receive waveform. Therefore all logic '1' bits would be received incorrectly and we would expect a BER of around 50 % maximum (assuming a true 50:50 logic '1' to logic '0' bit ratio from the BERT equipment). In fact, looking at the raw data, we see that at all noise levels above 40 mV, there are a significant number of logic '0' errors that contribute to the high overall BER.

We can surmise that this may be a function of the advanced digital demodulation techniques utilised in this device, but more research would needed to clarify the cause of these effects.

For the ST7537, the expected results would be that noise at one of the carrier frequencies would tend to cause bit errors at the logic level corresponding to the other carrier frequency. This was true at the highest signal levels (120 mV and above), but at lower levels there was again a tendency for both logic levels to be corrupted. As before, we would require further research to explain this anomaly.

We will now look at the last of the noise tests, the sweep frequency test.

8.3.13 Swept Frequency Test

As a final test, the modems were subjected to a swept frequency test. By its very nature, and due to the unsophisticated equipment available to the author, this is not a quantitative test, but was included for completeness.

The modem transmission amplitude was set to approximately 240 mV peak-to-peak (80 mV RMS) and the signal generator was set to sweep over the range of 80 kHz to 160 kHz at a rate of approximately 30 Hz.

The swept frequency amplitude was set to a range of increasing values, and the BER measured at each. These results were noted and plotted as graphs. The results are shown on the following pages.

8.3.14 Results for ST7537

The following data represents the effect on BER of a swept frequency signal, of variable amplitude, against a PL modem signal amplitude of 80 mV RMS.

	Sweep Frequency Amplitude (RMS)				
Bit Error Rate (%)	10 mV	20 mV	40 mV	80 mV	160 mV
	0.0025	**0.00375**	**0.219**	**2.50**	**4.56**

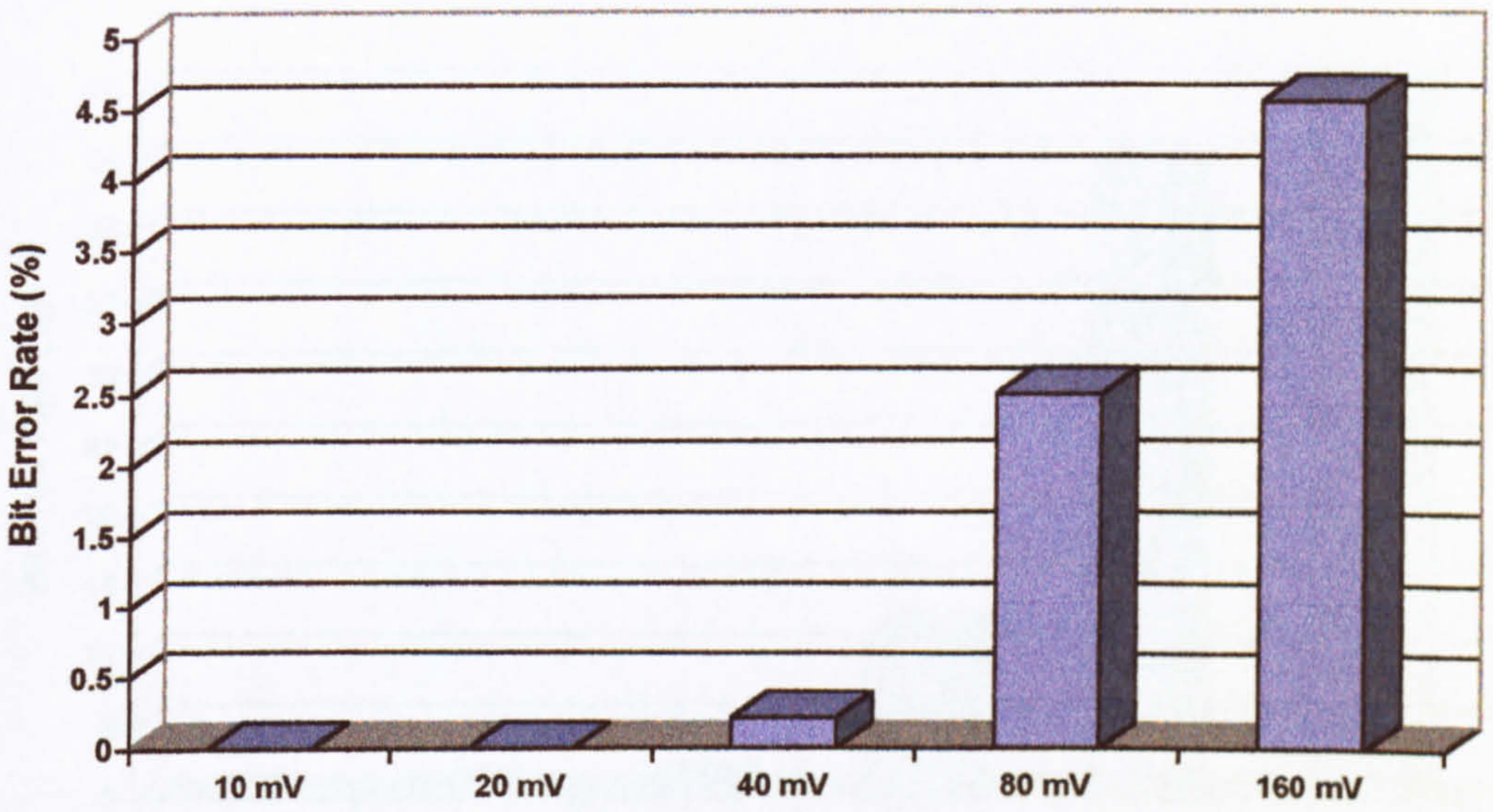


Figure 84: Results for ST7537 Swept Frequency Test

8.3.15 Results for TDA5051

The following data represents the effect on BER of a swept frequency signal, of variable amplitude, against a PL modem signal amplitude of 80 mV RMS.

	Sweep Frequency Amplitude RMS						
Bit Error Rate (%)	10 mV	15 mV	20 mV	30 mV	40 mV	80 mV	100 mV
	0.7	**0.12**	**0.25**	**0.9**	**11.7**	**44.4**	**49.9**

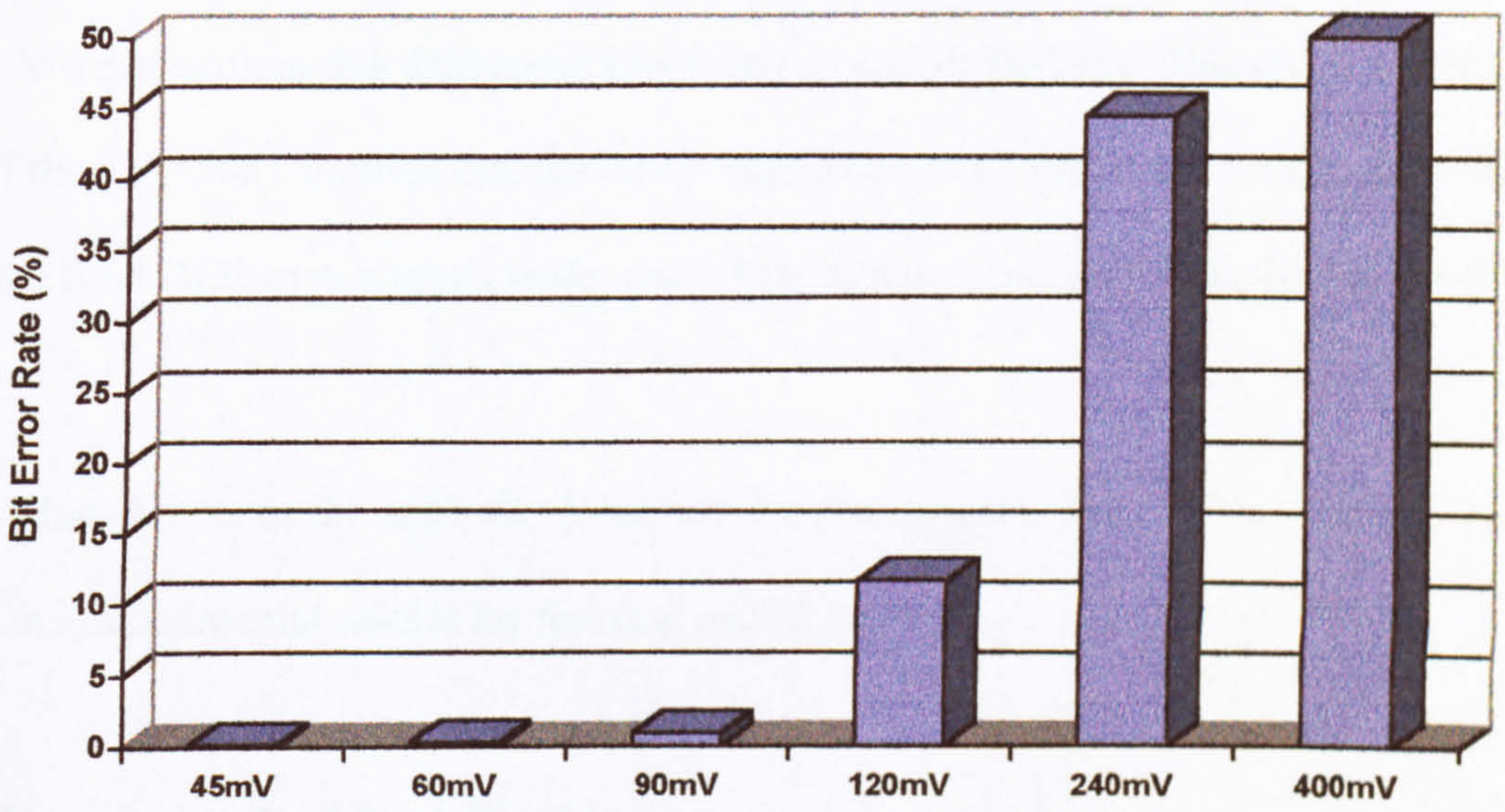


Figure 85: Results for TDA5051 Swept Frequency Test

8.3.16 Analysis of Results for Swept Frequency Test

It would be expected that the modems would be compromised as the frequency passed through their operational frequencies and this is indeed what was found.

The ST7537 showed a gradual increase in BER up to a maximum value of approximately 4.6 %. The TDA5051 showed a similar increase up to a maximum BER of around 50 %.

We can explain this difference based on our earlier findings. The much wider pass-band of the TDA5051 implies that the swept signal (when of sufficient amplitude) will affect the final BER over a much wider part of the sweep band, hence the higher BER overall.

That concludes the analysis of the spot frequency noise test results. We will finally look at the experimental results for the 'real world' tests.

8.4 Results for the 'Real World' Tests

As already described, these final tests were conducted over a period of time within an actual factory environment. A sample of one working week was then used as the basis of our analysis.

As with the FTB tests, some initial measurement of transmit carrier amplitudes were made. Due to the fact that in these tests, the PL modems are energised at mains voltages, an isolating circuits was used to measure the signal amplitudes. The circuit used is shown in the next figure.

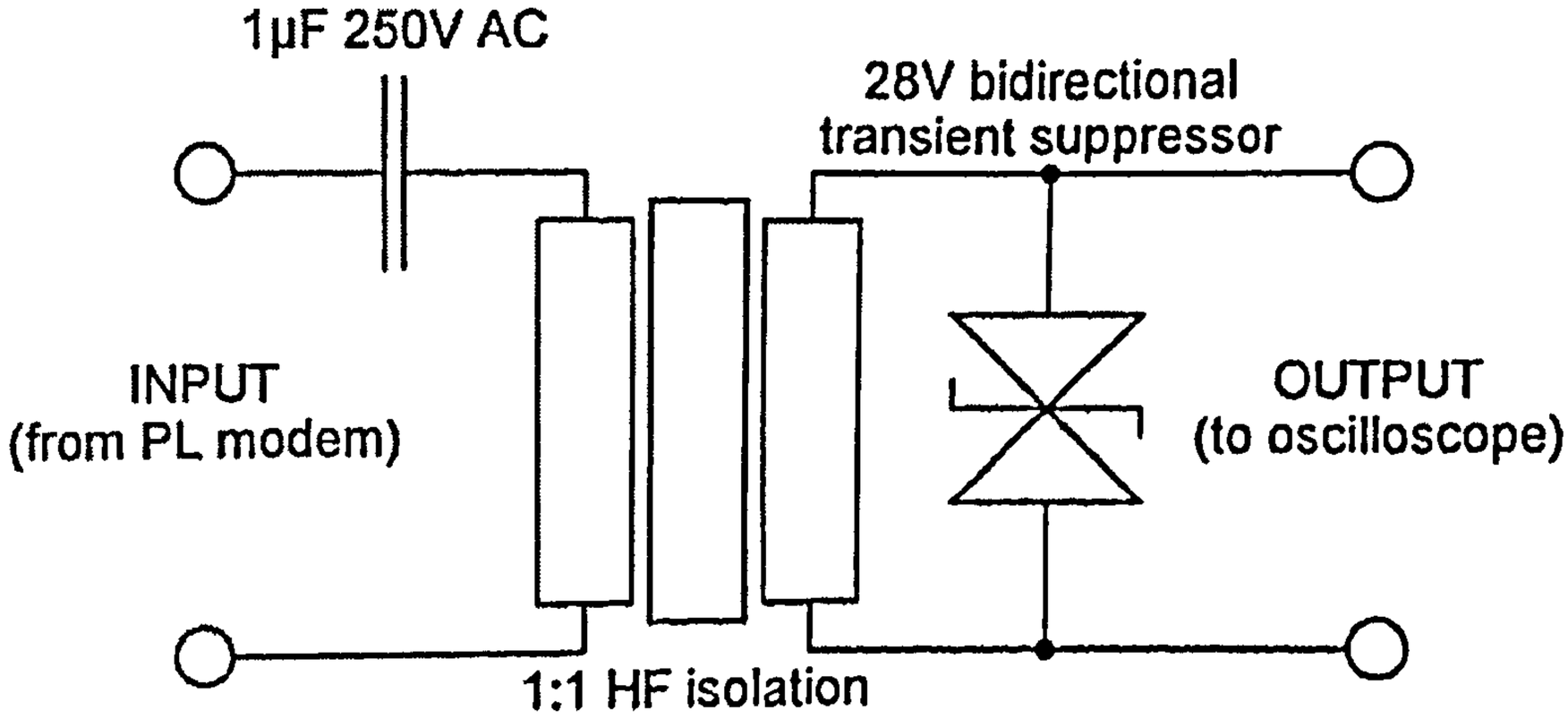


Figure 86: The Isolating Circuit used for Mains Signal Measurement

Using the above arrangement, the following values were measured:

TDA5051 Power Line Modem:	Measured Input (at Rx primary):		Measured Output (at Tx primary):	
State:	Pk-to-pk	RMS	Pk-to-pk	RMS
Connected to Power Line:	0.10 V	0.04 V	5.0 V	1.77 V
Transmitter value (unloaded):			3.0 V	1.06 V

Figure 87: 'Real World' Signal Levels for TDA5051

The unloaded transmitter value was measured without the transmitter being connected to the power line. It was intended to permit the effect of the isolating circuit to be gauged by comparing the values with the values already measured in the FTB tests.

For the TDA5051, the unisolated value was 1.21 V RMS, giving a correction factor of 1.21 / 1.06 = 1.14. Using this figure, we can estimate the true transmit output into the factory power line as 1.77 x 1.14 = 2.0 V RMS. Interestingly, this exceeds the unloaded value. Further investigation might provide an answer to this effect, but it may conceivably be due to the interrelationship between the modem mains coupling network and the characteristics of the power line.

Next, looking at the received signal at the Rx modem, applying the correction factor gives us a value of 0.04 x 1.14 = 0.046 V (46 mV) RMS.

ST7537 Power Line Modem:	Measured Input (at Rx primary):		Measured Output (at Tx primary):	
State:	Pk-to-pk	RMS	Pk-to-pk	RMS
Connected to Power Line:	0.15 V	0.05 V	8.0 V	2.84 V
Transmitter value (unloaded):			8.0 V	2.84 V

Figure 88: 'Real World' Signal Levels for ST7537

Moving on to the ST7537, the correction factor this time is 2.06 / 2.84 = 0.73. It is interesting to note that this correction factor is less than one, as the real world transmit value was greater than the value obtained on the bench tests. This different value may perhaps again be attributable to the interrelationship between the modem mains coupling network and the characteristics of the power line.

Anyway, applying this figure us a transmit amplitude of 2.8 x 0.73 = 2.06 V RMS, and it is also noticeable that the figure is not affected by the loading of the factory power line. The receiver value is calculated at 0.05 x 0.73 = 0.037 V (37 mV) RMS.

Referring back to our FTB tests, such receive amplitudes should result in BER values of 0.1 % or lower for the ST7537, equivalent to one bit in 1000 being corrupted. For the TDA5051 the figure is 2 % or lower, equivalent to 2 bits in 100 being corrupted. *These figure assume that the noise present on the power line is similar in nature to that produced by the FTB generator.*

At the end of this Chapter we will discuss what constitutes an acceptable BER value in a real communications scenario, but we will next look at the actual BER results obtained in the 'real world' tests.

The data is presented as follows: Each table of results shows the BER values, averaged over 15 minute time slots, for a working day in a 'typical' light industrial power line environment. The results are then plotted graphically. Results are shown, in turn, for an entire working week for each of the modems under test.

8.4.1 Results for ST7537, Day 1 (Monday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0074312**	1300-1315	**0.0022957**
0915-0930	**0.0090742**	1315-1330	**0.0017431**
0930-0945	**0.0050000**	1330-1345	**0.0032377**
0945-1000	**0.0019266**	1345-1400	**0.0017431**
1000-1015	**0.0032110**	1400-1415	**0.0014692**
1015-1030	**0.0011111**	1415-1430	**0.0018349**
1030-1045	**0.0025688**	1430-1445	**0.0022202**
1045-1100	**0.0027548**	1445-1500	**0.0013774**
1100-1115	**0.0024771**	1500-1515	**0.0016514**
1115-1130	**0.0023148**	1515-1530	**0.0004625**
1130-1145	**0.0017431**	1530-1545	**0.0008257**
1145-1200	**0.0010092**	1545-1600	**0.0009183**
1200-1215	**0.0007401**	1600-1615	**0.0013761**
1215-1230	**0.0018365**	1615-1630	**0.0010082**
1230-1245	**0.0013761**		
1245-1300	**0.0031452**		

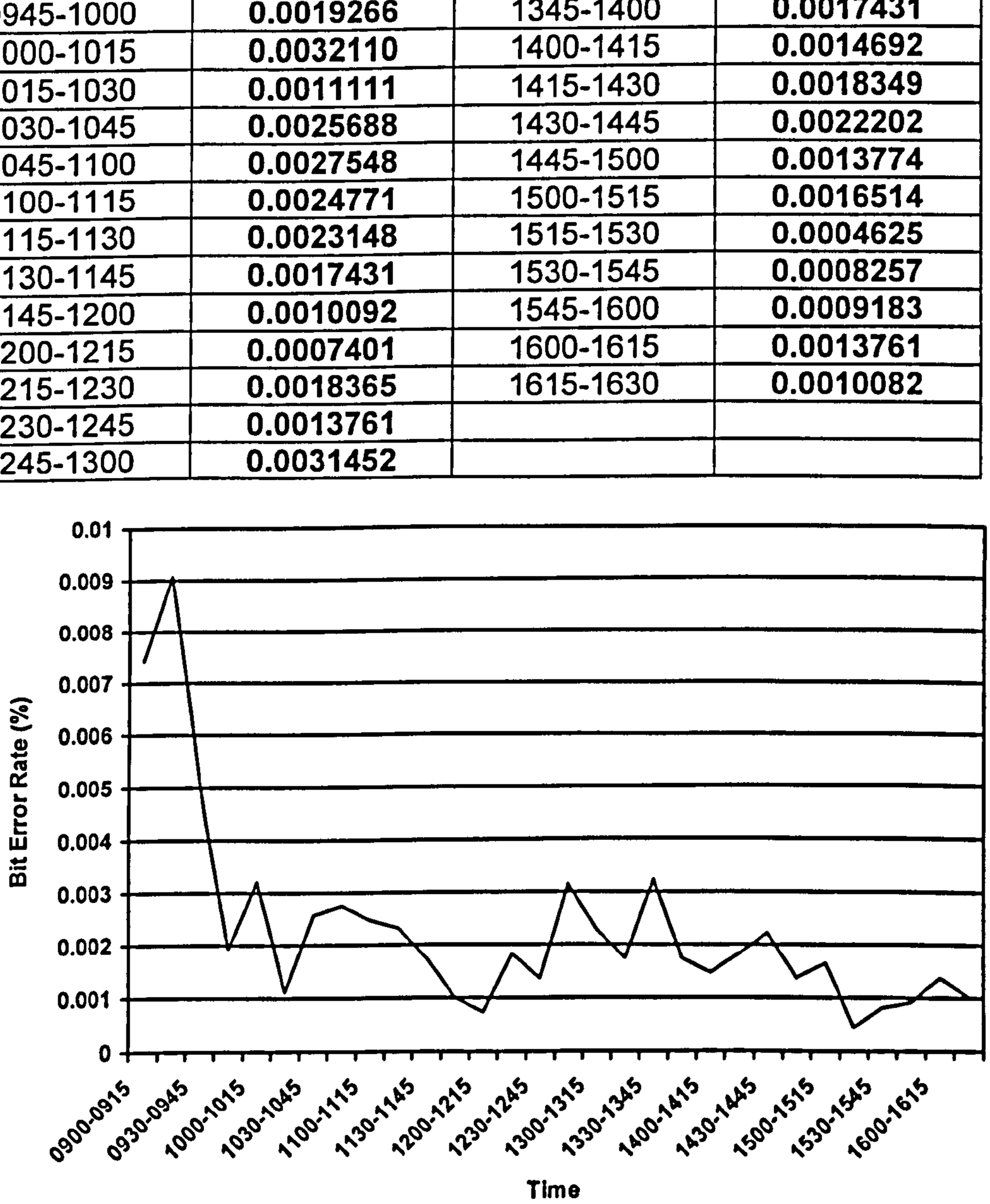


Figure 89: 'Real World' Test Results for ST7537, Day 1 (Monday)

8.4.2 Results for ST7537, Day 2 (Tuesday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	*BER:*	*Time:*	*BER:*
0900-0915	**0.0042202**	1300-1315	**0.0021120**
0915-0930	**0.0027752**	1315-1330	**0.0016514**
0930-0945	**0.0034862**	1330-1345	**0.0019426**
0945-1000	**0.0051423**	1345-1400	**0.0022936**
1000-1015	**0.0037928**	1400-1415	**0.0009183**
1015-1030	**0.0024771**	1415-1430	**0.0011101**
1030-1045	**0.0033058**	1430-1445	**0.0016514**
1045-1100	**0.0030275**	1445-1500	**0.0014692**
1100-1115	**0.0023127**	1500-1515	**0.0017431**
1115-1130	**0.0018365**	1515-1530	**0.0011101**
1130-1145	**0.0021101**	1530-1545	**0.0012844**
1145-1200	**0.0022202**	1545-1600	**0.0010101**
1200-1215	**0.0009174**	1600-1615	**0.0006422**
1215-1230	**0.0011938**	1615-1630	**0.0012026**
1230-1245	**0.0038532**		
1245-1300	**0.0005550**		

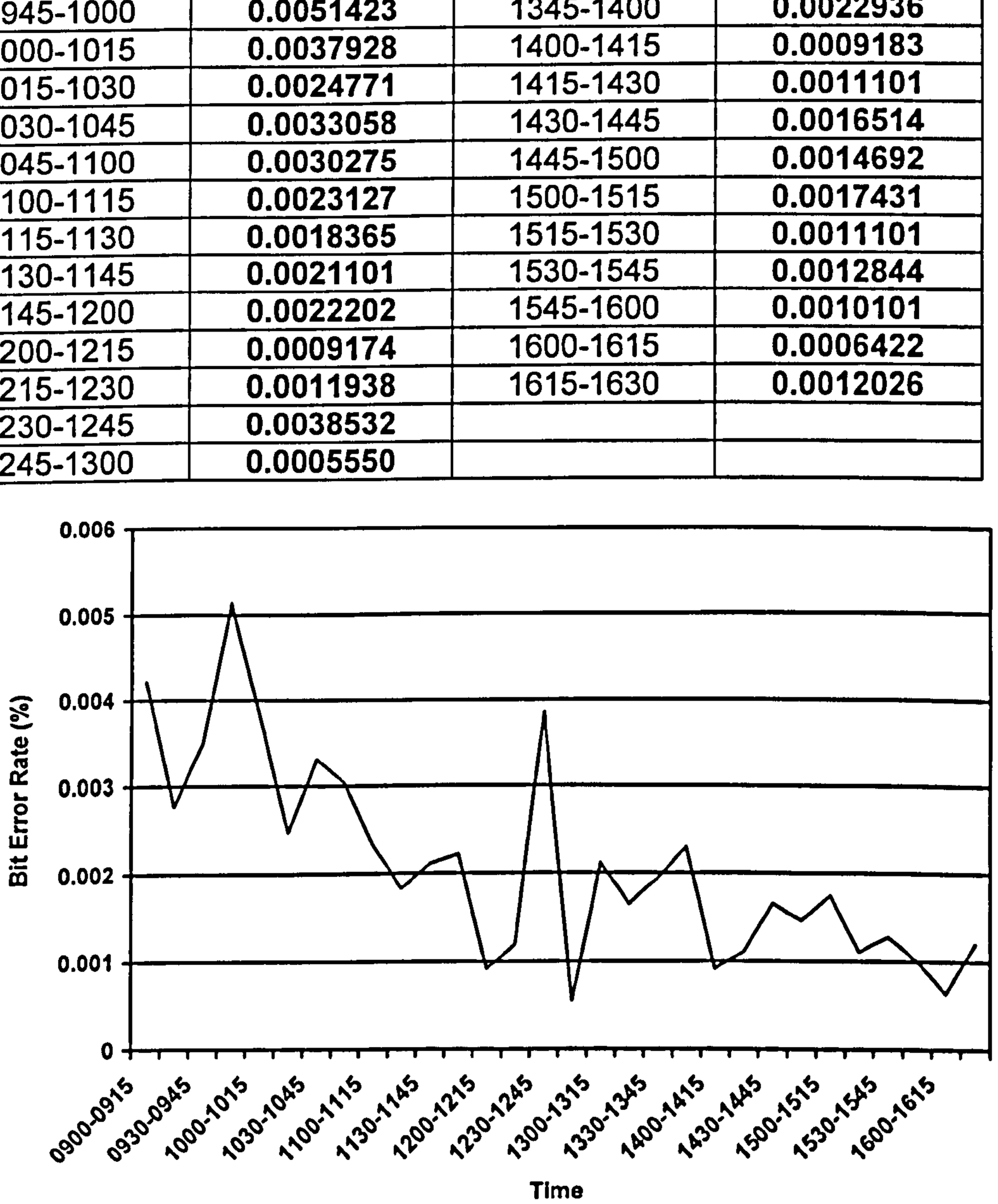


Figure 90: 'Real World' Test Results for ST7537, Day 2 (Tuesday)

8.4.3 Results for ST7537, Day 3 (Wednesday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	*BER:*	*Time:*	*BER:*
0900-0915	**0.0009251**	1300-1315	**0.0009183**
0915-0930	**0.0000000**	1315-1330	**0.0030527**
0930-0945	**0.0006428**	1330-1345	**0.0006422**
0945-1000	**0.0017431**	1345-1400	**0.0000000**
1000-1015	**0.0010176**	1400-1415	**0.0014679**
1015-1030	**0.0021120**	1415-1430	**0.0012026**
1030-1045	**0.0015596**	1430-1445	**0.0002752**
1045-1100	**0.0016651**	1445-1500	**0.0020202**
1100-1115	**0.0006422**	1500-1515	**0.0029602**
1115-1130	**0.0015611**	1515-1530	**0.0026606**
1130-1145	**0.0022936**	1530-1545	**0.0055096**
1145-1200	**0.0017576**	1545-1600	**0.0042202**
1200-1215	**0.0017447**	1600-1615	**0.0074006**
1215-1230	**0.0018349**	1615-1630	**0.0053211**
1230-1245	**0.0032377**		
1245-1300	**0.0016514**		

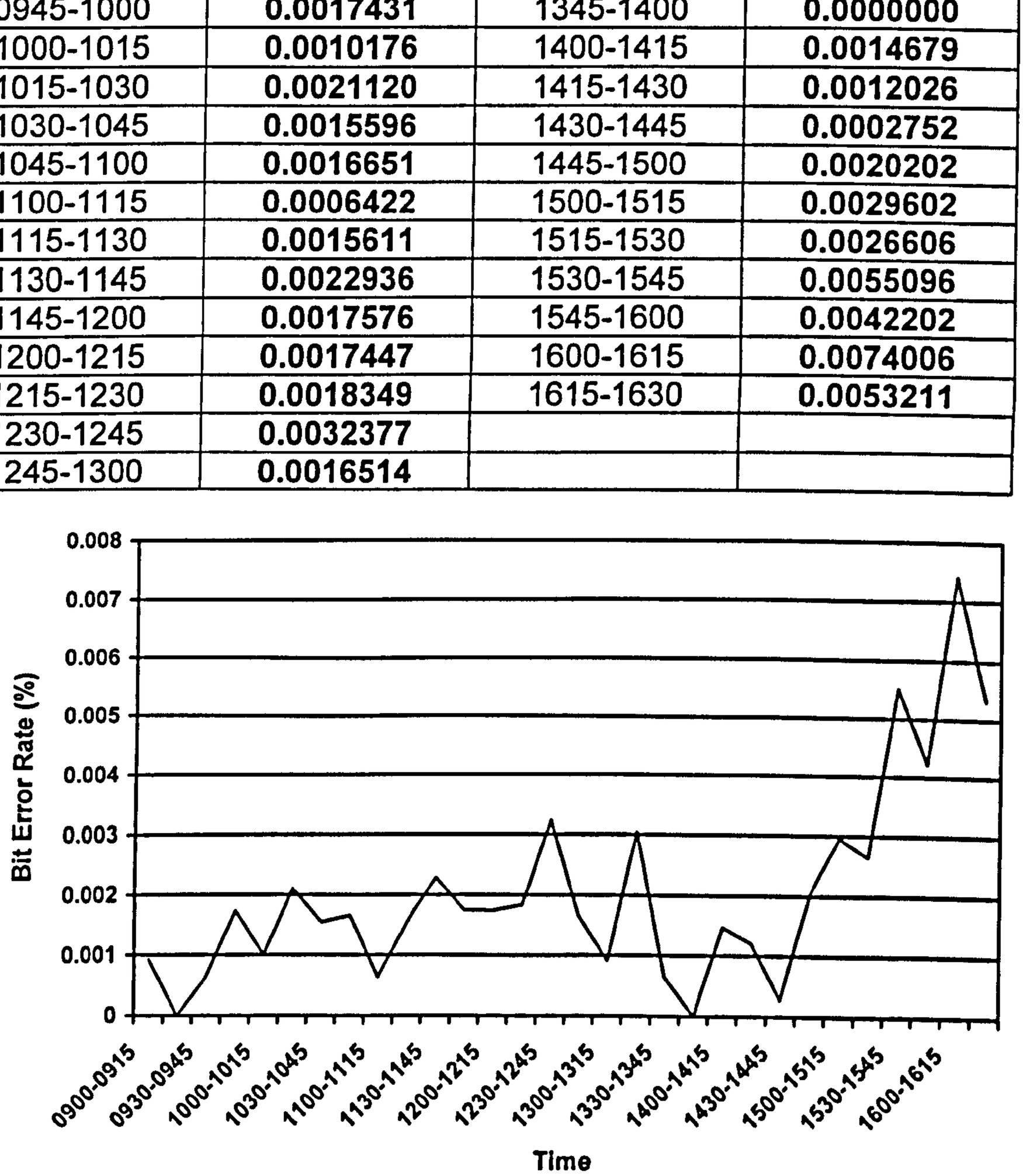


Figure 91: 'Real World' Test Results for ST7537, Day 3 (Wednesday)

8.4.4 Results for ST7537, Day 4 (Thursday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0012026**	1300-1315	**0.0071625**
0915-0930	**0.0022936**	1315-1330	**0.0071560**
0930-0945	**0.0010101**	1330-1345	**0.0057407**
0945-1000	**0.0023853**	1345-1400	**0.0062385**
1000-1015	**0.0026827**	1400-1415	**0.0066055**
1015-1030	**0.0020183**	1415-1430	**0.0076781**
1030-1045	**0.0030303**	1430-1445	**0.0070642**
1045-1100	**0.0003700**	1445-1500	**0.0042241**
1100-1115	**0.0014679**	1500-1515	**0.0081651**
1115-1130	**0.0018365**	1515-1530	**0.0085106**
1130-1145	**0.0038532**	1530-1545	**0.0087236**
1145-1200	**0.0056429**	1545-1600	**0.0053211**
1200-1215	**0.0059688**	1600-1615	**0.0081406**
1215-1230	**0.0052294**	1615-1630	**0.0076147**
1230-1245	**0.0088807**		
1245-1300	**0.0085321**		

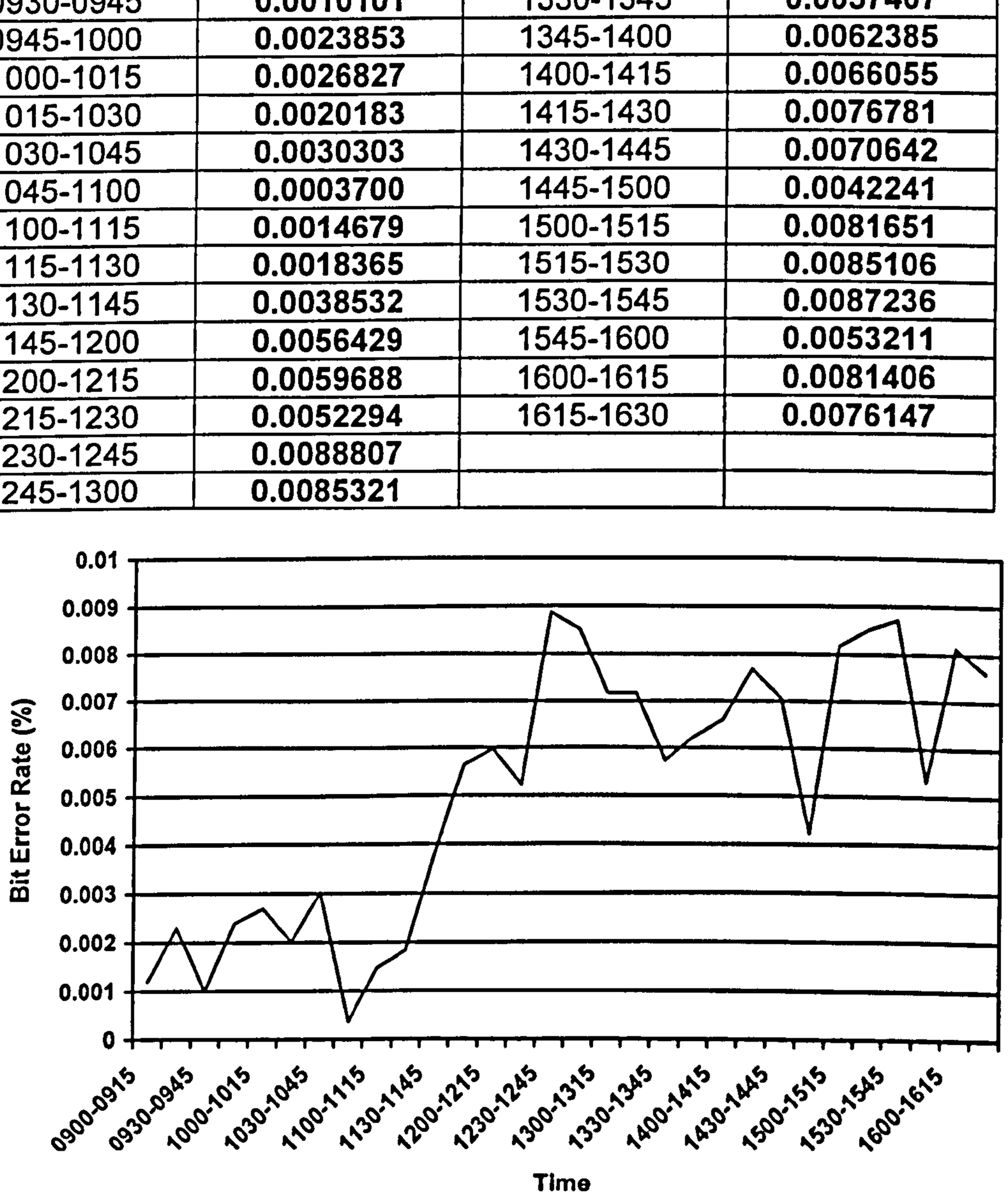


Figure 92: 'Real World' Test Results for ST7537, Day 4 (Thursday)

8.4.5 Results for ST7537, Day 5 (Friday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0074006**	1300-1315	**0.0075856**
0915-0930	**0.0059688**	1315-1330	**0.0070642**
0930-0945	**0.0077982**	1330-1345	**0.0084404**
0945-1000	**0.0054579**	1345-1400	**0.0100092**
1000-1015	**0.0059633**	1400-1415	**0.0060130**
1015-1030	**0.0078972**	1415-1430	**0.0069725**
1030-1045	**0.0086239**	1430-1445	**0.0064279**
1045-1100	**0.0035153**	1445-1500	**0.0024771**
1100-1115	**0.0038567**	1500-1515	**0.0030527**
1115-1130	**0.0018349**	1515-1530	**0.0011927**
1130-1145	**0.0037003**	1530-1545	**0.0011938**
1145-1200	**0.0021101**	1545-1600	**0.0027752**
1200-1215	**0.0063361**	1600-1615	**0.0002752**
1215-1230	**0.0045328**	1615-1630	**0.0016529**
1230-1245	**0.0088073**		
1245-1300	**0.0091827**		

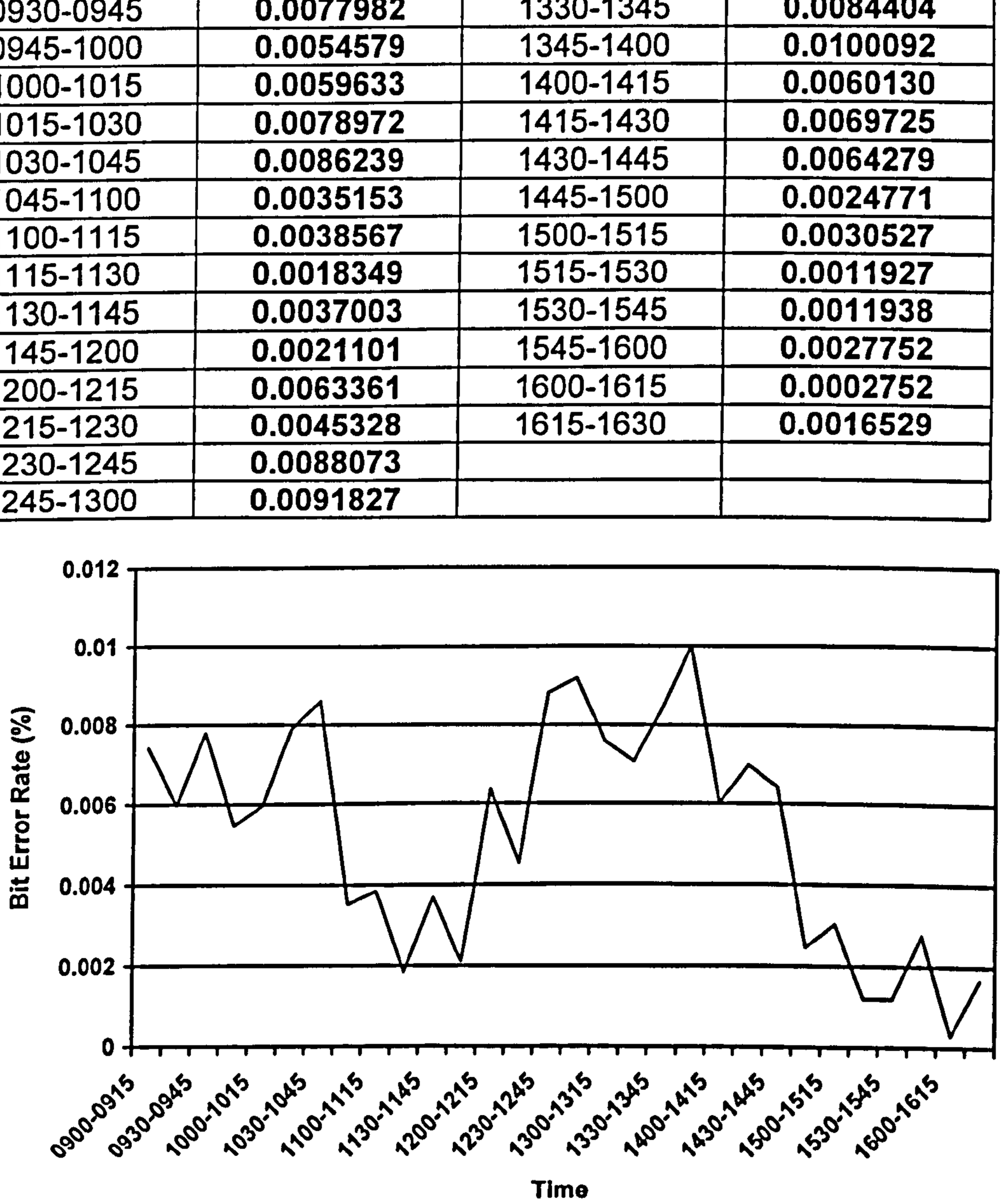


Figure 93: 'Real World' Test Results for ST7537, Day 5 (Friday)

8.4.6 Results for TDA5051, Day 1 (Monday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0006422**	1300-1315	**0.0002752**
0915-0930	**0.0001850**	1315-1330	**0.0009183**
0930-0945	**0.0022936**	1330-1345	**0.0007339**
0945-1000	**0.0005510**	1345-1400	**0.0006475**
1000-1015	**0.0005505**	1400-1415	**0.0000000**
1015-1030	**0.0001850**	1415-1430	**0.0001835**
1030-1045	**0.0008264**	1430-1445	**0.0000000**
1045-1100	**0.0004587**	1445-1500	**0.0001835**
1100-1115	**0.0006475**	1500-1515	**0.0005510**
1115-1130	**0.0002752**	1515-1530	**0.0000000**
1130-1145	**0.0003673**	1530-1545	**0.0000000**
1145-1200	**0.0003670**	1545-1600	**0.0000000**
1200-1215	**0.0009251**	1600-1615	**0.0002752**
1215-1230	**0.0002755**	1615-1630	**0.0000917**
1230-1245	**0.0004587**		
1245-1300	**0.0002775**		

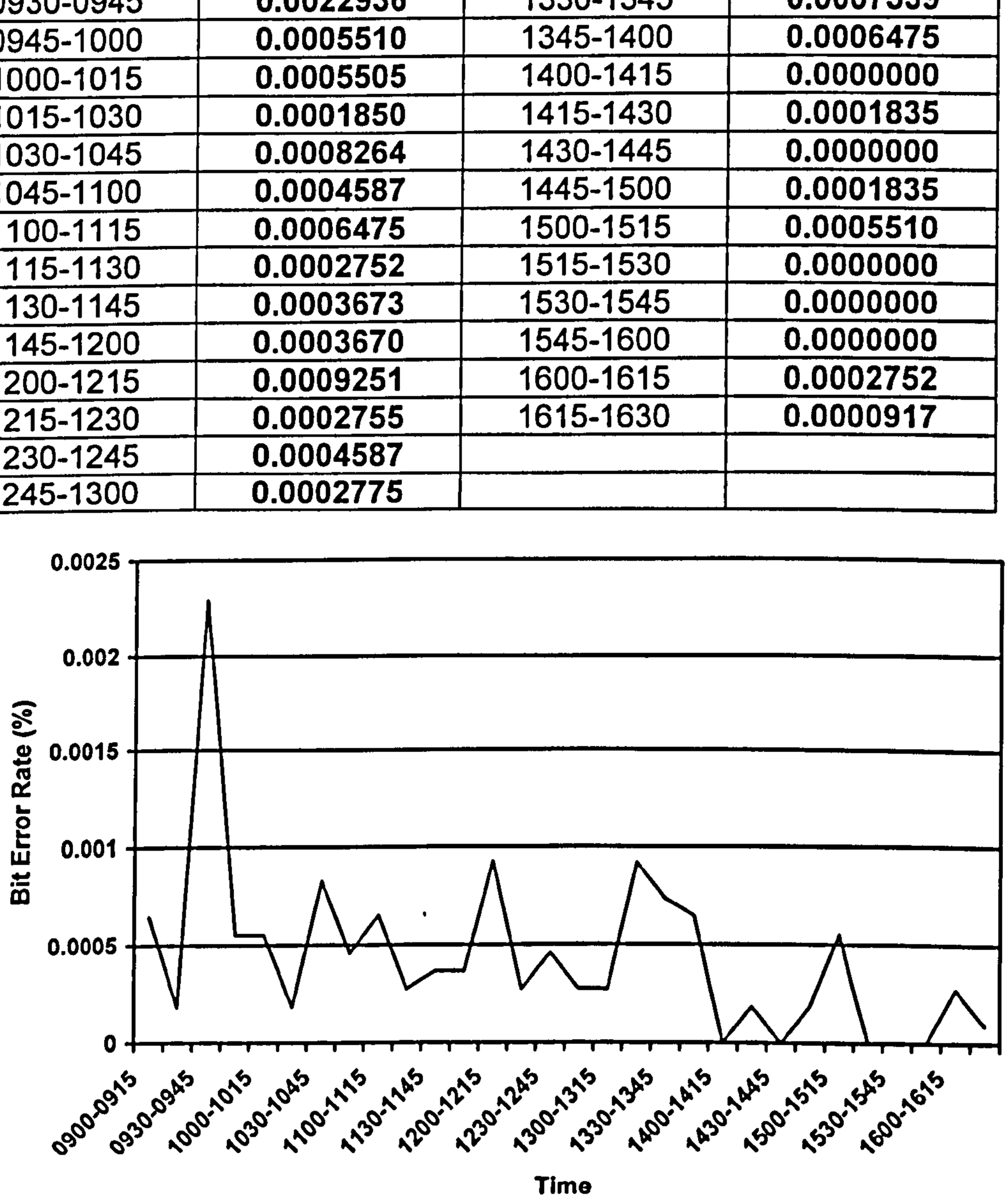


Figure 94: 'Real World' Test Results for TDA5051, Day 1 (Monday)

8.4.7 Results for TDA5051, Day 2 (Tuesday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0000000**	1300-1315	**0.0000000**
0915-0930	**0.0008326**	1315-1330	**0.0005505**
0930-0945	**0.0017447**	1330-1345	**0.0009251**
0945-1000	**0.0000000**	1345-1400	**0.0027548**
1000-1015	**0.0000000**	1400-1415	**0.0002752**
1015-1030	**0.0000000**	1415-1430	**0.0000000**
1030-1045	**0.0001837**	1430-1445	**0.0001850**
1045-1100	**0.0105505**	1445-1500	**0.0002755**
1100-1115	**0.0000000**	1500-1515	**0.0002752**
1115-1130	**0.0006428**	1515-1530	**0.0000925**
1130-1145	**0.0000000**	1530-1545	**0.0003673**
1145-1200	**0.0000925**	1545-1600	**0.0001835**
1200-1215	**0.0004587**	1600-1615	**0.0000000**
1215-1230	**0.0005510**	1615-1630	**0.1924771**
1230-1245	**0.0001835**		
1245-1300	**0.0000000**		

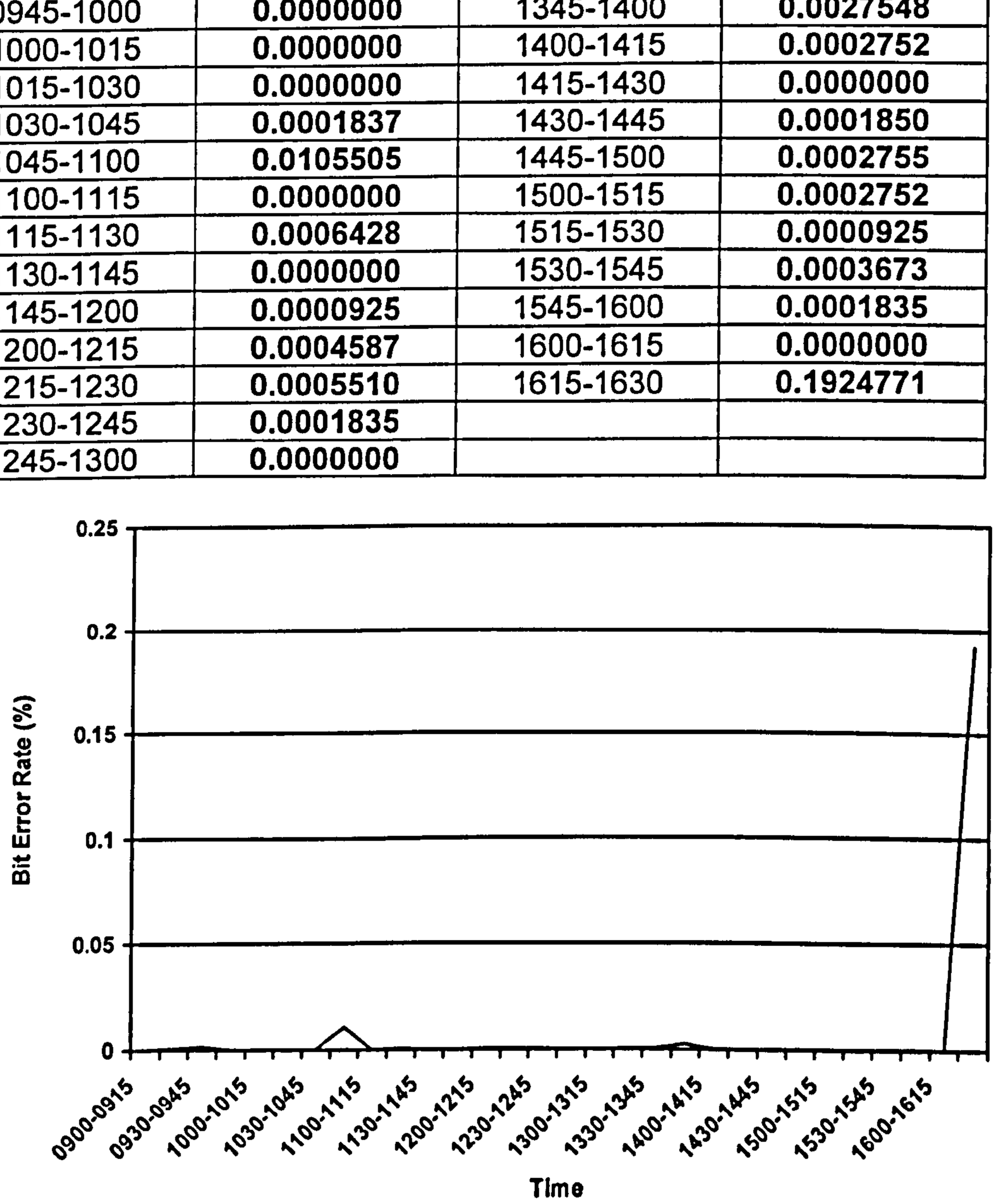


Figure 95: 'Real World' Test Results for TDA5051, Day 2 (Tuesday)

8.4.8 Results for TDA5051, Day 3 (Wednesday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0007346**	1300-1315	**0.0000000**
0915-0930	**0.0010176**	1315-1330	**0.0011938**
0930-0945	**0.0001835**	1330-1345	**0.0003700**
0945-1000	**0.0001837**	1345-1400	**0.0019266**
1000-1015	**0.0000000**	1400-1415	**0.0000918**
1015-1030	**0.0004625**	1415-1430	**0.0037615**
1030-1045	**0.0000000**	1430-1445	**0.0007401**
1045-1100	**0.0000917**	1445-1500	**0.0008257**
1100-1115	**0.0004625**	1500-1515	**0.0004591**
1115-1130	**0.0001835**	1515-1530	**0.0008257**
1130-1145	**0.0005510**	1530-1545	**0.0081406**
1145-1200	**0.0001835**	1545-1600	**0.0258953**
1200-1215	**0.0002775**	1600-1615	**0.0007339**
1215-1230	**0.0003673**	1615-1630	**0.0001850**
1230-1245	**0.0000000**		
1245-1300	**0.0000000**		

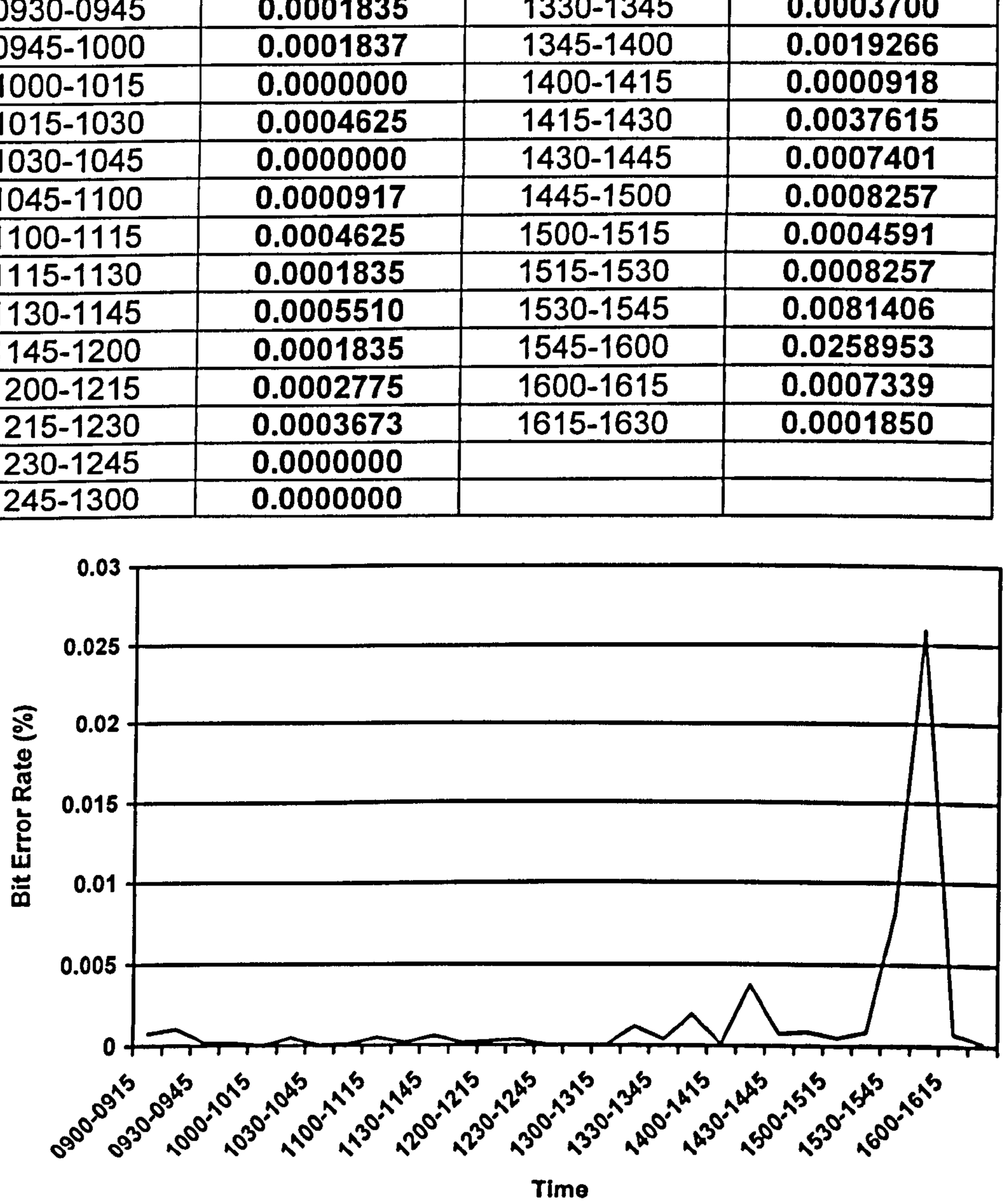


Figure 96: 'Real World' Test Results for TDA5051, Day 3 (Wednesday)

8.4.9 Results for TDA5051, Day 4 (Thursday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0014692**	1300-1315	**0.0005505**
0915-0930	**0.0000000**	1315-1330	**0.0001837**
0930-0945	**0.0004587**	1330-1345	**0.0007339**
0945-1000	**0.0000000**	1345-1400	**0.0001850**
1000-1015	**0.0000917**	1400-1415	**0.0000000**
1015-1030	**0.0000000**	1415-1430	**0.0001835**
1030-1045	**0.0002755**	1430-1445	**0.0003700**
1045-1100	**0.0004587**	1445-1500	**0.0013774**
1100-1115	**0.0005550**	1500-1515	**0.0002752**
1115-1130	**0.0001835**	1515-1530	**0.0009174**
1130-1145	**0.0003673**	1530-1545	**0.0008326**
1145-1200	**0.0001835**	1545-1600	**0.0033976**
1200-1215	**0.0007401**	1600-1615	**0.0004587**
1215-1230	**0.0000917**	1615-1630	**0.0002775**
1230-1245	**0.0003704**		
1245-1300	**0.0005505**		

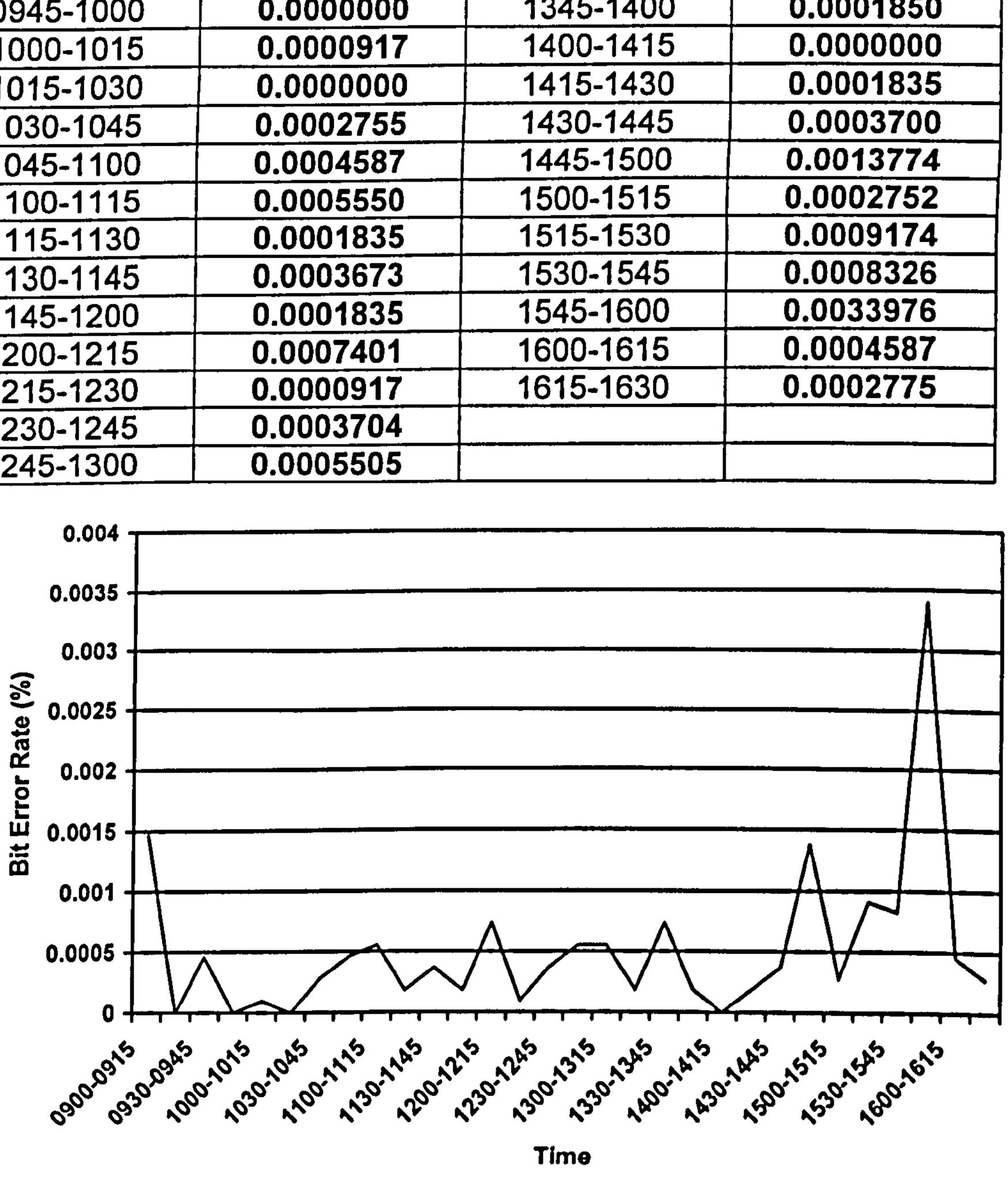


Figure 97: 'Real World' Test Results for TDA5051, Day 4 (Thursday)

8.4.10 Results for TDA5051, Day 5 (Friday)

The following data shows the measured BER, averaged over 15 minute time slots, over a working day in a 'typical' light industrial power line environment.

Time:	BER:	Time:	BER:
0900-0915	**0.0013876**	1300-1315	**0.0002752**
0915-0930	**0.0002755**	1315-1330	**0.0000000**
0930-0945	**0.0000917**	1330-1345	**0.0004587**
0945-1000	**0.0000000**	1345-1400	**0.0000918**
1000-1015	**0.0008257**	1400-1415	**0.0005550**
1015-1030	**0.0107438**	1415-1430	**0.0000000**
1030-1045	**0.0003670**	1430-1445	**0.0002755**
1045-1100	**0.0003700**	1445-1500	**0.0000917**
1100-1115	**0.0001837**	1500-1515	**0.0004625**
1115-1130	**0.0002752**	1515-1530	**0.0057798**
1130-1145	**0.0000925**	1530-1545	**0.0000000**
1145-1200	**0.0006422**	1545-1600	**0.0000925**
1200-1215	**0.0004591**	1600-1615	**0.0001835**
1215-1230	**0.0007339**	1615-1630	**0.0000000**
1230-1245	**0.0003700**		
1245-1300	**0.0017447**		

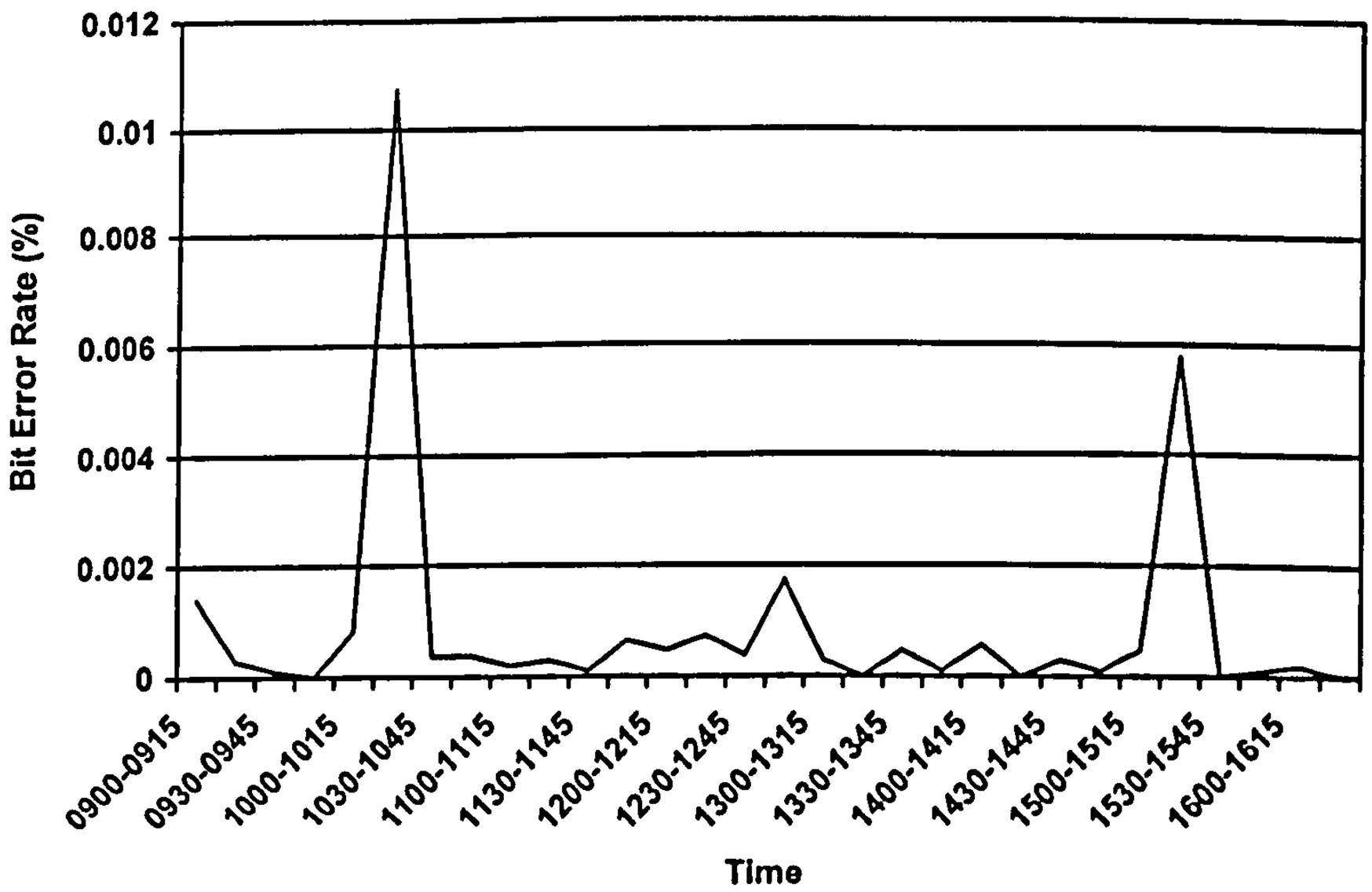


Figure 98: 'Real World' Test Results for TDA5051, Day 5 (Friday)

8.4.11 Analysis of 'Real World' BER Test Results

Looking at the results for the real world tests, we can make the following comments.

- The BER values measured are a lot less than might be expected, based on the FTB BER test results. This suggests that the noise levels experienced in the factory environment are generally significantly less harsh.

- The results for the TDA5051 are in some respects (which will be discussed later) *better* than those for the ST7537.

The ST7537, for example, shows a peak BER value (averaged over 15 minute time slots) of 0.01 %. This represents one corrupted bit in 10000. For the rest of the test period, BER values were at or below typically 0.003 % (three bits in 100000 corrupted).

The TDA5051, on the other hand, showed a peak BER value of 0.12 %, representing 12 corrupted bits in 10000. Aside from a few lesser peaks, the rest of the BER values tended to 0.001 % or less (one bit in 100000), in other words, better than the ST7537! Further research would be required try and ascertain why this should be so.

Study of the raw data for these tests shows that these peak values for the TDA5051 were a results of incidents of high errors over just one or two 1000 bit samples within the 15 minute time frame.

We can postulate, then that events occurred on the power line at these points that the TDA5051 was unable to withstand, resulting in the high data loss. We cannot speculate as to the exact nature of the events, and it would be a subject for further experimental tests to try and profile the noise characteristics.

Since the real world tests analysed took place on different weeks, we cannot absolutely guarantee that the noise levels would be comparable, although, since an entire weekly time frame was involved in each, they should at least have been similar. The only way around this shortcoming would be to produce a 'dual channel' BERT, capable of handling two PL modems simultaneously on the same power line. Either, each modem would pass a 1000 bit sequence in turn (although even this arrangement might miss short duration transient events), or (preferably) both modems would run simultaneously, passing identical data. This latter arrangement would require the modems to operate in exclusive frequency bands, to avoid mutual interference (of course, our modems already do this, as the TDA5051 carrier is at 115 kHz, and the ST7537 is centred around 132.5 kHz). The development of such an improved BERT is beyond the scope of this initial research, but will be further discussed in the next chapter.

8.5 Conclusions

To finish this chapter we will look how our results fit in to our proposed industrial application of PLC techniques.

In terms of the FTB test BER values alone it is evident that the ST7537 modem offers the better performance under almost all circumstances. This does not necessarily rule out the TDA5051 as will be explained next.

Taking as an example our HART data packet, which we analysed in a previous chapter. We have already calculated that a 'typical' HART packet might contain between 110 and 616 bits.

Since we will not be employing any error correction techniques, corrupted packets must be re-transmitted. In other words, a data packet must get through the communications link uncorrupted, and preferably without too many retries, within our response time frame of 1 to 2 s.

If a transmission link has a BER of 1%, it implies that in a sample of (say) 1000 bits there are likely to be 10 corrupted bits. From our experimental results, this BER is achievable for the ST7537 for all FTB amplitudes, at signal levels above 20 mV. Even the generally lower performing TDA5051 can achieve it above 20 mV for all but the most stringent (2 kV) FTB amplitude.

These corrupted bits could be contiguous, i.e. all together in a bunch, or might be evenly spaced over time. In the former instance, it implies that there should be a clear run of 990 bits with no interference, and in the latter a clear run of only 99 bits. Our example data packets would, in theory, be able to pass over the communications link with the former noise profile, but not with the latter. A small reduction in the minimum packet size would allow these to pass even with the latter noise profile.

Looking at the structure of the actual FTB noise signal, discussed in an earlier chapter, we can see that the 15 ms blocks of noise pulses are separated by 285 ms gaps. This does not however imply that all of the corrupted bits associated with the FTB waveform will occur during the noise period, and there will be the opportunity for 285 ms of clean transmission. For example, the TDA5051 automatic gain control system will likely react to the noise pulses, and take a finite time to recover afterwards, during which reliable communication might not be guaranteed. Also, it must be remembered that the FTB pulse train is a 'generic' waveform (designed by committee!), easy to replicate, but not necessarily indicative of noise in the real world. Real world noise is likely to be much less deterministic.

To make any judgements we would also need to ascertain the determinism of the 'real' power line noise. Such tests are beyond the scope of this initial work, but are another line for further experimentation.

To summarise then:

- Our experimental results have shown that we can achieve usable BER values with either of the PL modems evaluated.
- Our 'real world' tests have shown that actual BER values are likely to be lower than those achieved in the bench experiments.

Overall, our initial round of experimentation strongly suggests that PLC systems have a place in an industrial control scenario. We can achieve suitably low BER rates without special precautions, and have the scope to improve the power line noise environment further, utilising filters and similar techniques

That concludes our analysis of the results of this experimental work. We have touched on the need to analyse the noise profile of the industrial power line environment in more detail, and also to tailor our final choice of protocol and packet structure to that environment. We will further consider these, and the other additional lines of experimentation that have suggested themselves, in the next chapter, before concluding this Thesis with a look at other aspects of the future of power line communications.

Chapter 9 : Future Developments

We will conclude this Thesis with a look at the future, from various viewpoints. We will look at the directions in which our research could be continued (some of which have already been touched upon) and at enhancements that might be made to the BERT equipment, developed as a part of this research. Finally, we will look at some of the other directions in which PLC research and technologies are being applied.

9.1 Additional Topics for Research

The results obtained so far indicate that PLC does have a potential for use within an industrial environment. We have ascertained that communication is achievable with an acceptably low error rate, and at a signalling rate sufficient for carrying out control functions within an appropriate time-scale.

In the course of the experimental work carried out in this research, we have raised many questions that would benefit from additional investigation. We will firstly look at questions arising *directly* from the experimental work already carried out, before looking at future directions which the research might take.

9.1.1 Topics Arising Directly From the Experiments Carried Out

- In the real world tests, it was notable that the ST7537 performed (on average) somewhat worse than the TDA5051, despite the fact that theory would suggest the opposite. Of course, the actual levels experienced were sufficiently low that reliable communications would be perfectly feasible with either modem. Nevertheless, it would be useful to try and establish why this should be so.

- There were several other instances of somewhat anomalous results, which would also warrant further investigation, viz:

  - For the ST7537 FTB tests, why negative amplitude tests tended to produce noticeably lower BER values than positive amplitude tests at the same test voltage. This effect was much less evident with the TDA5051, but when noted tended to be the opposite sense – i.e. positive FTB tests produced a slightly lower BER value than negative.

  - For the spot frequency tests, why unexpected types of bit error (logic '0', or logic '1') were found, when a simple prediction of the effect of the noise suggested that only one bit level would be affected.

  - The variation of the noise susceptibility bandwidth of the TDA5051 in the presence of different input signal levels.

- All of the above effects warrant a closer look at the internal operation of each modem, with specific attention paid to some of the (modern) signal processing techniques employed, in an effort to achieve an explanation.

We will now take a broader outlook, and consider entire new lines of research that might be pursued.

9.1.2 Other Lines of Research

- To perform tests to gauge the nature of the power line noise within the industrial environment, and its determinism (or otherwise). This would certainly require additional, specialised, test equipment, not available to the author. It may be an additional opportunity to develop custom-built equipment, as has already been done with the BERT equipment used in this Thesis.

- In our 'real world' tests, we noted some unusual effects when the modems were coupled to the power line, regarding the change in the signal amplitude. It would therefore be worthwhile to investigate the effectiveness of the coupling circuitry between the PL modems and the power line, as well as attempting to measure the actual impedance values for the power line.

- Having carried out tests at the basic physical layer of the OSI model, the next step would be to consider the most appropriate choice of protocols. A theoretical evaluation could be backed up by a new series of experiments to assess the performance of the protocols under noise conditions.

- Once we start to incorporate a protocol in the communications link, the way would be opened to experiment with some of the more highly integrated modem chipsets.

- Finally, we would evaluate the advantages to be gained by the systematic use of filters, from the point of view of both decreasing noise levels and optimising the power line impedance.

An integral part of our experimental work was the BERT equipment. We will next discuss improvements and enhancements that might be made to this equipment.

9.2 Further Development of the BERT Equipment

The BERT equipment was designed specifically to assist in the experimental work for this Thesis. However, it has the potential to be used as an item of general purpose test equipment for power-line (or indeed, general) communications use.

The most notable limitation is the fact that the BERT is currently in prototype format, constructed on an open breadboard. It would certainly be advantageous to package the device in a secure manner. We have already discussed the fact that isolation circuitry needed to be included in the BERT for it to operate under the experimental FTB noise conditions. Even with the isolators, the standard BERT was still vulnerable to FTB levels of 4 kV. This was not a problem with our experiments, as the standards only required a maximum FTB level of 2 kV. However, it does indicate the pervasiveness of electromagnetic noise, and packaging the BERT equipment properly, with due attention paid to screening and filtering on the power and data lines, would almost certainly be advantageous.

Beyond these 'cosmetic' and EMC issues, the basic design of the BERT could be refined further for improved functionality:

- We have already mentioned that it would be desirable to create a twin channel BERT. This would be capable of simultaneous testing of two modems in a real world scenario, on the same power line, thus providing improved confidence in the real world results.

- We have also mentioned the incorporation of protocols in our experimentation. If we are to use the BERT equipment in these advanced tests, it must accommodate this. It would be feasible for the BERT equipment to handle the assembly and disassembly of data packets, in the format of various protocols, and to provide BER results to the user. Indeed, this is a function available in many commercial bit error rate testers. When dealing with integrated PL modem chip-sets, that incorporate their own protocol-handling microcontrollers, the BERT must handle and analyse the outputs from these, in whatever format the might be, in order to evaluate the link performance.

The changes proposed above would require significant enhancements to the hardware and software of the BERT front-end system. It would be necessary to consider if the simple PIC16F84 microcontroller has sufficient resources for this task. There are more advanced members of the PIC family available, that might be suitable, or it may even be necessary to go to a PC-based solution for the BERT hardware.

That concludes our discussion of enhancements to the BERT equipment. An important concept, used as the backbone of our research effort, is the 'Power Bus'. We will next look at potential further work in this specific area.

9.3 Further Development of the 'Power Bus' Concept

So far, we have evaluated some practical PL modem solutions suitable for our 'Power Bus' concept, and have proposed new lines of relevant research, such as investigating the performance of protocols.

Whilst future research may involve other types of PL modem, the two evaluated (ASK and FSK) are perfectly adequate for our purpose. Looking at the requirements from a practical viewpoint, our power bus node must be a compact device, as it may be fitted into a small item of equipment on the industrial plant. It may even have to be retrofitted to an existing item of equipment, where available space may be even more at a premium.

In addition, it must be remembered that a practical power bus node will require additional circuit elements above and beyond the modem itself:

- A power supply, probably derived from the power line itself. For simple devices, this may be stand-alone, and might not even require a mains transformer. Devices that are more complex (perhaps already incorporating electronics) may have their own power supply available.
- Some 'intelligence'. This will probably be a microcontroller, and so will be small in its own right. If a node is to be incorporated into an existing item of microcontroller based equipment, the main controller may have sufficient spare resources to handle the extra facilities.
- Interfacing elements to the items to be controlled or monitored (which will obviously depend on the complexity of the device with which the node is associated).

- A power line interface. This is usually built into the modem, but in a practical realisation may also incorporate line conditioning and filtering elements, which we have already discussed.

The authors' own preferences, from a practical engineering point of view, tend to lie with the TDA5051 modem, despite its (theoretically) poorer performance. The ST7537 requires a much greater amount of support circuitry, not to mention two power supply voltages. The TDA5051, on the other hand, is highly integrated, easily coupled to the power line, and only requires a single 5 V power supply.

Before concluding this final look at the 'Power Bus' concept, we must consider another important factor in any potential industrial application – safety and fault tolerance.

9.3.1 The Power Bus and 'Safety Critical' Systems

Within the realm of control systems, the term 'safety critical' refers to instances where equipment must be 'fail-safe'. The term fail-safe broadly implies that a system must, in the presence of one (or more) faults either:

- Continue to operate normally.
- Shut down to a safe state in a controlled fashion.

In either of the above examples, the equipment should ideally flag that a fault has occurred, in order that remedial action may be taken. 'Faults' within the context of an electronic system generally refer to the failure of individual components within the system.

The author has previously carried out research on the techniques applicable to the design of a fault tolerant microprocessor-based controller for safety critical applications [60].

The field of burner control, which we have used as an example of a potential 'power bus' application, is itself classed as a safety critical application (and indeed, this same subject area was chosen by the author in his previous work).

During this work, a burner controller was developed which was designed to be tolerant of single faults within its circuitry. The design was 'conventional' insofar as it interfaced with the various peripheral I/O devices over discrete wiring. In keeping with the certification requirements of a national testing body for this type of equipment (British Gas), the design was intended to function safely in the presence of any one fault [61].

Since the original work was carried out, standards covering the performance and operation of such controllers have been expanded to encompass the use of 'complex electronics', such as microcontrollers, in their design. The standard now lays down the component failure modes and test regimes that must be applied [62].

Should we wish to expand this to realise a practical burner control system utilising the 'power bus' concept to communicate with its various peripheral devices, we must apply similar levels of fault tolerance to the communications link.

We must not only consider the availability of the link, under all noise conditions, but must also consider the reliability of the circuitry of the power bus nodes themselves. It is likely that we will need to have 'fall-back' scenarios - perhaps involving multiple communications techniques over the same power line, and redundant or fault tolerant hardware in the nodes. In the event of catastrophic loss of the communications link, nodes would have to act autonomously, and to gracefully shut down their particular part of the overall control scheme.

All in all, the author considers that looking at PLC from the point of view of safety critical systems would offer an exciting and worthwhile line of future research.

That concludes our look at possible future research and experimentation work. We will conclude this thesis by taking an overview of developments in the power line communications field today, with special consideration given to the emergent field of high speed PLC systems.

9.4 High Speed Power Line Communications

The PLC techniques that we have discussed so far in this research are in line with the recommendations of the EN 50065 family of standards.

EN 50065 specifies discrete operational bands within the frequency range 9 kHz to 148.5 kHz, and in our work we have been specifically concentrating on the sub band of 125 to 140 kHz. The modem techniques we have been using only provide relatively low signalling rates. Whilst these rates are lower than the theoretical limits for a given communications channel, defined by researchers such as Shannon [63], they are nevertheless quite sufficient for the types of industrial control application that we are considering.

Even if we could make use of the entire bandwidth available, and the channel characteristics were perfect, we could not achieve signalling rates much above 15 kilo-baud, given the bandwidths available (for the band 125 to 140 kHz).

However, efforts are being made to establish PLC systems working at frequencies considerably above the 148.5 kHz frequency limit of EN 50065. As suggested above, the principle advantage of utilising higher frequencies is that they offer the potential for higher data rates. It has been suggested that such high speed PLC systems might be utilised as a convenient means of providing high-speed Internet access [64] by providing a link between a building and a central node (perhaps at a local electricity sub-station). In addition, within a home or building, high speed PLC has been cited as a means of achieving a LAN facility without the need for additional wiring.

9.4.1 Potential Disadvantages of High Speed PLC Systems

Such applications have drawbacks insofar as they must utilise higher carrier frequencies to achieve that data rates desired. We have already discussed the undisciplined topology of the mains distribution network and the mains wiring from the viewpoint of the transmission of higher frequency signals. In this instance, we are also working at frequencies that coincide with other services such as radio broadcasting. This has implications from both the emission and immunity standpoints. The PLC signals may be radiated from the power lines, disturbing radio broadcast signals, or the power lines may act as receiving antennae, picking up radio broadcasts, which might in turn compromise the PLC signals.

Work has been done [65] to evaluate the likely radiated signals from a high speed PLC system proposed for providing Internet connectivity. The study also worked with a system called 'Asymmetrical Digital Subscriber Line' (ADSL), another new means of high speed digital communication utilising existing copper telephone lines as the medium. Techniques for telephone cabling, by the nature of their intended function (the carrying of voice traffic), at least pay some attention to avoiding the pick-up of extraneous noise.

Such precautions will also improve emission characteristics, even when these telephone cables are carrying the much higher frequency ADSL signal, and it was found that relatively little extraneous radiation was produced. It should be noted, though, that the amounts involved are not considered *in*significant by various authorities, as will be discussed in the next section).

The PLC system, on the other hand, was much more problematical, especially at points, such as at the feeds to street lighting, where the cables have to move from below ground to above ground level. Within a building, where the majority of the power line wiring will already be above ground level and unshielded, the situation could be expected to be worse.

Consequently, there is great controversy surrounding these proposals for high speed PLC, which we will look at in the next section.

9.4.2 High Speed PLC and Radio Communications

The frequency bands specified in EN 50065 generally lie outside the bands used for radio communications. There are exceptions - radio time code signals are transmitted at frequencies within this band (for example, at 60 kHz from Rugby in the UK). In addition, Radio Amateurs are permitted to utilise frequencies within this band, specifically, 137 kHz. However, the nature of radio propagation at these low frequencies (LF) means that high transmission powers are required, so the low power levels used in PLC are unlikely to cause problems to these activities, and vice-versa. Conversely, once we go above 148.5 kHz we are well and truly within the realm of radio communications.

Technically, the band from 30 kHz to 300 kHz, encompassing the EN 50065 frequencies, is referred to as 'Low Frequency' (LF). The band from 300 kHz to 3 MHz is referred to as 'Medium Frequency' (MF), and the band from 3 MHz to 30 MHz is termed 'High Frequency' (HF). However, any PLC system operating above 148.5 kHz tends to be referred to as 'HF', so for convenience we will use this convention.

We have already mentioned the Intellon 'Chirp' system of spread spectrum, which occupies a bandwidth from 100 kHz to 400 kHz. Within the USA, where the system originated, and is utilised as a part of the CE-Bus system, MF broadcast radio stations begin at higher frequencies. However, in the UK and Europe, this is not the case, with many stations occupying this part of the frequency band.

The typical frequency band mooted for HF PLC systems is in the 1 MHz - 30 MHz area. This clearly covers the entire HF radio spectrum, and the upper part of the MF spectrum.

As a result of their studies, the authors of the Smith Group report [65] concluded that HF PLC would be likely to produce excessive levels of RF pollution, causing problems or disruptions to amateur and commercial radio services.

Such is the concern at the potential effects of HF PLC systems (and, it must be stated ADSL and similar technologies), that great concern is being shown by groups representing users of the radio spectrum.

The Radio Society of Great Britain (RSGB), which represents the interests of Amateur Radio in the UK, have raised serious reservations about the introduction of HF PLC systems [66], citing the fact that the likely signal levels involved in HF PLC will exceed the levels permitted under the terms of the EMC emissions standards.

The European Radiocommunications Committee (ERC), part of the European Conference of Postal and Telecommunications Administrations (CEPT), have also produced a report [67] which highlights the fact that the HF radio spectrum is still a greatly utilised resource in Europe.

Both organisations believe that the widespread introduction of such communications systems will jeopardise all HF radio communication activities, both commercial and amateur.

Surrounded as it is by such controversy, we will nevertheless now outline some of the initiatives and techniques proposed for HF PLC systems.

9.4.3 Some HF PLC Solutions

The list presented here is not intended to be exhaustive, but to give the reader an idea of the direction in which HF PLC is being pursued by various organisations. It is interesting to note that some organisations such as Nortel Networks have, after great initial enthusiasm, already given up on the concept of HF PLC, after deciding that the idea doesn't have market potential.

The 'Home Plug Alliance'

This is a non-profit making industry association consists of a number of interested parties from the fields of retailing, hardware and software, services, semiconductor technology and consumer electronics. It was formed early in the year 2000 with the stated aim of achieving a 10 Mbps, Ethernet class connection over a domestic mains network.

PolyTrax

PolyTrax Information Technology are a German company who, in association with Hitachi in Japan, have developed a PLC solution operating at a transmission rate of 2.4 Mbps maximum, with a claimed average rate of 1.5 Mbps achievable even under high noise conditions.

Main.net

Main.net is an Israeli organisation offering high-speed PLC solutions. The systems made by Main.net use frequencies between 1 MHz and 30 MHz to send data from the home to the local power substation at rates of up to 2.5 Mbps.

Local power companies in Germany are already utilising Main.net technology to provide Internet connections to its customers.

Itran

Itran are also an Israeli company, and have developed a range of sophisticated PL modem devices based on advanced ASIC (Application Specific Integrated Circuit) techniques.

Their devices range in speed up to a maximum of 24 Mbps. Their modems (as indeed do a number of other high speed PLC systems) utilise a modulation technique called Orthogonal Frequency Division Multiplex (OFDM). This is a rather complex scheme incorporating multiple signalling states (typically 64), and multiple carrier frequencies (the technique is also known as Multi-Carrier Modulation). A wide bandwidth of up to 10 MHz is required, depending on the signalling rate.

The designers claim a high immunity to noise at all signalling rates, compared to other techniques such as DS spread spectrum and FSK [68].

The success of such systems as those described above remains to be seen, especially in view of the strong objections voiced from organisations associated with users of the radio spectrum. Their potential usefulness within the realm of industrial control would be down to the fact that they offer much greater communications speeds, and so could conceivably replace some of the higher level industrial networks, such as MAP and TOP. At the level of industrial control considered in this Thesis, and for the Power Bus concept, they would seem to offer few advantages.

Moving away from HF PLC, a further noteworthy development is the concept of a local network having extended connectivity with the Internet, specifically with the World Wide Web (WWW).

9.5 The 'Web Connected Appliance'

The term 'Web Connected Appliance' is often associated with quite frivolous ideas, for example, linking your refrigerator to the Internet in order to remotely check its contents! However, there is a more serious side to the concept, such as permitting the remote monitoring of a building for security or safety purposes.

Consider the following scenario (quite common these days in an IT context):

A local area network of PCs is provided with a 'gateway' to the Internet. This permits the PCs on the local network to access the wider Internet. Conversely (in principle), users on the Internet would also be able to access the local network. In practice, such uncontrolled two way accessibility is a very bad idea. The 'gateway' that handles traffic flow between the Internet and the local network must provide essential security and other functions to prevent (possibly malicious) users on the Internet from accessing the machines on the local network. Equally, local users can be prevented from making unauthorised use of the Internet. A gateway performing this function is refereed to as a 'Firewall'.

If we now extend this idea to local control networks located within a building, factory or home, it is now (theoretically) possible for any equipment on the control network to be accessed from anywhere on the Internet. This means that users would have the capability to control or monitor the system remotely (in fact, from anywhere in the world!). There are even greater implications for security with this approach. The firewall must prevent any accidental or malicious attempts to access the local control system, as these might have grave safety implications if the operation of the process or plant could be compromised.

The Internet utilises a family of protocols that tend to be referred to by the generic abbreviation TCP/IP, referring to the two most important, 'Transmission Control Protocol' (TCP), and Internet Protocol (IP) [69]. However, there are many others that work alongside these, intended for carrying out different tasks. For example, transferring files over the Internet uses a protocol called 'File Transfer Protocol' (FTP), E-mail uses a protocol called 'Simple Message Transfer Protocol' (SMTP), and Web pages rely on a protocol called 'HyperText Transfer Protocol (HTTP).

In our previous example, the local network would need to implement the appropriate TCP/IP family protocols to allow the nodes on the local network to provide the required services over the Internet. This is not such a daunting task, given the power of modern microcontrollers, and indeed many example systems have been designed.

These systems often incorporate an Ethernet adapter, and connect to the Internet over an existing local LAN, via a gateway. Alternatively they may include a telephone modem, and connect directly to an Internet Service Provider (ISP) over a standard telephone line. The latter arrangement would be advantageous for a standalone controller requiring occasional Internet connectivity for purposes such as uploading or downloading data.

Even using a modest microcontroller, such systems are capable of generating a Web page that can contain dynamic information, related to the control task, and that can be accessed from anywhere on the Internet [70].

An alternative to this arrangement is to leave the existing local control network unchanged, and to have the interface gateway handle the conversion between the local protocol and TCP/IP family protocols. Such a system could create a 'virtual' network, from the point of view of users accessing it via the Internet. A system using these principles has been proposed for use with the CE-Bus home automation network [71, 72].

The ability to monitor a process over a LAN using a PC located elsewhere in the building or plant is potentially useful, but most control networks, whatever technology they are based on, can do this. The ability to do the same from anywhere else in the world might be considered less important, although the standardisation provided by the use of the TCP/IP protocols would at least give a level of standardisation.

That brings us to the end of the main body of this Thesis. The rest of the document consists of the Appendices, the Table of Figures, and the Bibliography. The Author sincerely hopes that you have found reading this Thesis to be worthwhile.

Appendix 1 : Detailed FTB Experimental Results

The following data shows the bit error rates measured when fast transient burst pulse trains were applied to the test set-up at a range of amplitudes, polarities, and modem signalling rates. The tests were repeated at various modem transmit signal amplitudes. These results are summarised and discussed in Chapter 8 of this Thesis.

Detailed ST7537 FTB Results for 10 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains with a modem transmit signal amplitude of 10 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**0.2228571**	**0.2611111**	**0.2930556**	**0.2726644**
-500 V	**0.1914286**	**0.1944444**	**0.2020833**	**0.2384083**
+1 kV	**1.4257143**	**1.3750000**	**1.5013889**	**1.4062284**
-1 kV	**1.1371429**	**1.1583333**	**1.2326389**	**1.2591696**
+2 kV	**2.3028571**	**2.3652778**	**2.4534722**	**2.3840830**
-2 kV	**2.4371429**	**2.3250000**	**2.3145833**	**2.3480969**

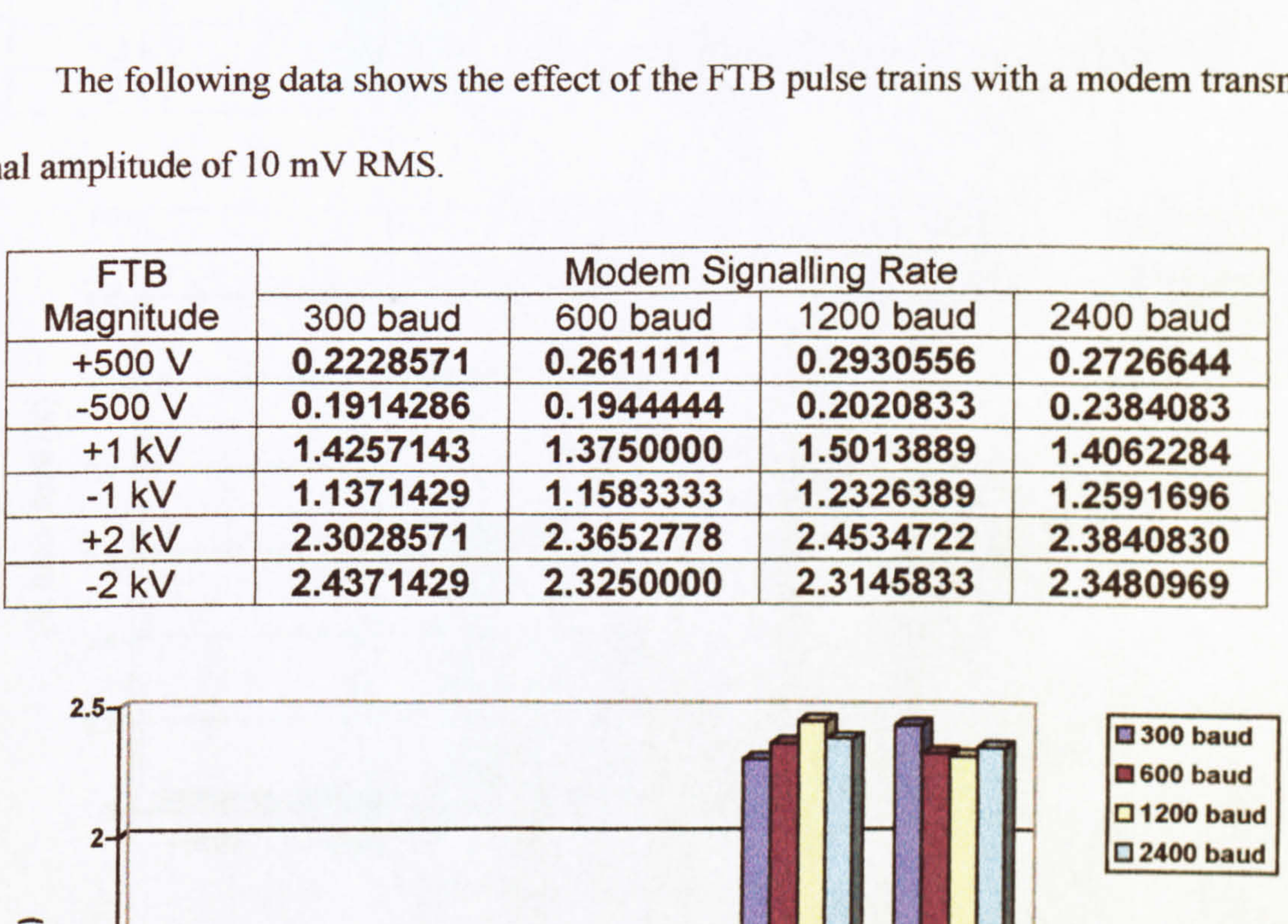


Figure 99: Detailed ST7537 FTB Results for 10 mV RMS Signal Level

Detailed ST7537 FTB Results for 20 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains with a modem transmit signal amplitude of 20 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**0.0314286**	**0.0277778**	**0.0243056**	**0.0283737**
-500 V	**0.0400000**	**0.0166667**	**0.0194444**	**0.0197232**
+1 kV	**0.6657143**	**0.6500000**	**0.6541667**	**0.6854671**
-1 kV	**0.4057143**	**0.4250000**	**0.4861111**	**0.5401384**
+2 kV	**1.0228571**	**1.1166667**	**1.2625000**	**1.2806228**
-2 kV	**0.7400000**	**0.7875000**	**0.8479167**	**0.8010381**

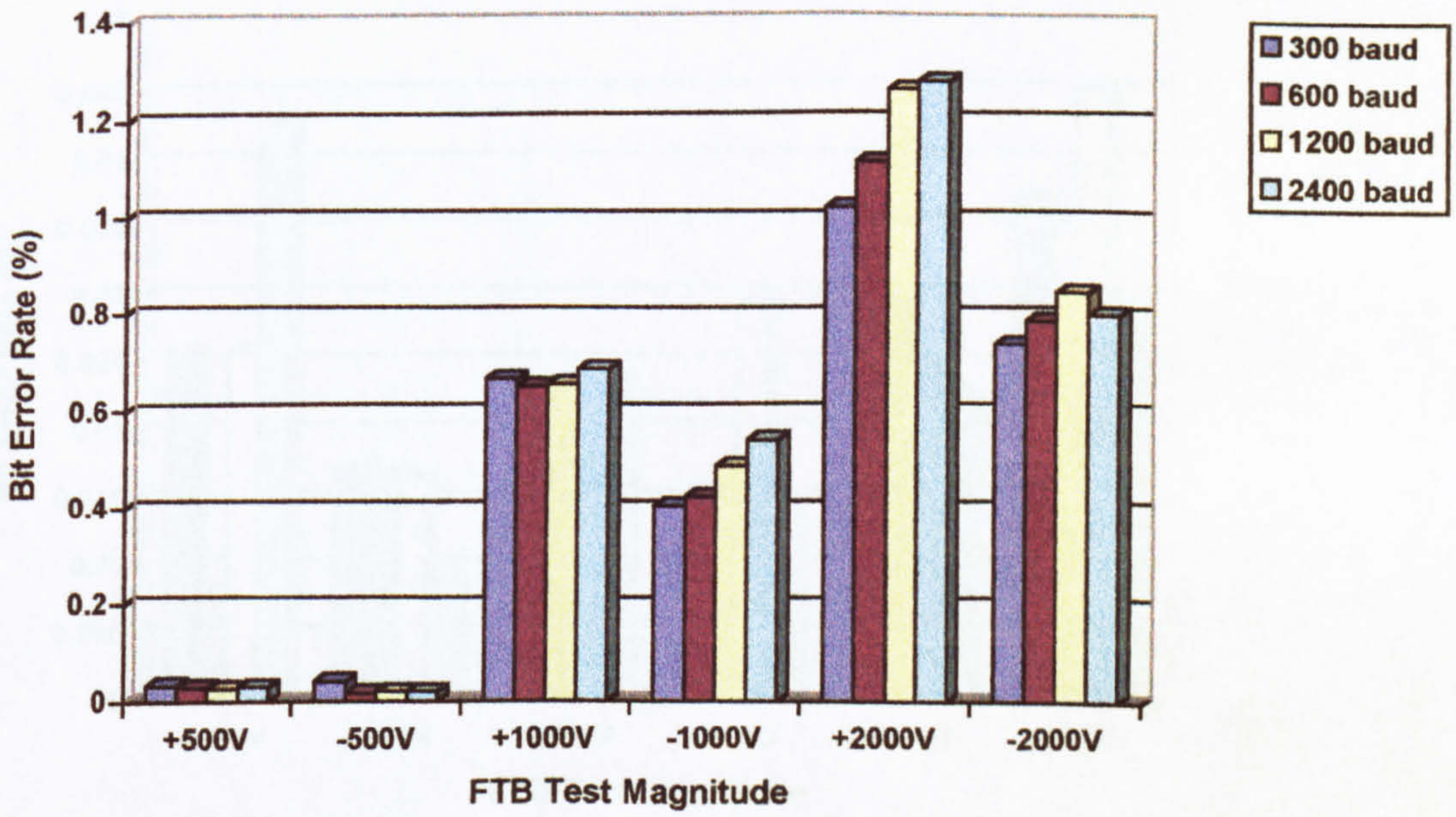


Figure 100: Detailed ST7537 FTB Results for 20 mV RMS Signal Level

Detailed ST7537 FTB Results for 40 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains with a modem transmit signal amplitude of 40 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**0.0257143**	**0.0083333**	**0.0256944**	**0.0425606**
-500 V	**0.0171429**	**0.0166667**	**0.0166667**	**0.0089965**
+1 kV	**0.0228571**	**0.0222222**	**0.0173611**	**0.0238754**
-1 kV	**0.0114286**	**0.0152778**	**0.0291667**	**0.0145329**
+2 kV	**0.0314286**	**0.0291667**	**0.0250000**	**0.0228374**
-2 kV	**0.0371429**	**0.0138889**	**0.0451389**	**0.0290657**

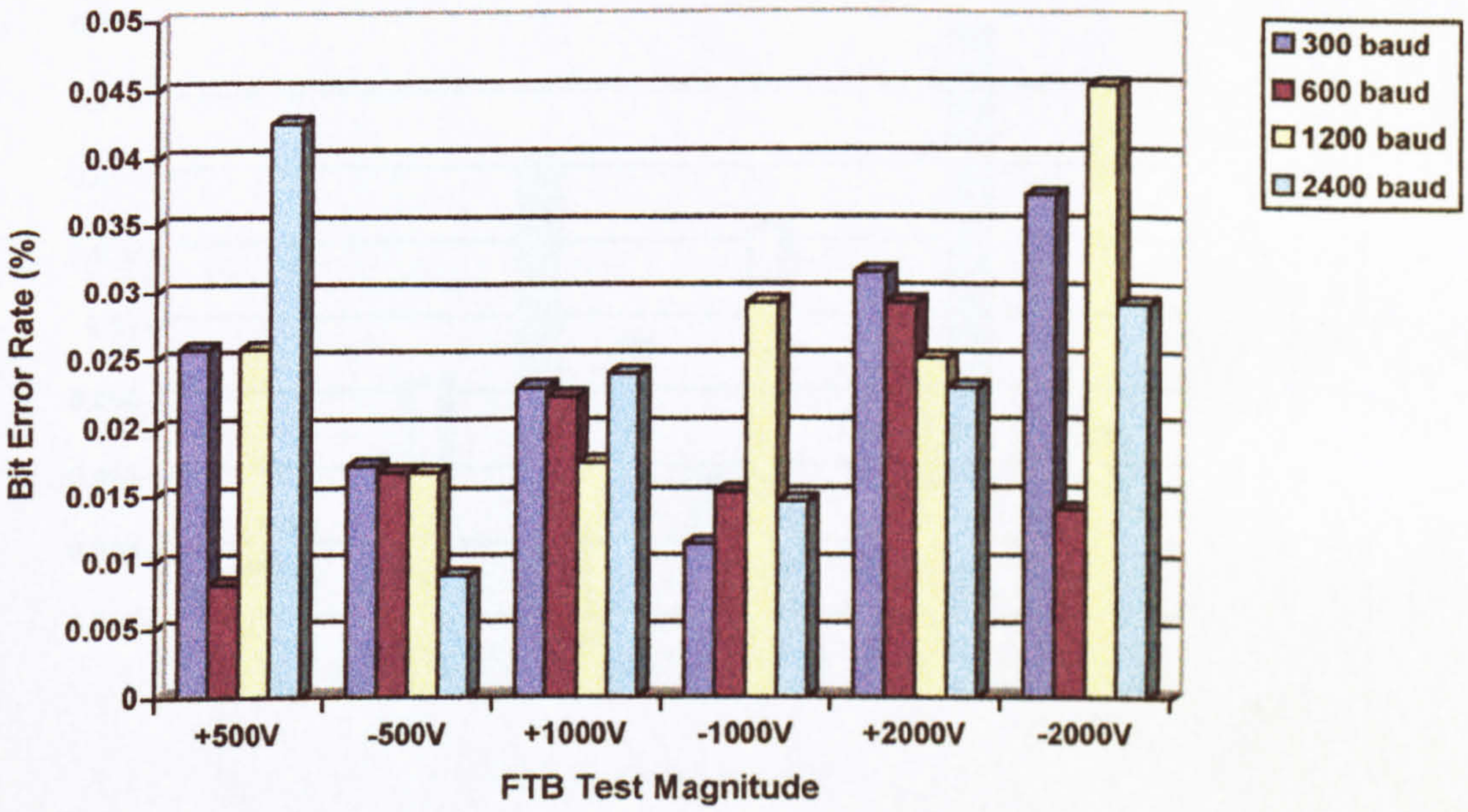


Figure 101: Detailed ST7537 FTB Results for 40 mV RMS Signal Level

Detailed ST7537 FTB Results for 80 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains with a modem transmit signal amplitude of 80 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**0.0028571**	**0.0013889**	**0.0034722**	**0.0044983**
-500 V	**0.0028571**	**0.0027778**	**0.0083333**	**0.0038062**
+1 kV	**0.0142857**	**0.0041667**	**0.0013889**	**0.0093426**
-1 kV	**0.0057143**	**0.0055556**	**0.0125000**	**0.0017301**
+2 kV	**0.0114286**	**0.0083333**	**0.0055556**	**0.0176471**
-2 kV	**0.0114286**	**0.0013889**	**0.0069444**	**0.0048443**

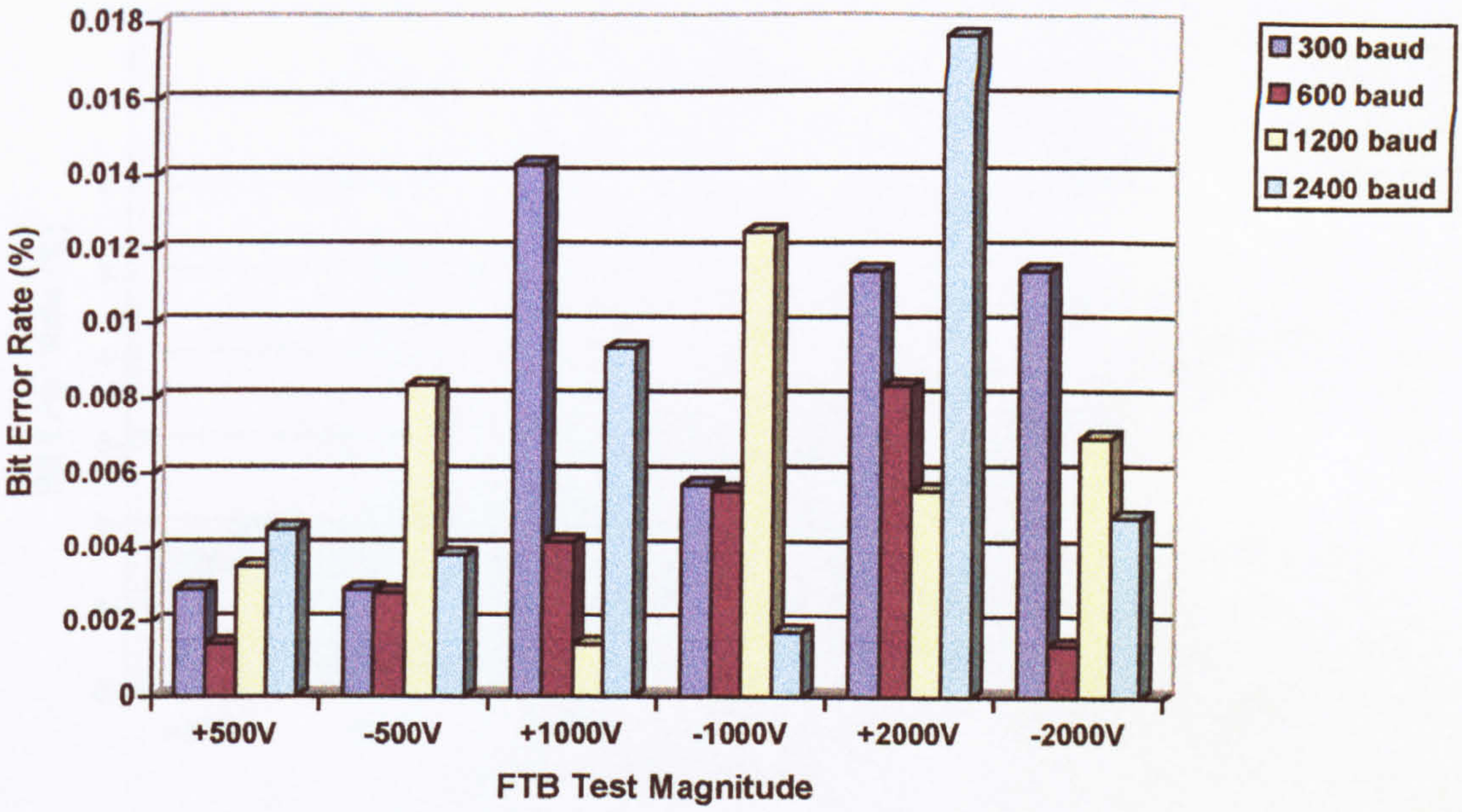


Figure 102: Detailed ST7537 FTB Results for 80 mV RMS Signal Level

Detailed TDA5051 FTB Results for 10 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains with a modem transmit signal amplitude of 10 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**1.6371429**	**1.6361111**	**1.5020979**	**2.0259516**
-500 V	**1.7200000**	**1.7972222**	**1.5958042**	**2.1761246**
+1 kV	**2.3114286**	**2.3694444**	**2.3349650**	**2.8370242**
-1 kV	**1.9571429**	**2.0000000**	**1.9440559**	**2.6020761**
+2 kV	**3.2914286**	**2.4375000**	**2.3013986**	**4.3525952**
-2 kV	**3.0114286**	**2.6861111**	**2.7489510**	**7.0221453**

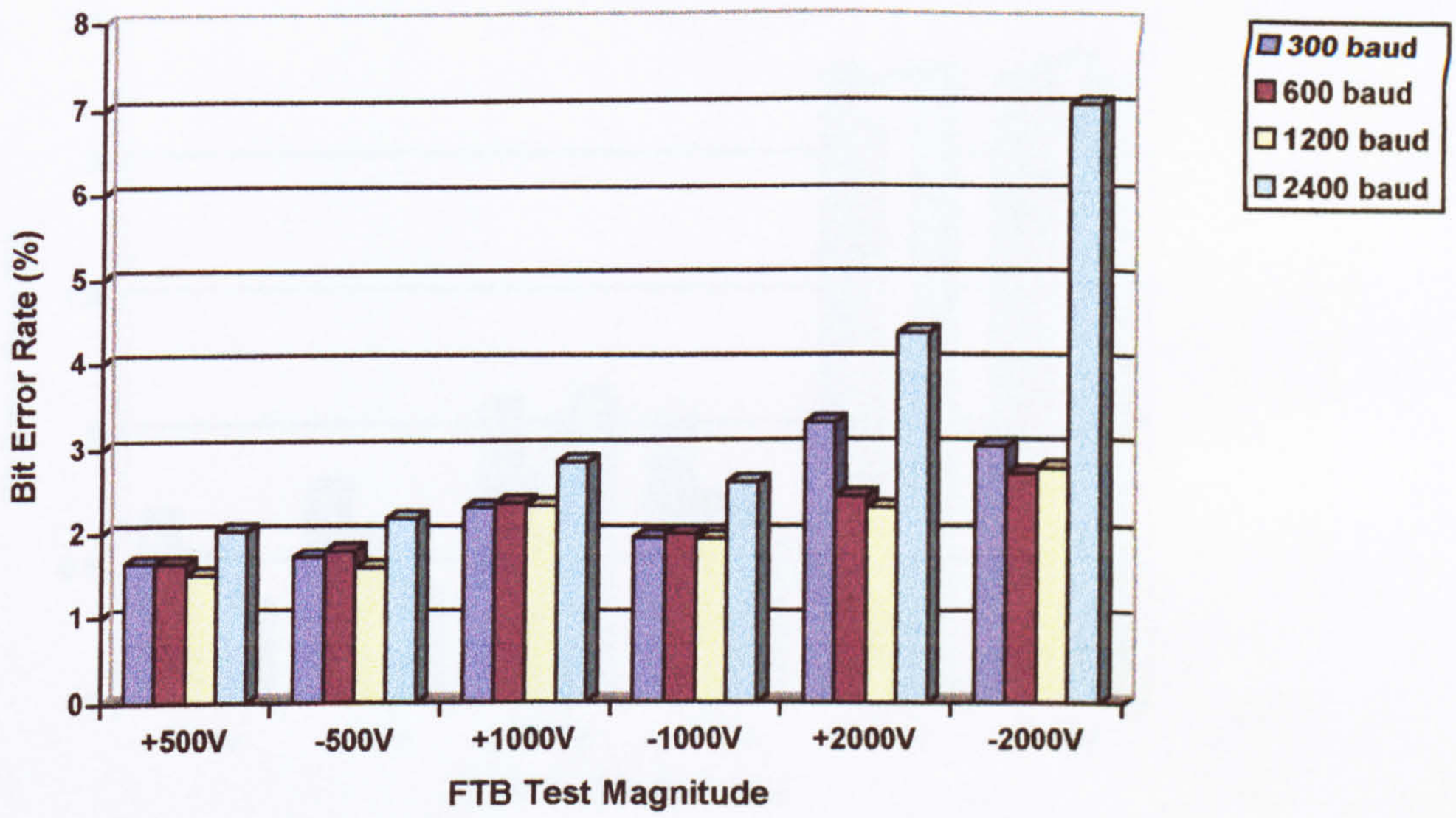


Figure 103: Detailed TDA5051 FTB Results for 10 mV RMS Signal Level

Detailed TDA5051 FTB Results for 20 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains with a modem transmit signal amplitude of 20 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**0.6914286**	**0.5361111**	**0.4388889**	**0.3522491**
-500 V	**0.8028571**	**0.6277778**	**0.4222222**	**0.3975779**
+1 kV	**1.0885714**	**0.8236111**	**0.9576389**	**1.1301038**
-1 kV	**1.0085714**	**0.7500000**	**0.6979167**	**0.6570934**
+2 kV	**2.3085714**	**2.2736111**	**2.2909722**	**2.3093426**
-2 kV	**2.2828571**	**2.3263889**	**2.3520833**	**2.2737024**

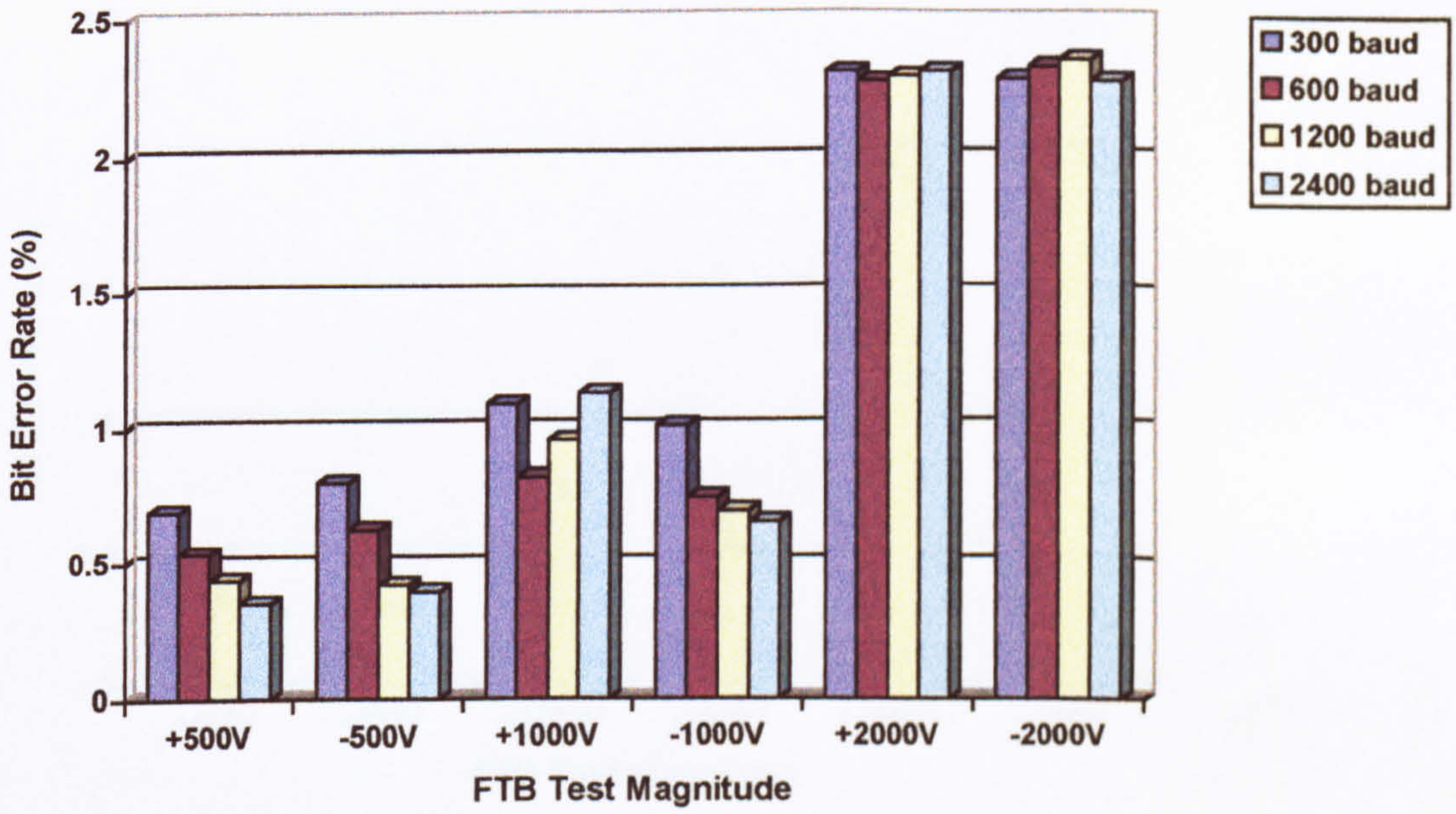


Figure 104: Detailed TDA5051 FTB Results for 20 mV RMS Signal Level

Detailed TDA5051 FTB Results for 40 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains for a modem transmit signal amplitude of 40 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**0.4657143**	**0.3791667**	**0.2965278**	**0.2494810**
-500 V	**0.2571429**	**0.4555556**	**0.2826389**	**0.2128028**
+1 kV	**0.5371429**	**0.7597222**	**0.7013889**	**0.5972318**
-1 kV	**0.7800000**	**0.6291667**	**0.5076389**	**0.4166090**
+2 kV	**1.9342857**	**1.9583333**	**2.0180556**	**1.8830450**
-2 kV	**1.9657143**	**2.0069444**	**2.0145833**	**1.9190311**

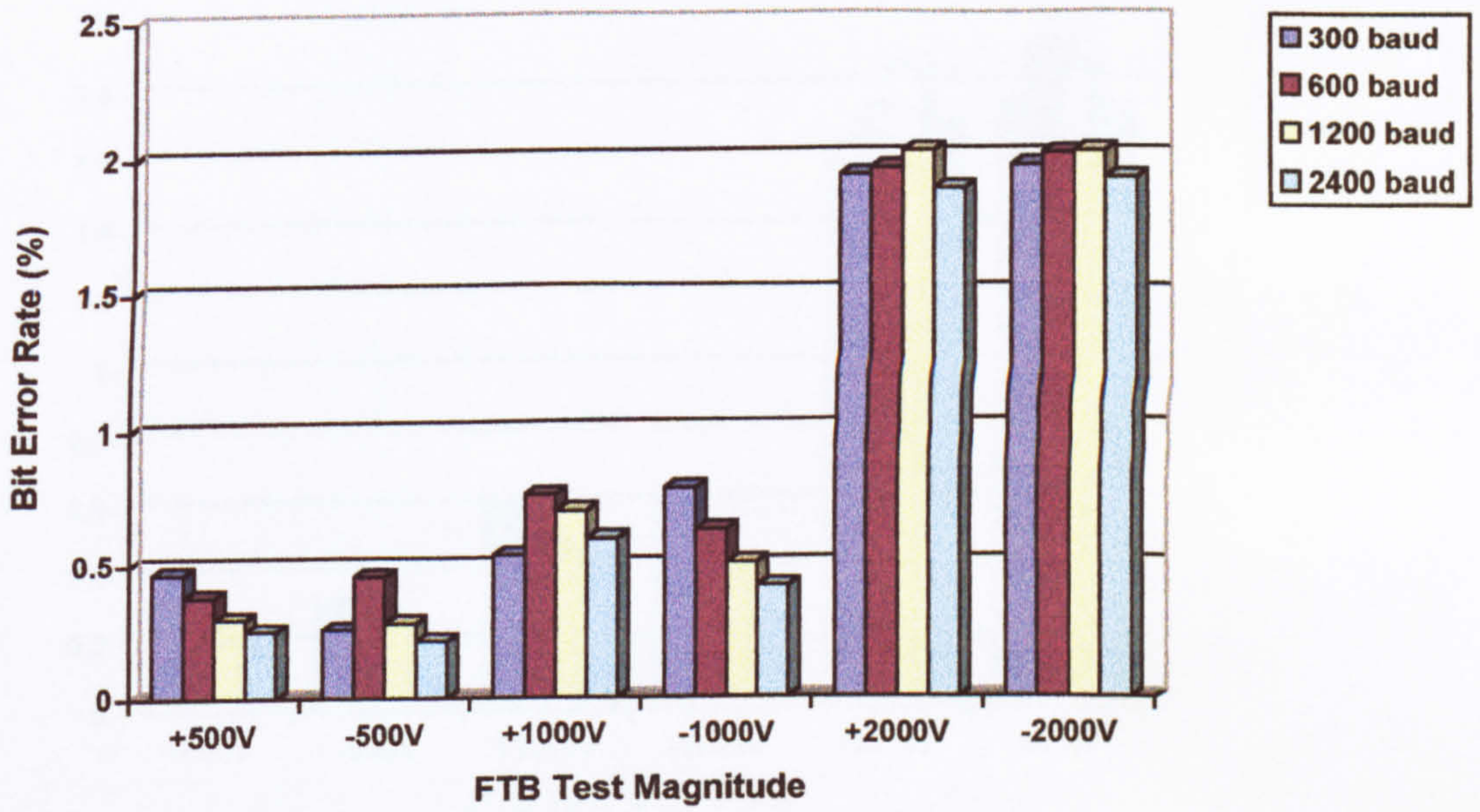


Figure 105: Detailed TDA5051 FTB Results for 40 mV RMS Signal Level

Detailed TDA5051 FTB Results for 80 mV RMS Signal Level

The following data shows the effect of the FTB pulse trains for a modem transmit signal amplitude of 80 mV RMS.

FTB Magnitude	Modem Signalling Rate			
	300 baud	600 baud	1200 baud	2400 baud
+500 V	**0.3228571**	**0.2263889**	**0.1930556**	**0.1750865**
-500 V	**0.3171429**	**0.2569444**	**0.2520833**	**0.2183391**
+1 kV	**0.6114286**	**0.5083333**	**0.4680556**	**0.4249135**
-1 kV	**0.6028571**	**0.4083333**	**0.3888889**	**0.3716263**
+2 kV	**1.6600000**	**1.7375000**	**1.8604167**	**1.6868512**
-2 kV	**1.7685714**	**1.9277778**	**1.8437500**	**1.7307958**

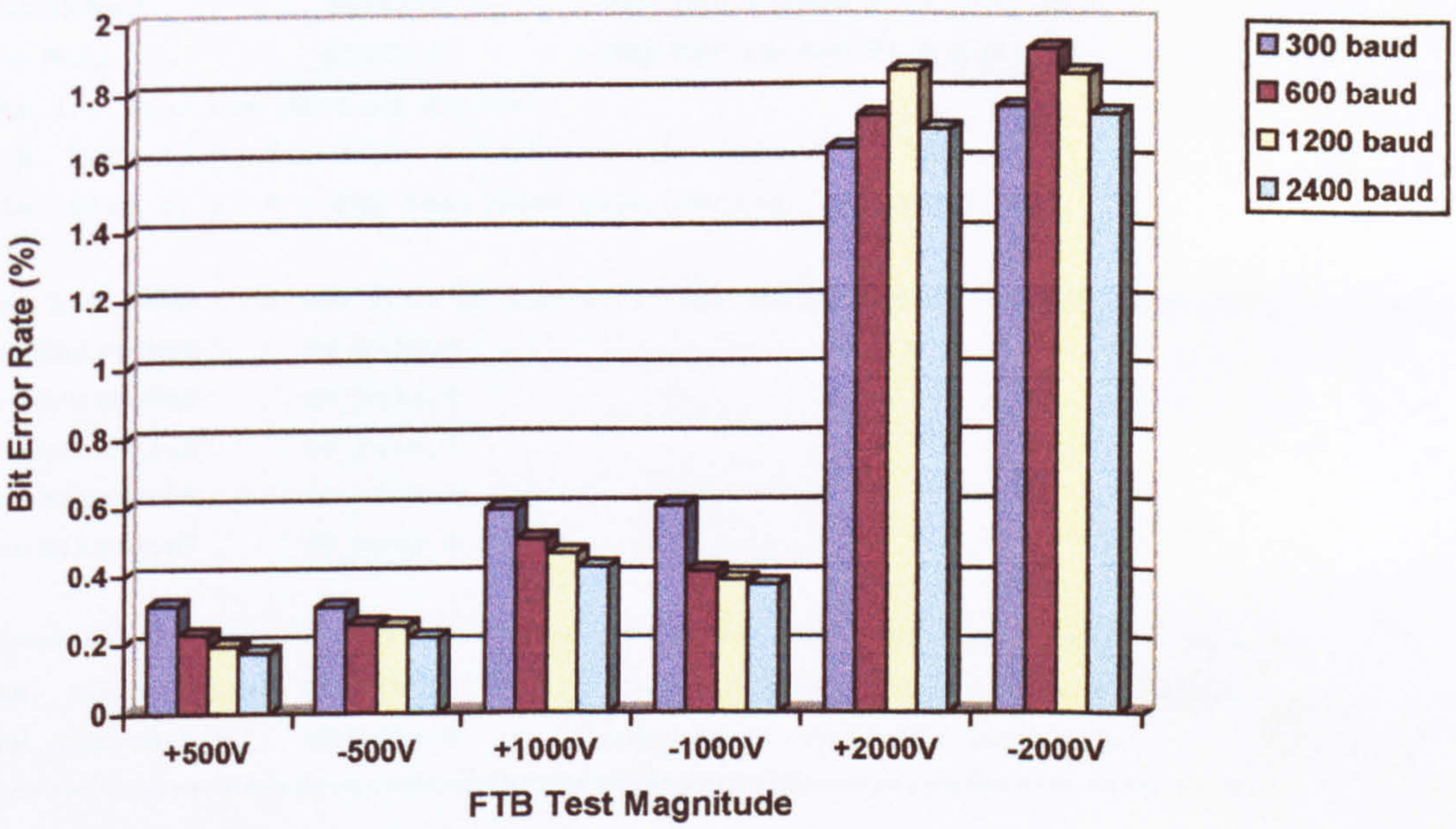


Figure 106: Detailed TDA5051 FTB Results for 80 mV RMS Signal Level

Appendix 2: BER Tester Assembly Code Firmware

```
BER_test.ASM
        TITLE "PLC Modem Bit-Error-Rate Test Set"
;*****************************************************************************
        Processor       16C84
        Radix           DEC
        EXPAND
        include         "16Cxx.h"
;*****************************************************************************

rtccDivider     set     0x9f    ;divide value for 4800 baud

        NOLIST
;*****************************************************************************
; Pin Assignements
;*****************************************************************************
#define TX              _portb,7        ; RS232 transmit pin
#define BERout          _portb,2        ; BER bit stream Tx output pin
#define BERin           _portb,3        ; BER bit stream Rx input pin
; other i/o pins are used as follows:
; PortB, bits 4, 5, 6 - delay setting switch, bits 0, 1, 2
; PortA, bits 0, 1, 2 - BER test baud rate setting, bits 0, 1, 2

; these bit locations are used to store the BER output state used by the delay counters
#define bitstore1       GP_bits,0
#define bitstore2       GP_bits,1
#define bitstore3       GP_bits,2
#define bitstore4       GP_bits,3
#define bitstore5       GP_bits,4

;*****************************************************************************
#define _txmtProgress   GP_bits,6       ; flags if RS232 transmission is under way
#define _StartBit       GP_bits,7       ; defines if start bit sent yet
;*****************************************************************************

        LIST
; file register locations used within the 16F84
        CBLOCK 0x0C     ; start address of general purpose register block
TxReg                   ; RS232 transmit data holding/shift register
GP_bits                 ; array of general purpose flag registers (defined later)
BitCount                ; bit counter for RS232 transmission routine
SaveWReg                ; temporary holding register for WREG during INTERRUPT
SaveStatus              ; temporary holding register for STATUS register during INTERRUPT
temp1, temp2            ; temporary locations
RandHi, RandLo          ; random number seeds
_baud                   ; baud rate divider for BER bitstream
_baud_rat               ; current ber baud rate divider value
                        ; 1=4800, 2=2400, 3=1200, 4=600, 5=300
delayval                ; current delay value after outputting data, before sampling input
                        ; 1=208µs, 2=417µs, 3=635µs, 4=833µs, 5=1042µs (max)
BERcnt1, BERcnth        ; counter for 1000 bits test sample
```

```
;*****************************************************************
;** the next locations hold the various test bit and error counts **
;*****************************************************************
loERRl                  ; LSB of the count of low bit errors (Tx=0, Rx=1)
loERRh                  ; MSB of the count of low bit errors (Tx=0, Rx=1)
hiERRl                  ; LSB of the count of high bit errors (Tx=1, Rx=0)
hiERRh                  ; MSB of the count of high bit errors (Tx=1, Rx=0)
loBITl                  ; LSB of the count of low bits
loBITh                  ; MSB of the count of low bits
hiBITl                  ; LSB of the count of high bits
hiBITh                  ; MSB of the count of high bits

;*****************************************************************************
;** these locations hold a mirror of the above data, used during the transmission of **
;** the data to the PC host, whilst a new set of results are concurrently obtained   **
;*****************************************************************************
loERRlx, loERRhx, hiERRlx, hiERRhx, loBITlx, loBIThx, hiBITlx, hiBIThx

;*****************************************************************
;** Tx-Rx delay counters, dynamically assigned by the software **
;*****************************************************************
delay1, delay2, delay3, delay4, delay5

        endc            ; end of code block

;************************************************
;** Firstly the reset and interrupt vectors **
;************************************************
        ORG     _ResetVector
        goto    Start
;
        ORG     _IntVector
        goto    Interrupt

;*****************************************
;** Hardware & software initialisation **
;*****************************************
Start
        bsf     _rp0
        bcf     _rp1            ; first select register page 1

        ; ready to set the characteristics of I/O port A
        movlw   b'11111111'
        movwf   _trisa          ; set port A as all inputs
                                ; (bits 0-2 are used to select the BER test baud rate)
                                ; (bits 0-2 are used to select the BER test baud rate)

; ready to set the characteristics of I/O port B
MOVLW   B'01111011'
MOVWF   _trisb          ; set port B AS all inputs except bit 2 (TX) & 7 (BERout)
                        ; (bits 4-6 are used to select the BER Tx-Rx delay)
```

```
; ready to set the OPTION register of the PIC
MOVLW   B'10010000'     ; bit 7=1 - port B pullups are disabled
                        ; bit 6=0 - interrupt on falling of RB0 pin (not used)
                        ; bit 5=0 - RTCC signal source is internal
                        ; bit 4=1 - RTCC increments on high-low transition of RA4
                        ; (irrelevant since source is internal)
                        ; bit 3=0 - prescaler is assigned to RTCC
                        ; bit 2=0 \
                        ; bit 1=0 - prescaler is set to 1:2 (RTCC)
                        ; bit 0=0 /
MOVWF   _option         ;

BCF     _rp0            ; finished with page 1, so restore page 0

bsf     TX              ; initially set the TX output pin high
bsf     BERout          ; & the same for the BER test output

movlw   0xFF            ; initialise the delay counters to their idle values
movwf   delay1
movwf   delay2
movwf   delay3
movwf   delay4
movwf   delay5

movlw   rtccDivider
movwf   _rtcc           ; load the RTCC divider value

movlw   0x30
movwf   RandHi
movlw   0x45
movwf   RandLo          ; initialise the random number generator seeds

call    ClrCnt          ; set up the counters & delay values
call    setBAUD         ; and the BER test baud rate

bsf     _rtie
bsf     _gie            ; finally enable the interrupts ready to start

;*************************
;** MAIN PROGRAM LOOP **
;*************************
; wait for the end of a BER test cycle
Loop
Call    Random          ; keep stirring the random no. generator whilst waiting
movf    BERcnth,w       ; check if the MSB of the 1000-bit counter is zero
btfss   _z
goto    Loop            ; carry on looping if not
movf    BERcntl,w       ; else test the LSB
btfss   _z
goto    Loop            ; carry on looping if not
```

```
;*****************************************************************
; ** count has reached zero, so capture data and start another run **
;*****************************************************************
; transfer the various data bytes to their mirrors
        movf    loERRl,w
        movwf   loERRlx
        movf    loERRh,w
        movwf   loERRhx
        movf    hiERRl,w
        movwf   hiERRlx
        movf    hiERRh,w
        movwf   hiERRhx
        movf    loBITl,w
        movwf   loBITlx
        movf    loBITh,w
        movwf   loBIThx
        movf    hiBITl,w
        movwf   hiBITlx
        movf    hiBITh,w
        movwf   hiBIThx

;************************************************
;** now reset the counters for the next run **
;************************************************
; (also update delay value and baud rate if necessary)
        call    ClrCnt

;************************************************
;** now send the saved data to the host PC **
;************************************************
        movf    loBIThx,w       ; MSB total number of low bits in run
        call    sendch          ; send it
        movf    loBITlx,w       ; LSB total number of low bits in run
        call    sendch          ; and again

        movf    hiBIThx,w       ; MSB total number of high bits in run
        call    sendch          ; send it
        movf    hiBITlx,w       ; LSB total number of high bits in run
        call    sendch          ; and again

        movf    loERRhx,w       ; MSB total number of low bit errors in run
        call    sendch          ; send it
        movf    loERRlx,w       ; LSB total number of low bit errors in run
        call    sendch          ; and again

        movf    hiERRhx,w       ; MSB total number of high bit errors in run
        call    sendch          ; send it
        movf    hiERRlx,w       ; LSB total number of high bit errors in run
        call    sendch          ; and again
```

```
; send a CR/LF to delimit each line of data
        movlw   13
        call    sendch          ; send a CR
        movlw   10
        call    sendch          ; and an LF
        ; (NOTE: CRLF should never occur in the normal data stream)

        goto    Loop            ; carry on until the end of the next run

;************************************************
;** send a byte value to the serial port **
;************************************************
sendch
        movwf   TxReg
        call    PutChar         ; send character
sendch1                         ; now wait for the transmission to finish
        btfss   _txmtProgress
        return                  ; return if finished
        call    Random          ; keep stirring that seed!
        goto    sendch1         ; and continue looping

;*************************************************************
;** Reset the various count parameters prior to a new run **
;*************************************************************
ClrCnt
        movlw   03
        movwf   BERcnth
        movlw   232
        movwf   BERcntl         ; for a total bit count of 1000
        ; reset the various counters
        clrf    loERRl
        clrf    loERRh
        clrf    hiERRl
        clrf    hiERRh
        clrf    loBITl
        clrf    loBITh
        clrf    hiBITl
        clrf    hiBITh

;*************************************************************
;** get the baud rate value from the switch (valid input range 0-4) **
;** & convert it to a binary division ratio                          **
;*************************************************************
        incf    _porta,w        ; get switch value +1
        andlw   b'00000111'     ; mask the unused bits
        movwf   temp1           ; & save the value
        ; now test if >5
        sublw   5               ; 5 is maximum value (300 baud)
        btfsc   _carry          ;
        goto    clrcnt0         ; carry on if the value is <=5
        movlw   5               ; else set to the default maximum value
        movwf   temp1           ; re-save the new value
```

```
; convert the value to a binary divisor 1=1, 2=2, 3=4, 4=8, 5=16
clrcnt0
        clrf    temp2
        bsf     _carry          ; carry will shift into bit 0
clrcnt1
        rlf     temp2,f         ; shift data along
        decfsz  temp1,f
        goto    clrcnt1         ; loop 1-5 times according to original value
; temp2 now holds the binary divider value
        movf    temp2,w
        movwf   _baud_rat       ; save the value

;*****************************************************************************
;** get the Tx-Rx delay value from the switch (valid input range 0-4) **
;*****************************************************************************
        movf    _portb,w        ; (bits 4, 5, 6 are the switch inputs)
        andlw   b'01110000'     ; mask the unused bits
        movwf   temp1           ; place the data in temporary store
        rrf     temp1,f         ; then
        rrf     temp1,f         ; shift
        rrf     temp1,f         ; it along
        rrf     temp1,f         ; into bits 0-2
        incf    temp1,w         ; increment it & place it in w
        movwf   delayval        ; then save it
        ;now test if >5
        sublw   5               ; 5 is maximum delay value (c.1ms)
        btfsc   _carry          ;
        return                  ; exit if ok (<=5)
        movlw   5               ; else reset to the default value
        movwf   delayval        ; and save
        return                  ; before returning

;*****************************************************************************
;** routine to set the BER (i.e. pseudorandom bit stream) baud rate **
;*****************************************************************************
setBAUD
        movf    _baud_rat,w     ; get current value
        movwf   _baud           ; put in the prescaler
        return

;*****************************************************************
;** the following routines are utilised by the counter    **
;** routines to update the various bit and error counters **
;*****************************************************************
;routine to increment the high bit counter
incHBIT
        movlw   1
        addwf   hiBIT1,f        ; increment no. of high bits in run
        btfsc   _carry
        incf    hiBITh,f
        return
```

```
;routine to increment the high bit error counter
incHERR
        movlw   1
        addwf   hiERRl,f        ; bit was low, so increment error count
        btfsc   _carry
        incf    hiERRh,f        ; process carry bit if applicable
        return

;routine to increment the low bit counter
incLBIT
        movlw   1
        addwf   loBITl,f        ; increment no. of low bits in run
        btfsc   _carry
        incf    loBITh,f
        return

;routine to increment the low bit error counter
incLERR
        movlw   1
        addwf   loERRl,f        ; bit was high, so increment error count
        btfsc   _carry
        incf    loERRh,f
        return

;*************************************************************
; INTERRUPT SERVICE ROUTINE - called solely by the RTCC **
;*************************************************************
Interrupt
        btfss   _rtif
        retfie                  ; another spurious interrupt, simply return & enable GIE

; Save Status On INT : WREG & STATUS Regs
        movwf   SaveWReg
        swapf   _status,w               ; affects no STATUS bits : Only way OUT to save STATUS
Reg ?????
        movwf   SaveStatus

        movlw   rtccDivider
        movwf   _rtcc                   ; RESET RTCC

;*****************************************************************
;** test if output transmission under way (always at 4800 baud!) **
;*****************************************************************
test tx
    btfsc   _txmtProgress
    call    _TxmtNextBit            ; Txmt Next Bit
```

```
;*****************************************************************************
;** next process the delay counters (those having a value of 255 are on **
;** standby, and ignored), others are decremented and processed if zero **
;*****************************************************************************
test_d1 ; test delay counter #1
        incfsz  delay1,w        ; skip if not in use
        call    dec_d1          ; else decrement counter

test_d2 ; test delay counter #2
        incfsz  delay2,w        ; skip if not in use
        call    dec_d2          ; else decrement counter

test_d3 ; test delay counter #3
        incfsz  delay3,w        ; skip if not in use
        call    dec_d3          ; else decrement counter

test_d4 ; test delay counter #4
        incfsz  delay4,w        ; skip if not in use
        call    dec_d4          ; else decrement counter

test_d5 ; test delay counter #5
        incfsz  delay5,w        ; skip if not in use
        call    dec_d5          ; else decrement counter
        goto    dec_dend        ; none are in use, so carry on

;************************************************
;*** decrement those delay counters in use **
;************************************************
dec_d1  ; decrement delay counter #1
        decfsz  delay1,f
        return                  ; not yet zero, so carry on
; else counter 1 is zero, so process the results
        decf    delay1,f        ; now set to 255, so counter available for re-use
        btfss   bitstore1       ; test the stored state for this counter
        goto    outLO1          ; if stored state is low
;else output state was high
        call    incHBIT         ; increment high bit count
        btfsc   BERin           ; now test input pin,
        return                  ; carry on if input high i.e. ok
        call    incHERR         ; else increment high bit error count
        return
;else output state was low
outLO1  call    incLBIT         ; increment low bit count
        btfss   BERin           ; test input pin
        return                  ; carry on if input is low
        call    incLERR         ; else increment low bit error count
        return
dec_d2  ; decrement delay counter #2
        decfsz  delay2,f
        return                  ; not yet zero, so carry on
```

```
; else counter 2 is zero, so process the results
        decf    delay2,f        ; now set to 255, so counter available for re-use
        btfss   bitstore2       ;
        goto    outLO2
;else output state was high
        call    incHBIT         ; increment high bit count
        btfsc   BERin           ; now test input pin,
        return                  ; carry on if input high i.e. ok
        call    incHERR         ; else increment high bit error count
        return
;else output state was low
outLO2  call    incLBIT         ; increment low bit count
        btfss   BERin           ; test input pin
        return                  ; carry on if input is low
        call    incLERR         ; else increment low bit error count
        return

dec_d3  ; decrement delay counter #3
        decfsz  delay3,f
        return  ; not yet zero, so carry on
; else counter 3 is zero, so process the results
        decf    delay3,f        ; now set to 255, so counter available for re-use
        btfss   bitstore3       ;
        goto    outLO3
;else output state was high
        call    incHBIT         ;increment high bit count
        btfsc   BERin           ;now test input pin,
        return          ;carry on if input high i.e. ok
        call    incHERR         ;else increment high bit error count
        return
;else output state was low
outLO3  call    incLBIT         ;increment low bit count
        btfss   BERin           ;test input pin
        return          ;carry on if input is low
        call    incLERR         ;else increment low bit error count
        return

dec_d4  ; decrement delay counter #4
        decfsz  delay4,f
        return  ; not yet zero, so carry on
; else counter 4 is zero, so process the results
        decf    delay4,f        ; now set to 255, so counter available for re-use
        btfss   bitstore4       ;
        goto    outLO4
;else output state was high
        call    incHBIT         ;increment high bit count
        btfsc   BERin           ;now test input pin,
        return  ;carry on if input high i.e. ok
        call    incHERR         ;else increment high bit error count
        return
```

```
;else output state was low
outLO4  call    incLBIT         ;increment low bit count
        btfss   BERin           ;test input pin
        return  ;carry on if input is low
        call    incLERR         ;else increment low bit error count
        return

dec_d5  ; decrement delay counter #5
        decfsz  delay5,f
        return  ; not yet zero, so carry on
; else counter 5 is zero, so process the results
        decf    delay5,f        ; now set to 255, so counter available for re-use
        btfss   bitstore5       ;
        goto    outLO5
 ;else output state was high
        call    incHBIT         ;increment high bit count
        btfsc   BERin           ;now test input pin,
        return  ;carry on if input high i.e. ok
        call    incHERR         ;else increment high bit error count
        return
 ;else output state was low
outLO5  call    incLBIT         ;increment low bit count
        btfss   BERin           ;test input pin
        return  ;carry on if input is low
        call    incLERR         ;else increment low bit error count
        return

;(unified exit point for these routines)
dec_dend

;*****************************************************************************
;** Test the BER baud rate divider to see if it is time to alter the BER output bit **
;*****************************************************************************
_BERtest
        decf    _baud,f
        btfss   _z              ; if result zero then send next bit
        goto    setdelend       ; carry on if not

;***************************************
;** decrement the 1000 bit counter **
;***************************************
        movlw   1
        subwf   BERcntl,f
        btfss   _carry          ; test if LSB of count has passed through zero
        decf    BERcnth,f       ; if so, decrement the MSB count
```

```
;***********************************
;** set up the next output bit **
;***********************************
        call    setBAUD         ; reset the baud rate counter
        call    Random          ; get the next random number
        btfss   RandLo,1        ; bit 1 is used as the BER data, skip if set
        bcf     BERout          ; else set BER output low
        btfsc   RandLo,1        ; skip if clear
        bsf     BERout          ; else set the BER output high

;*****************************************************************
;** store the current BER output value and set up a delay counter **
;*****************************************************************
 ;first find a free counter (with a value of 255)
 setdel1
         incfsz  delay1,w       ; skip if counter not in use
         goto    setdel2        ; else try the next counter
 ; counter 1 is available, so use it!
         movf    delayval,w     ; delay count, from input switch
         movwf   delay1         ; save value
         bcf     bitstore1
         btfsc   RandLo,1
         bsf     bitstore1      ; save the BER bit state
         goto    setdelend      ; finished

setdel2
         incfsz  delay2,w       ; skip if counter not in use
         goto    setdel3        ; else try the next counter
; counter 2 is available, so use it!
         movf    delayval,w     ; delay count, from input switch
         movwf   delay2         ; save value
         bcf     bitstore2
         btfsc   RandLo,1
         bsf     bitstore2      ; save the BER bit state
         goto    setdelend      ; finished

setdel3
         incfsz  delay3,w       ; skip if counter not in use
         goto    setdel4        ; else try the next counter
; counter 3 is available, so use it!
         movf    delayval,w     ; delay count, from input switch
         movwf   delay3         ; save value
         bcf     bitstore3
         btfsc   RandLo,1
         bsf     bitstore3      ; save the BER bit state
         goto    setdelend
```

```
setdel4
        incfsz  delay4,w        ; skip if counter not in use
        goto    setdel5         ; else try the next counter
; counter 4 is available, so use it!
        movf    delayval,w      ; delay count, from input switch
        movwf   delay4          ; save value
        bcf     bitstore4
        btfsc   RandLo,1
        bsf     bitstore4       ; save the BER bit state
        goto    setdelend

setdel5
        incfsz  delay5,w        ; skip if counter not in use
        goto    setdelend       ; (should never happen in practice!!!)
; counter 5 is available, so use it!
        movf    delayval,w      ; delay count, from input switch
        movwf   delay5          ; save value
        bcf     bitstore5
        btfsc   RandLo,1
        bsf     bitstore5       ; save the BER bit state

;unified exit point for this routine
setdelend

;*************************************
;** end of the interrupt routine **
;*************************************
RestoreIntStatus:
        clrwdt
        swapf   SaveStatus,w
        movwf   _status         ; restore STATUS Reg
        swapf   SaveWReg,f      ; save WREG
        swapf   SaveWReg,w      ; restore WREG
        bcf     _rtif           ; clear the int flag
        retfie

;*************************************
;** asynchronous transmit routine **
;*************************************
; Function to transmit A Byte Of Data
; Before calling this routine, load the Byte to be transmitted into TxReg
PutChar:
        bsf     _txmtProgress   ; flag transmission in progress
        bsf     _StartBit       ; these flags are used to indicate when start
        movlw   9
        movwf   BitCount        ; total bit count-1 + two stop bits
        return
```

```
;*****************************************************************************
; Internal Subroutine entered from Interrupt Service Routine when transmission in progress
;*****************************************************************************
_TxmtNextBit
        btfss   _StartBit       ; first test if at start of transmission?
        goto    _next           ; if not, then carry on

;else at start, so send start bit
        bcf     TX              ; the start bit is low
        bcf     _StartBit       ; flag that start bit has now been sent
        return                  ; carry on

; sending body of data
_next
        movf    BitCount,f      ; test if finished data transmission?
        btfsc   _z              ; count will be 0 if so
        goto    _finished       ; yes, finished
        decf    BitCount,f      ; else just decrement the counter

; and transmit the next bit
_NextTxmtBit
        bsf     _carry          ; ready for sending stop bits
        rrf     TxReg,f         ; shift data right, into carry
        btfss   _carry          ; if the data is high, then skip
        bcf     TX              ; else set the Tx output low
        btfsc   _carry          ; if the data is low, then skip
        bsf     TX              ; else set the Tx output high
        return                  ; then carry on
_finished
        bcf     _txmtProgress   ; flag the end of the transmission
        return                  ; and carry on

;*****************************************************************************
; RANDOM - Generates a pseudorandom number. Works best if called from a loop so that the *
; value of its workspace variable (consisting of lowB and hiB) is constantly stirred.    *
;*****************************************************************************
Random  movf    RandHi,w        ; First, ensure that hiB and lowB aren't
        iorwf   RandLo,w        ; all zeros. If they are, NOT hiB to FFh.
        btfsc   _z              ; Otherwise, leave hiB and lowB as is.
        comf    RandHi,f
        movlw   #80h            ; We want to XOR hiB.7, hiB.6, hiB.4
        btfsc   RandHi,6        ; and lowB.3 together in W. Rather than
        xorwf   RandHi,f        ; try to line up these bits, we just
        btfsc   RandHi,4        ; check to see whether a bit is a 1. If it
        xorwf   RandHi,f        ; is, XOR 80h into hiB. If it isn't,
        btfsc   RandLo,3        ; do nothing. When we're done, the
        xorwf   RandHi,f        ; XOR of the 4 bits will be in hiB.7.

        rlf     RandHi,w        ; Move hiB.7 into carry.
        rlf     RandLo,f        ; Rotate c into lowB.0, lowB.7 into c.
        rlf     RandHi,f        ; Rotate c into hiB.0.
        return

        end
```

Appendix 3: Host Computer Logging Software Listing

```
PROGRAM TEST_BER ;

uses
  Dos,
  Crt,
  Async4 ;

VAR
  c                : char ;
  cnum, cnum1      : byte;
  TestPort         : INTEGER ;
  TestRate         : aBpsRate ;
  TestParity       : aParitySetting ;
  TestWordLen      : byte ;
  TestStopBits     : byte ;
  CurrRate         : aBpsRate ;
  CurrParity       : aParitySetting ;
  CurrWordLen      : byte ;
  CurrStopBits     : byte ;
  DelayCount       : INTEGER ;
  YorN             : CHAR ;
  CharMask         : byte ;
  State            : (MenuMode, TermMode, Exitting) ;
  Open             : BOOLEAN ;
tHour, tMinute, tSecond, tHundredth : word;
  sample : integer; (* counter for time stamping *)

  OP_file : text;    (* text output file *)
  OP_data : integer; (* data to be stored *)

PROCEDURE OpenPort ;

BEGIN { OpenPort }
  IF NOT Async_Open( TestPort,
                     TestRate,
                     TestParity,
                     TestWordLen,
                     TestStopBits ) THEN BEGIN
    WRITELN('**ERROR: Async_Open failed') ;
    Open := FALSE
  END
ELSE
  Open := TRUE
END { OpenPort } ;
```

```
PROCEDURE TermTest ;

  Function Get_Data : integer; (* get and return a 2-byte value *)
  var temp : integer;
  begin
       temp := 0;
       repeat until Async_Buffer_Check(c);
       temp := ord(c) * 256;
       repeat until Async_Buffer_Check(c);
       Get_Data := temp + ord(c)
  end;

BEGIN { TermTest }
sample:=10; (* initialise timestamp counter *)


IF Open THEN BEGIN
  assign(OP_file,'DATAFILE.TXT');
  Rewrite(OP_file);
  WRITELN('Data Logging begins now... (Press <F10> to terminate..)');
  State := TermMode ;
  REPEAT
    repeat (* first get CRLF delimiter *)
      repeat until Async_Buffer_Check(c);
      cnum1:=cnum;
      cnum:=ord(c);
    until (cnum1=13) and (cnum=10);
    OP_data := get_data;
    write(OP_data,' ');
    write(OP_file,OP_data,',');
    OP_data := get_data;
    write(OP_data,' ');
    write(OP_file,OP_data,',');
    OP_data := get_data;
    write(OP_data,' ');
    write(OP_file,OP_data,',');
    OP_data := get_data;
    write(OP_data);
    write(OP_file,OP_data);
    (* add time stamp to data every 10 samples*)
          if sample = 0 then
          begin
               GetTime(tHour,tMinute,tSecond,tHundredth);
               write(' - ',tHour,':',tMinute,':',tSecond);
               write(OP_file,' - ',thour,':',tMinute,';',tSecond);
               sample := 10
          end;
          sample := pred(sample); (* decrement sample *)
    writeln;
    writeln(OP_file);
```

```
      IF KeyPressed THEN BEGIN
        c := ReadKey ;
        IF (c = #0) THEN  { handle IBM Extended Ascii codes } BEGIN
          c := ReadKey ;  { get the rest of the extended code }
          if c= #68 then State:=MenuMode;
          END
        END
    UNTIL State = MenuMode
    END
  ELSE BEGIN
    WRITELN( 'You must open the port first!' )
    END;
    END { TermTest } ;



BEGIN { TtyDG }
  ClrScr ;
  WRITELN( '* Data Logging Software for BER Tester *' ) ;

  Open          := false ;
  DelayCount    := 1 ;
  TestPort      := 2 ;
  TestRate      := bps4800 ;
  TestWordLen   := 8 ;
  TestStopBits  := 1 ;
  TestParity    := NoParity ;
  CharMask      := $FF ;


REPEAT
  State := MenuMode ;
  OpenPort;
  WRITE( 'R(un, Q(uit ' ) ;
  REPEAT
    c := upcase( ReadKey ) ;
    UNTIL c IN ['R', 'Q'] ;
  WRITELN( c ) ;
  CASE c OF
    'R' : TermTest ;
    'Q' : State := Exitting
    END ; { CASE }
  UNTIL State = Exitting ;
  WRITELN( 'Closing async' ) ;
    Async_Close;
    close(OP_file)
END { TTYDG } .
```

Appendix 4 : Published Papers

Power Line Carrier Systems For Industrial Control Applications

Dr John E. Newbury, The Open University
Manchester, M21 9UN, UK
E-mail: J.E.Newbury@open.ac.uk

Kerry J. Morris, Elcontrol Ltd.
Weymouth, Dorset, DT4 9DW, UK
E-mail: kerry@elcontrol.demon.co.uk

Abstract - **This paper addresses the potential 4applications of power-line-carrier (PLC) communications technology within the field of industrial plant/equipment control. The special needs and requirements for this application (in terms of such factors as system integrity and response times) will be considered in comparison with those for other types of PLC application. Existing PLC technologies will be discussed and their suitability (or otherwise) for this application considered.**

I. Introduction

The low voltage distribution line, operating at 230V within the United Kingdom, potentially has a dual function. Firstly, as a carrier of electrical energy, operating at 230V and 50Hz, and secondly as a communications medium. The concept of using the power line for communications or control purposes has been with us for some time. By the 1940's, practical PLC systems were already in use over the high voltage distribution network [1], and during the same period, proposals were even made to utilise PLC to provide a telephone service to domestic users in remote areas [2]. In recent years, especially with the growth of interest in concepts such as 'home automation' moves have been made to define international standards relating to PLC.

This form of communication has potential coverage nation-wide, into both industrial, commercial and residential buildings throughout the UK, although in this instance we are concerned only with the in-building/on-site context.

However, there are disadvantages with this form of transmission medium. Unlike other media used for the transmission of data, which have well defined characteristics for bandwidth, characteristic impedance and potential noise levels, PLC is very undeterministic.

PE-390-PWRD-0-11-1998 A paper recommended and approved by the IEEE Power System Communications Committee of the IEEE Power Engineering Society for publication in the IEEE Transactions on Power Delivery. Manuscript submitted July 20, 1998; made available for printing December 2, 1998.

Even allowing for these disadvantages, PLC as a means of communication into buildings, both industrial and residential, have many advantages, as identified by Formby and Adams [3].

These problems are being addressed in the European Economic Commission's Committee for Electrotechnical Standardisation' (CENELEC) standard EN50065.
This standard provides the key characteristics for transmission and reception over the low voltage distribution line, in the frequency band 3KHz to 148.5KHz. The band 3KHz to 95KHz is reserved for communications by the utilities (e.g. meter reading or load control), and the band 95KHz to 148.5KHz for 'consumer' communications. In addition, the standard endeavours to tie-down other key characteristics of the power line, including impedance variation, signal disturbance and immunity to signal disturbance, modulation systems and protocols, and also to specify filters to condition the line, all with a view to facilitating efficient, seamless communication. Specifying all of these parameters is a quite formidable task, however good progress is being made.

II. A 'Typical' Industrial Control Scenario

An area in which PLC technology may prove to be of value is that of industrial process control. By this, we mean the 'real-time' control of an item of plant, machinery, or process. At its most grand, this may cover an entire industrial complex, but we are in this instance considering the control of a single 'stand-alone' installation (which may in turn be part of an overall distributed control system). The advantages which PLC might offer over conventional solutions will be discussed in subsequent sections.

Whilst this concept falls broadly under the heading of a 'Fieldbus', it is the intention of this paper to concentrate solely on the use and suitability (or otherwise) of the PLC technologies currently available, and not to dwell on other types of fieldbus physical layers.

Consider a typical industrial control scenario - a large burner installation used as a source of process heat for an industrial site. Physically, such plant can be quite large (at least as large as a medium-sized house).

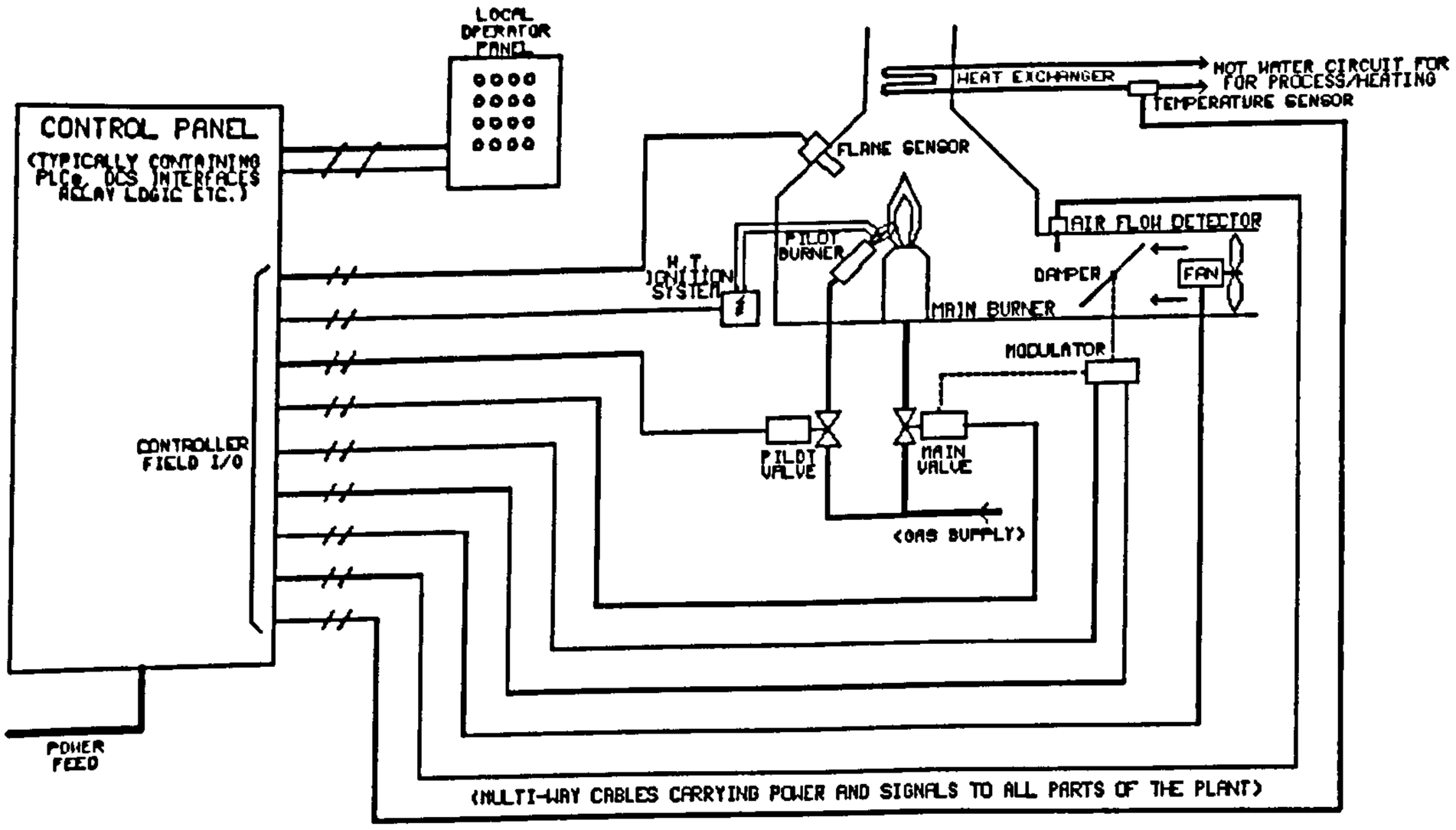


Fig. 1. Typical control application (simplified)

Conventionally, such an installation may have a local control panel, dedicated to the control of the particular installation, which may in turn link into a distributed control system for the entire site. In this paper we are primarily interested in considering the local control functions of the system.

There is likely to be a cabinet, containing the 'intelligence' of the control system - Programmable Logic Controllers, relays, indicators, operator control switches, and other electronic systems. The control panel will be operating a variety of valves and actuators on the plant, and likewise be monitoring the input from a range of sensors. Conventionally, all of these will be hard-wired to the control cabinet using a myriad of individual cables (Fig. 1).

In the example shown, most of the outputs from the control system are mains operated, as indeed are many of the sensors. Consider the benefits if all of this individual cabling could be replaced with a simple 'power-bus' running around the plant, distributing power and sending/receiving commands and data to the various plant inputs and outputs (Fig. 2). In addition to the much simplified initial wiring, modifications and upgrades would be facilitated.

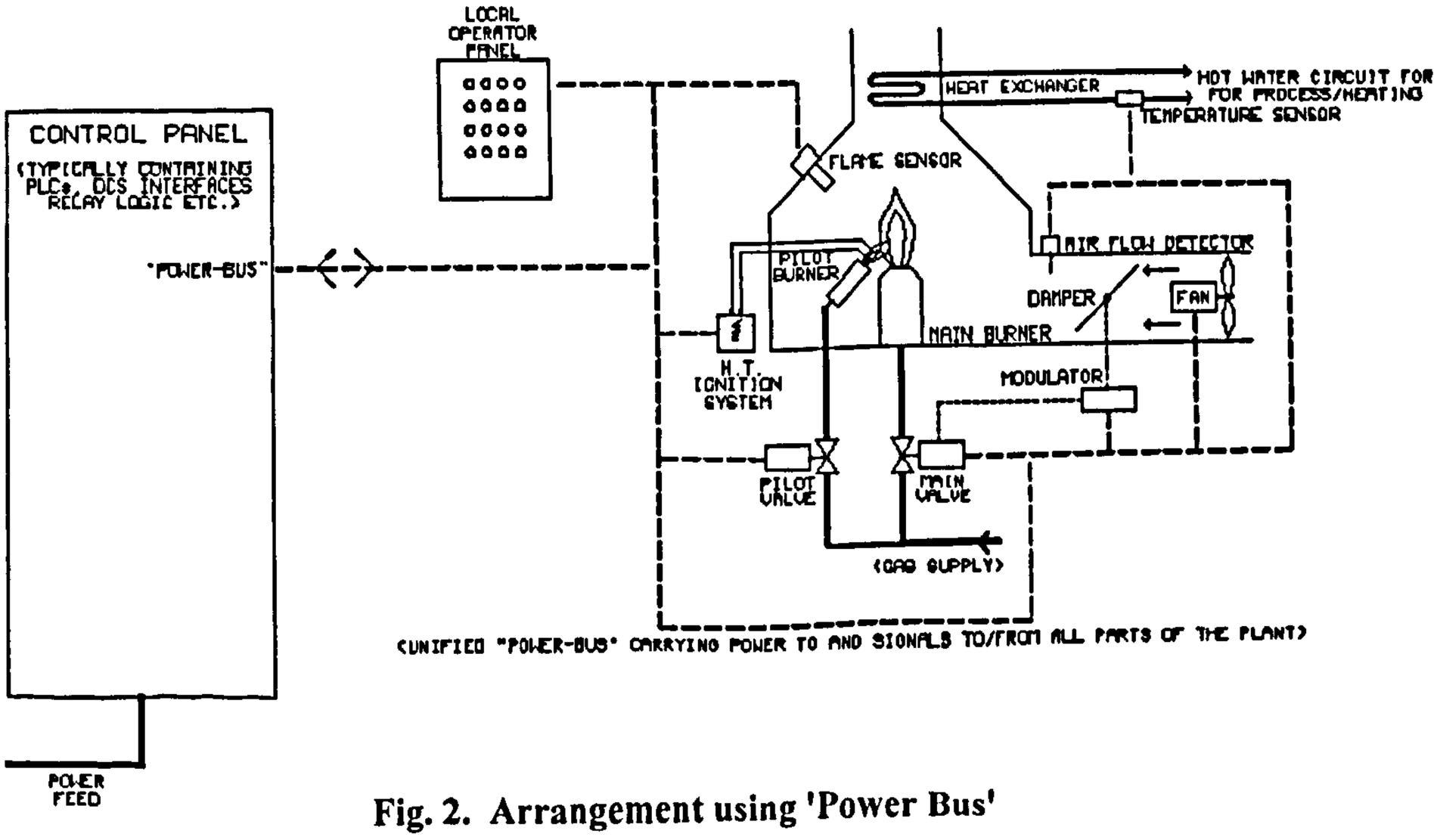


Fig. 2. Arrangement using 'Power Bus'

III. Practical Considerations

Much has been written of the unpredictable nature of the mains distribution network [4, 5, 6], and it is extremely difficult to make any generalisations regarding the characteristics likely to be experienced *on any one installation.*

In the context under consideration in this paper, we are at a slight advantage, in so far as the extent of the PLC network is known (i.e. the size of the plant), and the PLC environment is controllable (i.e. the equipment to be connected to it is known). The feed to the 'power-bus' (via the control cabinet) can easily be provided with in-line filters or stabilisation networks. Likewise, the various plant inputs and outputs, since they will be purpose built for the application, will be manufactured with predictable PLC characteristics. This may appear to make the design of such a system somewhat easier, but there are still many factors which must be considered for the safe and reliable operation of the plant. Because of the effective isolation of the envisaged 'power bus' from the rest of the distribution network, it can be argued that we do not necessarily have to conform to the recommendations of the international standards such as EN50065-1 [7], although, in truth, it would be unwise not to do so, and this is the approach which we will take in this paper.

In addition, in view of the 'safety critical' aspects of the type of application under consideration, regard must be given to the safety aspects of the PLC system, both in terms of the resilience of the communications network and the fault-tolerance of the hardware employed, particularly in view of the reliance on microprocessors/microcontrollers and other LSI or VLSI parts [8].

IV. Typical PLC Networks

It would next be prudent to consider some of the requirements for the industrial control PLC network, as against some other typical applications of PLC:

Let us first define some parameters to use in these comparisons:

Extent: An indication of the likely physical area to be covered by the communications network.

Response Time: How quickly can a transmission be sent from node to node on the network. This will depend on such factors as transmission speed, the number of nodes in service, and the protocol involved, plus of course the response requirements of the application.

Worst Case Response Time: The maximum delay, above and beyond the typical response time, that can be tolerated in a particular application (caused by re-transmissions due to line noise etc.)

Implications in the Event of Link Loss: How should the network behave if there is a breakdown of the communications link itself.

Implication of Node Loss: How should the network behave if one of the nodes is lost (through being disconnected or becoming faulty).

Data Security Implications: Is it necessary for the link to be secure (i.e. incapable of being monitored by third parties), and how necessary is it to avoid data corruption from interference, either caused deliberately, (due to malicious tampering), or as a result of such factors as line noise.

Now let us look at specific applications:

A) Automatic Meter Reading

Extent: Possibly very wide, but most likely to be between a local electricity sub-station and the consumers served by it. Data would most likely be sent onwards from the substation by other network systems which may or may not utilise PLC.

Response Time: A typical scenario (for the electricity supply industry) would involve meter readings being taken every 30 minutes. Other types of utility could probably tolerate even longer response times.

Worst Case Response Time: A delay of a few minutes in acquiring the next reading would not present a significant problem in any likely A.M.R. application.

Implications in the Event of Link Loss: Since (at least in the simplest form of the application) data is simply being read, and nothing is being controlled, there would be no serious implications.

Implication of Node Loss: Again, there would be no serious implications.

Data Security Implications: The ability to falsify the data would be highly undesirable.

B) Home Automation:

Extent: By definition, local, within a home or building.

Response Time: A response within 1-2 seconds would be acceptable in most instances. Certain types of device (e.g. heating appliances) could probably tolerate even longer response times.

Worst Case Response Time: Longer times than those above would present no serious problems, apart from possibly being inconvenient to the users.

Implications in the Event of Link Loss: Inconvenient, but no serious implication in most instances.

Implication of Node Loss: Again, inconvenient, but no serious implication in most instances.

Data Security Implications: If the system permitted access to the home/building or incorporated a security system, then susceptibility to external monitoring/tampering would be most unacceptable. Otherwise, no serious implications.

C). Industrial Automation:

Extent: Relatively localised (within the context under consideration) - it may involve a self-contained section of a plant, or may involve several items of plant sharing a network. The transfer of information over larger areas is likely to be handled by an alternative system such as a formal Fieldbus.

Response Time: A response time within 1-2 seconds maximum would be essential for real-time control of the type envisaged.

Worst Case Response Time: Longer times than (typically) twice those above would be unacceptable.

Implications in the Event of Link Loss: Potentially serious, if the loss existed for longer than a certain period, or occurred at the wrong point within an operational sequence of a process. Ideally, each node should have the ability to perform autonomously in a safe manner, and to gracefully shut down the process being controlled, should the link be lost.

Implication of Node Loss: Potentially serious in most instances. Impact can be minimised by the rest of the network hardware being able to gracefully shut down the process being controlled in the event of such a failure. This implies that the status of the nodes must be capable of being determined via the network itself, possibly with communication between nodes as well as simply via the master control cabinet.

Data Security Implications: Less important, unless there were a risk of malicious disruption to the process under control.

Analysing the previous statements, it can be seen that safety-critical real-time industrial control has some of the most stringent requirements of all of the applications discussed, requiring both a (relatively) fast response time and high levels of data and hardware integrity.

We will now consider some of the PLC technologies currently available and attempt to make an initial assessment as to their suitability for our purposes.

In reality, such systems must be split into two parts, the transmission technique, and the protocol. At this stage we need not concern ourselves with those aspects of the protocol relating to the higher levels of the OSI model, simply those which govern the integrity and routing of the data (i.e. level 4 and below). Whenever possible, we will discuss both transmission technique and protocol together.

V. Spread Spectrum vs. The Rest

Spread spectrum is much vaunted as a resilient technique for overcoming the problems inherent in real world PLC applications, although some commentators do express certain reservations [9]. It may be simply defined as a technique for deliberately increasing the bandwidth requirements of a transmission above and beyond those limits dictated by simple signalling theory. Spread spectrum techniques have implications with regard to both transmission security, bandwidth sharing, and immunity to noise and other interference sources. In this context, the latter attributes are of most interest.

The term spread spectrum can be applied to a range of different techniques for spreading the bandwidth of the signal.

Direct Sequence: Here the spreading is achieved by modulating the data stream with a pseudo-random spreading sequence.

Frequency Hopping: As the name suggests, this technique uses a range of different carrier frequencies, and either moving between them rapidly, in a known sequence, or changing in response to varying line conditions.

Chirp: Here, the transmitted signal consists of a carrier swept over a certain frequency range.

A factor which limits the usefulness of spread spectrum techniques for the purpose under consideration is the relatively small bandwidths permitted for 'consumer' transmissions under the CENELEC standard for PLC [7]. Vendors who offer spread spectrum solutions for use within the wider 'utility' part of the PLC spectrum have to resort to other modulation techniques for their 'consumer' products. An example is Echelon, whose PLC modem is mentioned later in this paper.

VI. The X-10 System

X-10 is a relatively long established (almost 20 years) system of power line carrier communication. It is very popular amongst the 'home automation' fraternity, particularly in the USA. It has a relatively simple protocol and command set [10] geared up towards home automation functions (i.e. switching lights on and off, controlling heating etc.).

In essence it can be described as an on-off keying (OOK) system, utilising a fixed single carrier frequency of 120KHz. The protocol is extremely simple, indeed, at its most basic there is not even any mechanism to acknowledge that a particular command has been received correctly. The only concession towards error detection is a bi-phase bit transmission protocol, coupled with duplication of each transmission. There are certain enhancements to the basic protocol which do permit some scope for two-way data traffic, and thus the potential for improved error detection/correction.

The relatively slow bit rate (synchronised to that mains zero-crossing points) and bit redundancy, means that X-10 commands take around a second to send at best, and commands requiring acknowledgements, or the transfer of data, correspondingly longer.

In conclusion, X-10 probably represents a minimum standard for a workable PLC control system, although it would be essential that a protocol allowing error detection was implemented. It does already operate within the CENELEC frequency band designated for 'consumers' [7], although not at the preferred 'Access Protocol' frequency. Conceivably, the carrier frequency could be moved in order to become compliant, but this would represent a variation of the X-10 system.

VII. CEBus

CEBus ('Consumer Electronic Bus') is an open standard for home automation systems endorsed by the Electronic Industries Association ('EIA'). Although primarily intended for home automation applications, it comprises a comprehensive and sophisticated protocol, suitable for our application, and is capable of operating over a range of other media as well as power line. The manufacturer Intellon support CEBus with their range of products, including a spread spectrum power line modem using the 'chirp' principle. Unfortunately though, this solution does not comply with the CENELEC requirements for the 'consumer' band.

VIII. Echelon LonWorks PLC Modems

Echelon offer a PLC solution based on the requirements of EN50065-1 [7] in terms of both frequency band and access protocol. The 'consumer' ('C') band variant operates at a nominal carrier frequency of 132.5KHz (for compliance with the CENELEC access protocol), using Binary Phase Shift Keying (BPSK) as the modulation type, and Echelon's proprietary 'LonTalk' protocol.

IX. Other Digital Techniques & Protocols:

Other manufacturers have responded to the need for PLC hardware with a range of different modem solutions. The more recent parts comply with the CENELEC 'Access Protocol', as outlined in EN50065-1 - operating at or around a frequency of 132.5KHz. The access protocol permits the sharing of the band, both by other systems of the same type, or by different systems utilising different modulation types or protocols. Examples of such devices are the ST7537HS1 from SGS-Thomson [11], which utilises a narrow-band FSK modulation technique centred around 132.45KHz, and the recently introduced TDA5051 from Philips [12], which uses an ASK technique centred on 132.5KHz. The ST7537HS1 part ties in with the 'European Home System' ('EHS') a European effort directed at a similar market to the CEBus already discussed. Another power line modem is the National Semiconductor LM1893/LM2893, an older FSK part, released before EN50065, which is nevertheless capable of complying with the requirements of that standard.

X. Conclusions:

It is the intention to consider the suitability of these different PLC technologies for the purposes of industrial control, based on the pre-requisites already discussed. These conclusions will be backed up by appropriate experimental findings, to determine the performance of the technology. Where proprietary combinations of transmission technique and protocol exist, they will be considered together. In other cases (such as the discrete modem chips described in section 10), appropriate protocol(s) will be chosen to suit. The results will hopefully be discussed in subsequent papers.

XI. References:

[1] M. J. Brown, *Power-Line Carrier Channels*, AIEE Transactions on Electrical Engineering, Vol. 64, May 1945

[2] J. M. Barstow, *A Carrier Telephone System for Rural Service*, AIEE Transactions on Electrical Engineering, Vol. 66, 1947

[3] Formby and Adams, *Low Voltage Mains Signalling* , Electricity Association Report, 1972

[4] Moulinex, *Examination of Document EN 50 0065-7*, August 1993

[5] R. M. Vines et. al, *Noise on Residential Power Distribution Circuits*, IEEE Transactions on EMC, Vol. EMC26, No. 4, November 1984

[6] R. M. Vines et. al, *Impedance of the Residential Power Distribution Circuit*, IEEE Transactions on EMC, Vol. EMC27, No. 1, February 1985

[7] CENELEC, *Signalling on low-voltage electrical installations the frequency range 3kHz to 148.5kHz*, EN 50065-1, January 1991

[8] Health and Safety Executive, *Programmable Electronic Systems in Safety Related Applications*, Parts 1 & 2, HMSO 1987

[9] CENELEC SC105A, *Reflection on the Transmission by Current Carriers in Household Units*, SC105A (Secretariat), October 1993

[10] X-10 (USA) Inc. *X-10 Technology Transmission Theory*

[11] SGS-Thomsom Microelectronics, *ST7537HS1 Home Automation Modem Data Sheet*, June 1995

[12] Philips Semiconductors, *TDA5051 Home Automation Modem, Preliminary Specification*, March 1997

[13] National Semiconductor, *LM1893/LM2893 Carrier Current Transceiver Data Sheet*, April 1995

XII. Author Biography:

John Newbury is head of the Power Communications Research Group, Open University, Manchester, England. He holds the BSc, MSc and PhD Degrees in Physics. He is currently researching metering communications, signalling techniques, modulation systems and protocols for low/ voltage and medium voltage systems.

He holds positions with British Standards Institute Committees, European Committees, CENELEC and IEC Committees, together with the I.E.E.E. PES Communication Systems Committees and I.E.E.E. AMRA SCC31.

Kerry Morris is an external research student with the Open University. He holds the degree of BA(Honours) in the subject area of Electronics and Computing, and is a Member of the British Computer Society (MBCS).

He is employed by Elcontrol Ltd, a small UK industrial control equipment manufacturer, where he is Chief Engineer.

He is researching the practical applications of PLC technology within the control industry.

Appendix 5: Table of Figures

NOTE: Some of the figures in this Thesis are reproduced from other sources, such as technical papers, manufacturers data sheets, or Web pages. The following references acknowledge the source of such figures.

Fig. 1 Propagation of Power Line carrier Signals through the Distribution Transformer, Paul Horridge, PhD Thesis, The Open University, 1996

Figs. 2, 3, 4, 5 Computer Modelling of Distribution Networks to Predict the Propagation of Mains-Marked Signals for Tariff and Load Control, M. R. Gasteen, R. F. Burbridge, University of Bristol, 1982

Figs. 6, 7 Ripple Control System and Load Control in Electricity Supply Networks HD-Comsys & Itd tim, Hungary
www.tel.hr/hdc-itd/RCS/RCS-Introduction.htm
www.tel.hr/hdc-itd/RCS/RCS-Choice%20of%20control%20frequency.htm
www.tel.hr/hdc-itd/images/RCS/PulsePattern.gif

Figs. 8, 9 — Programmable Logic Controllers, Eugene Kowch, PID Consultants Inc.
HTI Home Toys News, February 1997
hometoys.com/htinews/feb97/articles/pid/plc.htm
hometoys.com/htinews/feb97/articles/pid/PLC.gif
hometoys.com/htinews/feb97/articles/pid/SBD.gif

Fig. 10 — Technical Note: Using IEC 1131 Languages for Programmable Motion Control
Innovative Motion Control Solutions for Industry, UNICO Inc., USA
www.unicous.com/html/1131.html
www.unicous.com/scans/ld.gif

Fig. 11 — Integrated Circuit/Spread Spectrum Power Line Communication,
National Semiconductor et Al., 1991

Figs. 12, 13 — TechFest Ethernet Technical Summary, TechFest.com, 1999
www.techfest.com/networking/lan/ethernet5.htm
www.techfest.com/networking/cabling/utp.gif
www.techfest.com/networking/cabling/thinnet.gif

Fig. 14 — Communication Systems and Technology, Lecture 11: Optical Fiber Technology
R. Victor Jones, Harvard University, December 15, 1999
people.deas.harvard.edu/~jones/cscie129/lectures/lecture11/lecture_11.html
people.deas.harvard.edu/~jones/cscie129/lectures/lecture11/images/tir_2.gif

Figs. 15, 16 — Digital X-10, Phillip Kingery, Advanced Control Technologies, Inc.
HTI Home Toys magazine Article, February 1999
www.hometoys.com/htinews/feb99/articles/kingery/kingery13.htm
www.hometoys.com/htinews/feb99/articles/kingery/hti-2-14.gif
www.hometoys.com/htinews/feb99/articles/kingery/hti-2-03.gif

Fig. 17 — Charles Spurgeon's Ethernet Web Site
wwwhost.ots.utexas.edu/ethernet/
wwwhost.ots.utexas.edu/ethernet/metcalfe-enet.gif

Figs. 18 - 21 — Introduction to Network Topologies and Technologies
R L Warrender, Sunderland University
osiris.sunderland.ac.uk/~cs0rwa/ITE/Lecture4.htm
osiris.sunderland.ac.uk/~cs0rwa/ITE/Lecture4_files/image007.gif
osiris.sunderland.ac.uk/~cs0rwa/ITE/Lecture4_files/image009.gif
osiris.sunderland.ac.uk/~cs0rwa/ITE/Lecture4_files/image008.gif
osiris.sunderland.ac.uk/~cs0rwa/ITE/Lecture4_files/image011.gif

Fig. 24 — An Example of a MAP Implementation, Hugh Jack, 'Engineer On a Disk', 2001
claymore.engineer.gvsu.edu/~jackh/eod/hardware/
hardware-78.html#pgfId-153439
claymore.engineer.gvsu.edu/~jackh/eod/hardware/hardware-33.gif

Fig. 25 — The I²C Faq, Vincent Himpe
www.ping.be/~ping0751/i2cfaq/i2cproto.htm
www.ping.be/~ping0751/i2cfaq/g01proto.gif

Figs. 26, 43 What is HART?, Romilly Bowden, 1997
www.romilly.co.uk/whathart.htm
www.romilly.co.uk/hartwave.gif
www.romilly.co.uk/hmessage.gif

Fig. 29, 44 EMC for Product Designers, Tim Williams, Newnes 1996

Figs. 31 - 35 Course T322, Digital Telecommunications
Block 6: Coding and Modulation
The Open University, 1990

Figs. 36, 37 Spread Spectrum, Witold Jachimczyk
www.ece.wpi.edu/courses/ee535/hwk11cd95/witek/witek.html#4
www.ece.wpi.edu/courses/ee535/hwk11cd95/witek/dsexample.gif
www.ece.wpi.edu/courses/ee535/hwk11cd95/witek/fh1.gif

Fig. 38 Intellon Corporation White Paper #0027,
CEBus Power Line Encoding and Signalling
Intellon Corporation, March 1997

Figs. 45, 46 The ST7537HS1 Home Automation Modem,
SGS-Thomson Microelectronics, June 1995

Fig. 49 TDA5051 Home Automation Modem,
Philips Semiconductors, September 1997

Fig 50 TDA5051A – Application Note MOD_V1
A Multi-Purpose Power Line Communication Module
Eric Michat, Michat Electronique, 1998

Appendix 6: References and Bibliography

1 W. Hacklander, S. Furchtbar
Mains Signalling System
Elektor Electronics, April 1994

2 M. J. Brown,
Power-Line Carrier Channels
AIEE Transactions on Electrical Engineering,
Vol. 64, May 1945

3 J. M. Barstow
A Carrier Telephone System for Rural Service
AIEE Transactions, Vol. 66, 1947

4 M. R. Gasteen, R. F. Burbridge
Computer Modelling of Distribution Networks to Predict the Propagation of Mains-Marked Signals for Tariff and Load Control
University of Bristol, 1982

5 Distribution Control Systems, Inc.
Features of TWACS Communications
www.twacs.com

6 Horst Ziegler et. Al.
The M-Bus: A Documentation
M-Bus user group, November 1997

7 John Newbury & Kerry Morris
Power Line Carrier Systems for Industrial Control Applications
IEEE Transactions on Power Delivery,
Volume 14, No. 4, October 1999

8 R. Loxton & P. Pope,
Instrumentation: A Reader
Open University Press, 1986

9 Konrad Zuse
My first computer and first thoughts about data processing
Symposium: 'Computer Design Past, Present, Future',
Lund, Sweden, October 1987

10 Dick Morley
The History of the PLC
R. Morley Incorporated, 2001

11 The Bluetooth Consortium
Specification of the Bluetooth System
Version 1.1
February 22nd, 2001

12 The X-10 Corporation
X-10 FAQ, Section 3: Details on X-10 Protocol
January 1997

13 Intellon Corporation
CEBus Power Line Encoding and Signalling
Intellon Corporation White Paper #0027, March 1997

14 Pierre Guillemin
The European Home Systems Protocol -
Concepts and Products
SGS-Thomson Microelectronics
www.domotics.com/homesys/HSpapers/EHSproto.htm

15 Reinhard Seyer and Dr. Manfred Stege
System Technology for Private Houses - EHS
Home Automation for Heating,
White Goods and Energy Management
Daimler-Benz AG Research and Technology
www.domotics.com/homesys/HSpapers/daimlerbenz.htm

16 SGS-Thomson Microelectronics
The ST7537HS1 Home Automation Modem
June 1995

17 Ira Goldschmidt
The Development Of BACnet
RNL Design, 1998
www.bacnet.org/Bibliography/SPEE-11-98.html

18 Robert H Zakon
Hobbes' Internet Timeline v5.2
2000
www.zakon.org/robert/internet/timeline/

19 J.C.R. Licklider and Robert W. Taylor
The Computer as a Communication Device
Science and Technology, April 1968

20 Adrian Rawlings et Al.
T322 Digital Telecommunications,
Block 10: Networks
The Open University, 1990

21 Robert M. Metcalfe and David R. Boggs,
Xerox Palo Alto Research Center
Ethernet: Distributed Packet Switching for Local Computer Networks
Communications of the ACM, Vol. 19, No. 5, July 1976

22 Professor John Larmouth
Understanding OSI
Salford University, 1994

23 Colin Pye
What is MAP?
NCC Publications, 1988

24 Philips Semiconductors,
The I^2C Bus Specification, version 2.1
January 2000

25 Robert Bosch GmbH
CAN Specification
Version 2.0, September 1991

26 Romilly Bowden,
HART Field Communications Protocol, a Technical Description
Rosemount AG, 1991

27 International P-Net User Organisation
An Overview of the P-Net Fieldbus
www.p-net.dk/download/conf3/504500.pdf

28 Profibus Users Organisation
The Profibus Standard
August 1992

29 Robin Garside
Electrical Apparatus and Hazardous Areas (Third Edition)
Hexagon Technology Limited, 2000

30 R. Cortina, Gioltini et. Al.
Telecommunication Systems on Power Distribution Networks: High Frequency Performances of Carrier Channels
IEEE Transactions on Power Delivery, April 1993

31 Olaf G. Hooijen and A. J. Van Vinck
On the Channel Capacity of a European-Style Residential Power Circuit
PLC'98 Conference, 1998

32 J. B. O'Neal
The Residential Power Circuit as a Communications Medium
North Carolina State University, 1986

33 J. A. Malack and J. R. Engstrom
RF Impedance of Power Lines and Line Impedance Stabilisation Networks in Conducted Interference Measurements
IEEE Transactions on Electromagnetic Compatibility, May 1973

34 R. M. Vines, H. Joel Trussell et Al.
Impedance of the Residential Power-Distribution Circuit
IEEE Transactions on Electromagnetic Compatibility, February 1985

35 M. Chan and R. W. Donaldson
Attenuation of Communications Signals on Residential and Commercial Intrabuilding Power Distribution Circuits
IEEE Transactions on Electromagnetic Compatibility, 1986

36 M. Chan and R. W. Donaldson
Width and Interarrival Distributions for Noise Impulses on Intrabuilding Power Line Communications Networks
IEEE Transactions on Electromagnetic Compatibility, August 1989

37 J. H. Bull and W. Nethercot
The Frequency of Occurrence and the Magnitude of Short Duration Transients in Low-Voltage Supply Mains
The Radio and Electronic Engineer, 1964

38 Tim Williams
EMC for Product Designers
Newnes, 1996

39 CENELEC
EN 50081-1:1992
Electromagnetic Compatibility
Generic Emission Standard
Residential, Commercial and Light Industry

40 CENELEC
EN 50081-2:1993
Electromagnetic Compatibility
Generic Emission Standard
Industrial Environment

41 CENELEC
EN 50082-1:1997
Electromagnetic Compatibilty
Generic Immunity Standard
Residential, Commercial and Light Industry

42 CENELEC
EN 50082-2:1995
Electromagnetic Compatibility
Generic Immunity Standard
Industrial Environment

43 CENELEC SC205A
prEN 50065-4-1 : 1999
Signalling on Low-Voltage Electrical Installations
in the Frequency Range 3 kHz to 148.5 kHz
Part 4-1 : Low-Voltage Decoupling Filters - Generic Specification
August 1999

44 Philips Semiconductors
TDA5051 Home Automation Modem
September 1997

45 Echelon Corporation
LonWorks PLT-22 Power Line
Transceiver User's Guide
110 kHz to 140 kHz Operation
1999

46 National Semiconductor, Cyplex et Al.
IC/SS – Integrated Circuit/Spread Spectrum
Power Line Communication
1991

47 National Semiconductor
ICSS1001, ICSS1002, and ICSS1003
IC/SS Power Line Carrier
Local Area Network Chip Set
September 1993

48 CENELEC
EN 50065-1:1991
Specification for Signalling on Low-Voltage Electrical Installations in the Frequency Range 3 kHz to 148.5 kHz. General Requirements, Frequency Bands and Electromagnetic Disturbances

49 CENELEC SC205A
prEN 50065-2-1
Signalling on Low Voltage Electrical Installations in the Frequency Range 3 kHz to 148.5 kHz
Part 2-1 : Immunity Requirements for Mains Communications Equipment and Systems Operating in the Range of Frequencies 95 kHz to 148.5 kHz and intended for use in Residential Commercial and Light Industrial Environments
November 2000

50 CENELEC SC205A
prEN 50065-2-2
Signalling on Low Voltage Electrical Installations in the Frequency Range 3 kHz to 148.5 kHz
Part 2-2 : Immunity Requirements for Mains Communications Equipment and Systems Operating in the Range of Frequencies 95 kHz to 148.5 kHz and intended for use in Industrial Environments
April 1999

51 CENELEC SC205A
prEN 50065-2-3
Signalling on Low Voltage Electrical Installations in the Frequency Range 3 kHz to 148.5 kHz
Part 2-3 : Immunity Requirements for Mains Communications Equipment and Systems Operating in the Range of Frequencies 3 kHz to 95 kHz and intended for use by Electricity Suppliers and Distributors
May 1998

52 CENELEC SC205A
prEN 50065-7
Signalling on Low Voltage Electrical Installations in the Frequency Range 3 kHz to 148.5 kHz Equipment Impedance
January 1999

53 Gaby Smol et Al.
T322 Digital Telecomminications,
Block 3: Reliability, Traffic and Information (Section 6.3.4)
The Open University, 1990

54 High Tech Horizon
S.N.A.P. - Scaleable Node Address Protocol, Revision 0.91
High Tech Horizon, 1998

55 Eric Michat
TDA5051A – Application Note MOD_V1 A Multi-Purpose Power Line Communication Module
Michat Electronique, 1998

56 Amar Palacherla
Application Note: AN544 Maths Utility Routines: Pseudo random Number Generator
Microchip Technology Incorporated, 1997

57 Microchip Technology Inc.
The PIC16F84 8-Bit CMOS FLASH Microcontroller
Microchip Technology Data Book, 1993

58 Michael Quinlan and Arley Dealey
Async4: Combined IBM, DG/1 serial interrupt handler unit for Turbo Pascal, version 4.0b
November 1987

59 Moulinex, France
Examination of the document 50065-7 (Project dated August 1993)
SC 105A/WG4, Paris/Rome, 16th September 1993

60 Kerry J. Morris
The Design of a Microprocessor-Based Controller for Safety Critical Applications (T401 Project)
The Open University, 1991

61 Marek Kuczsynski
Certification Testing: Guidelines for Writing and Submitting Software for Microprocessor Based Burner Control Units
British Gas Research and Technology publication MRS I 3523

62 CENELEC
EN 298 : 1993 Automatic Gas Burner Control Systems for Gas Burners and Gas Burning Appliances with or without Fans

63 Claude Shannon
A Mathematical Theory of Communication
The Bell System Technical Journal, Vol. 27, July, October 1948

64 John E. Newbury
Data Communications at High frequency using the Power Grid
Open University, Manchester, England, 1999

65 The Smith Group Ltd. for the Radiocommunications Agency (RA)
A study to develop a model to predict the radiation properties of certain line transmission systems
2000

66 The Radio Society of Great Britain
Compatibility Between Radio Communications Services and Power Line Communication Systems
RSGB EMC Committee, February 2001

67 European Radiocommunications Committee
Current and Future Use of Frequencies in the LF, MF and HF Bands
ERC Report 107, February 2001

68 Dan Raphaeli and Evgeni Bassin
A Comparison between OFDM, Single Carrier, and Spread Spectrum for High Data Rate PLC
Itran Communications, Israel, 1999

69 Department of Computer Engineering, Kasetsart University
What is TCP/IP?
(extract from course #204325 - Introduction to Computer Communications and Networks)
www.cpe.ku.ac.th/~nguan/204325/slides/tcpip.pdf

70 Steve Freyder, David Helland and Bruce Lightner
A $25 Web Server
Circuit Cellar Magazine, July 1999

71 Joe Desbonnet and Peter M. Corcoran
Browser-Style Interfaces to a Home Automation Network
IEEE Transactions on Consumer Electronics, June 1997

72 Joe Desbonnet and Peter M. Corcoran
System Architecture and Implementation of a CEBus/Internet Gateway
IEEE Conference on Consumer Electronics, Chicago, June 1997