

Zero to Mastery In
Computer Troubleshooting & Maintenance

Zero to Mastery In
**Computer Troubleshooting
& Maintenance**

Dr. RK Jain

• Shadab Saifi (*Illustrator*) • Ayaz Uddin (*Editor*)



An ISO 9001:2008 Certified Company

Vayu Education of India

2/25, Ansari Road, Darya Ganj, New Delhi-110 002

Contents

1.Repair, Servicing and Maintenance Concepts	1
1.1. Introduction of Servicing and Maintenance	1
1.1.1 Preventive Maintenance	2
1.1.2 Corrective Maintenance	3
1.1.3 Maintenance Activities	2
1.1.4 The Indenture level	4
1.1.5 The Maintenance Level	4
1.1.6 The Maintenance Line or Echelon	5
1.1.7 The Maintenance Policy	6
1.2 Meantime Between Failure (MTBF), Meantime To Repair (MTTR) Maintenance Policy	7
1.2.1 Introduction	7
1.2.2 What is a Failure? What are the Assumptions?	7
1.2.3 Reliability, Availability, MTBF, and MTTR Defined	8
1.2.4 Methods of Predicting and Estimating MTBF	11
1.2.4.1 Reliability Prediction Methods	11
1.2.4.2 Reliability Estimation Methods	13
1.2.5 Conclusions	14
1.3 Potential Problems of Preventive Maintenance and Corrective Maintenance	14
1.3.1 Relationship to Preventive Maintenance to Corrective Maintenance	16
1.4 Circuit Tracing techniques	18
1.5 Concept of Shielding, Grounding and Power Supply requirements	29
1.5.1 Power Grounding Basics	29
1.5.2 Grounding, Bonding and Overload Protection	30
1.5.2.1 Grounding Electrode Resistance	31
1.5.2.2 Power Grounding Definitions	31
1.5.2.3 Separately derived Instrumentation Power System	32
1.5.2.4 Single-Point Grounding of Power Supplies	33
1.5.2.5 The Ungrounded System	34
1.5.2.6 Resistance Grounding	35
1.5.2.7 Shielding Theory	35
1.5.2.8. Power Supply Shielding	40
1.6. Considerations of Computers and its Peripherals	42
Exercise	43
2.Fundamental Troubleshooting Procedures	44
2.1 Troubleshooting Process	44
2.1.1 Fault Establishment	44
2.2 Fault Location	44

(Vii)

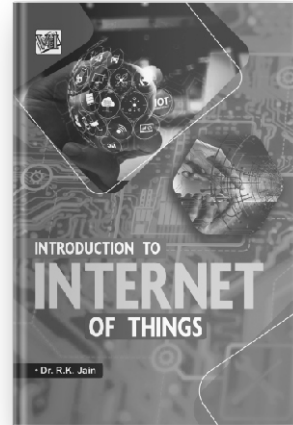
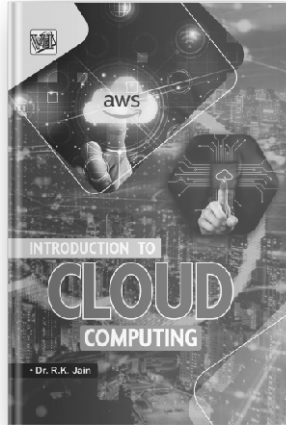
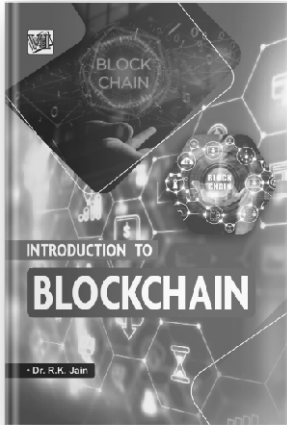
2.2.1	Fault Correction	44
2.2.2	Fault Location Procedure	44
2.3	Fault Finding Aids	46
2.4	Service Manuals	46
2.5	Testing and Measuring Instruments	47
2.6	Special Tools	47
	Exercise	50
3.	Hardware and Software Faults	51
3.1.	Troubleshooting Techniques	51
3.1.1	Preliminary Observations	51
3.2	Different Troubleshooting Techniques and Methods	53
3.3	Functional Area Approach	53
3.4	Split-Half Method	53
3.5	Divergent, Convergent and Feedback path circuits	54
3.5.1	Divergent Paths	54
3.5.2.	Convergent Paths	55
3.5.2.	Feedback Paths.....	55
3.5.2.1.	Switching Paths	56
3.6	Analysis Measured techniques.....	56
3.6.1	Software Test Techniques for System Fault-Tree Analysis	61
	Exercise	65
4.	Troubleshooting of Computers: Components and Peripherals	66
4.1	Motherboard	66
4.1.1	Troubleshooting of Mother Board	67
4.2	Floppy Disk Drive (FDD)	71
4.2.1	Trouble shooting of FDD	73
4.2.1.1	Bad Floppy Diskette	73
4.2.1.2	Not Setup in CMOS	74
4.2.1.3	Confliction with other hardware	74
4.2.1.4	Not Connected Properly	74
4.2.1.5	Bad Drivers	75
4.2.1.6	Bad Hardware	75
4.3	Hard Disk Drive (HDD)	75
4.3.1	Form Factors	76
4.3.2	Troubleshooting of Hard Drive	77
4.3.2.1	Checking Physical connectivity	77
4.3.2.2	Checking Jumper Settings	78
4.3.2.3	Checking SCSI Termination	78
4.3.2.4	Checking BIOS Setup (IDE only)	79
4.3.2.5	Virus Checking	79
4.3.2.6	Checking for a Valid Partition	79
4.3.2.7	Checking Drive Formatting	80
4.3.2.8	Fixing Physical and Logical Drive Errors	80
4.3.2.9	Checking and Reactivating Disks in the Windows 2k/XP Oss	81
4.4	CD ROM/DVD	81
4.4.1	Troubleshooting of CD ROM/DVD	82
4.5	Printers	85
4.5.1.	Troubleshooting of Printers	86

4.6	Modems	86
4.7	Monitors	89
4.7.1	Troubleshooting of Monitors	90
4.7.1.1	Monitor is Blank after Restarting System	90
4.7.1.2	After Connecting a Monitor, the Picture Looks Bad	90
4.7.1.3	The Monitor has Started Making a Strange Noise	90
4.7.1.4	Monitors Display Settings are not Correct	91
4.7.1.5	Display is Rotated	91
4.8	Switched – mode power supply (SMPs)	91
4.7.1	Troubleshooting of Monitors	90
4.8.1	SMPS and Linear Power Supply Comparison	92
4.8.2	Theory of Operation	94
4.8.2.1	Input Rectifier Stage	94
4.8.2.2	Inverter Stage	95
4.8.2.3	Voltage Converter and Output Rectifier	95
4.8.2.4	Regulation	96
4.8.2.5	Transformer Design	96
4.8.2.6	Power Factor	96
4.8.3	Troubleshooting of SMPs	97
	Exercise	102
5.	Computer Repair and Maintenance	103
5.1	Specification, Maintenance and Repair of CVT (Constant Voltage Transformer)	103
5.1.1	History of CVT	105
5.1.2	Uses of CVT	105
5.1.3	Operation of CVT	105
5.1.4	Advantages and disadvantages	106
5.1.5	Instructions for Use (Installation)	107
5.1.6	Features	107
5.1.7	Output Voltage vs. Input Voltage	108
5.1.8	Typical Service, Storage, and Shipment Conditions	109
5.1.9	Application Considerations-Output Performance under Dynamic Supply Conditions	110
5.1.9.1	Performance: Voltage Interruption	110
5.1.9.2	Performance: Voltage Sag	111
5.1.9.3	Performance: Voltage Phase Shift	111
5.1.9.4	Performance: Oscillating Transient	111
5.1.9.5	Performance: Oscillating Transient	112
5.1.10	Application Considerations—CVT Electrical Characteristics during Linear and Nonlinear Loading	112
5.1.10.1	Performance: Line Current Distortion	112
5.1.10.2	Performance: Power Factor	113
5.1.11	Specifications: Below there is a chart of general specifications:	114
5.1.12	Maintenance and Repair of CVT	115
5.2	Specification, Maintenance and Repair of UPS (Uninterruptible Power Supply)	115
5.2.1	Common Power Problems	115
5.2.2	Applications	116
5.2.2.1	N+1	116
5.2.2.2	Multiple Redundancy	116
5.2.2.3	Outdoor Use	116

5.2.2.3	Internal Systems	116
5.3	Technologies	116
5.3.1	Offline/Standby	117
5.3.2	Line-interactive	117
5.3.3	Double-conversion/online	118
5.3.4	Ferro-resonant	119
5.3.5	DC Power	119
5.3.6	Rotary	119
	Exercise	120
6.	Environmental Requirement of Computer System and Peripherals	121
6.1	Environmental Requirements of Computer Systems and its Peripherals	121
6.1.1	Operating Specifications	124
6.1.2	Temperature	124
6.1.3	Humidity	125
6.1.4	Troubleshooting Environmental Conditions	125
6.1.5	Cooling and Aisle Airflow	127
6.1.6	Acclimatization	128
6.1.7	Vibration and Shock	128
6.1.8	Contaminants	128
6.1.9	Fire Containment	129
	Exercise	130
7.	Site Preparations and Designs	131
7.1	Site Preparations and Design of Computer Rooms	131
7.1.1	Site Selection	131
7.1.2	Fitting Out Requirements	132
7.1.3	Equipment Layout Planning	134
7.1.4	Electrical Requirements	135
7.1.5	Air-conditioning System	137
7.1.6	Fire Prevention, Detection and Suppression	138
7.1.7	Prevention of Water Leakage	140
7.1.8	Physical Security	140
7.2	Testing Specifications and Installation of Computer Systems and Peripherals	141
7.2.1	Validation Overview	141
7.2.2	Validation Master Plan and Project Plan	144
7.2.3	Design Qualification and Specifications	145
7.2.4	Vendor Assessment	147
7.2.5	Installation Qualification	149
7.2.6	Operational Qualification	150
7.2.7	Performance Qualification	151
7.2.8	Configuration Management and Control	152
7.2.9	Validation report and Other Documents	153
	Exercise	153
	Multiple Choice Questions & Answers	154
	Glossary	160
	Index	175

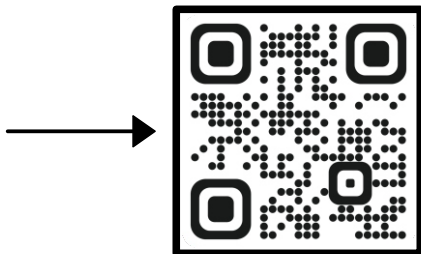
SPECIAL BONUS!

Want These 3 Bonus Books for free?



**Get FREE, unlimited access to these
and all of our new books by joining
our community!**

SCAN w/ your camera TO JOIN!



**OR Visit
freebie.kartbucket.com**

Repair, Servicing and Maintenance Concepts

Chapter

1

Instructional Objectives

- 1.1 Introduction to Servicing and Maintenance Concepts
- 1.2 Meantime Between Failure (MTBF) Meantime the Repair Maintenance Policy
- 1.3 Potential Problems of Preventive and Corrective Maintenance
- 1.4 Circuit Tracing Techniques
- 1.5 Concept of Shielding, Grounding and Power Supply Requirements
- 1.6 Considerations of Computer and its Peripherals

1.1 Introduction to Servicing and Maintenance Concepts

Maintenance is defined as those activities and actions that directly retain the proper operation of an item or restore that operation when it is interrupted by failure or some other anomaly. (Within the context of maintenance, proper operation of an item means that the item can perform its intended function.) These activities and actions include removal and replacement of failed items, repair of failed items, lubrication, servicing (includes replenishment of consumables such as fuel), and calibrations. Other activities and resources are needed to support maintenance. These include spares, procedures, labor, training, transportation, facilities, and test equipment. These activities and resources are usually referred to as logistics.

According to the maintenance definition, maintenance is a combination of actions intended to retain an item in, or restore it to, a state in which it can perform the function that is required for the item to provide a given service. This concept leads to a first classification of the maintenance actions in two main groups or types: actions oriented towards retaining certain operating conditions of an item and actions dedicated to restoring the item to said conditions. “Retention” and “restoration” are denominations for action types that are then converted into “preventive” and “corrective” maintenance types in the maintenance vocabulary. Following this criterion, the European standard for maintenance terminology presents the different types of maintenance classified according to Figure 1.1.

From the point of view of the maintenance actions, the more complex the item, the more need for the technical subdivision of the item. Complex items maintenance will therefore require the item subdivision into so-called indenture levels. It is common to find that maintenance needs — resources, qualification of resources, and so on — for each indenture level vary importantly. This leads us to the definition of maintenance levels, which are associated to indenture levels of the items. Notice that this association normally involves resource assignments and therefore resources needs to be properly organized and

managed at different positions in our organization. These positions are called maintenance lines, and they will be responsible for the accomplishments of different maintenance levels of different items.

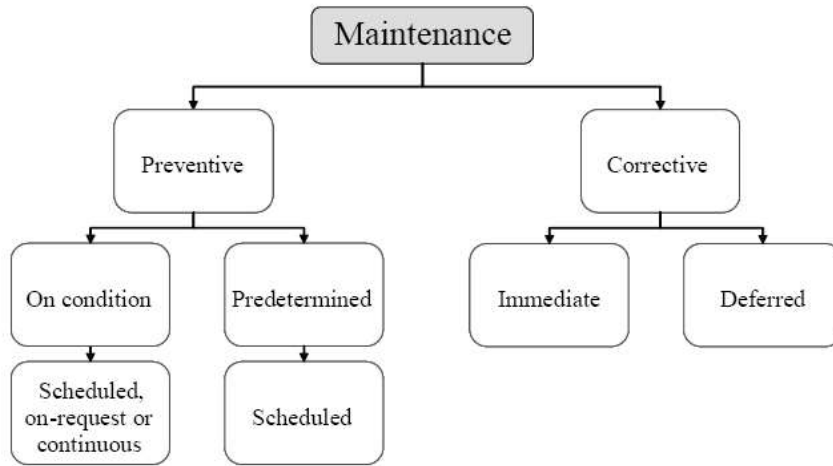


Figure 1.1: Maintenance types according to EN 13306:2001 [1]

1.1.1 Preventive Maintenance

Preventive maintenance is defined as maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the functioning of the equipment. Preventive maintenance can be predetermined or condition based:

- *Predetermined maintenance.* Preventive maintenance carried out in accordance with established intervals of time or number of units of use (*i.e. scheduled maintenance*) but without previous item condition investigation,
- *Condition based maintenance.* Preventive maintenance based on performance and/or parameter monitoring and the subsequent actions. Performance and parameter monitoring may be *scheduled, on-request* or *continuous*. Within the condition based maintenance we include the predictive maintenance, that can be defined as follows:

Predictive maintenance: Condition based maintenance carried out following a forecast derived from the analysis and evaluation of the significant parameters of the degradation of the equipment.

1.1.2 Corrective Maintenance

Corrective maintenance is maintenance carried out after fault recognition and intended to put the equipment into a state in which it can perform a required function. Corrective maintenance can be immediate or deferred:

- *Immediate maintenance.* Maintenance which is carried out without delay after a fault has been detected to avoid unacceptable consequences,
- *Deferred maintenance.* Corrective maintenance which is not immediately carried out after fault detection but is delayed according to given maintenance rules.

1.1.3 Maintenance Activities

Maintenance types consist of a set of maintenance activities in a given sequence. Most common maintenance activities can be listed and defined as follows:

- *Inspection*. Check for conformity by measuring, observing, testing or gauging the relevant characteristics of an item. Generally, inspection can be carried out before, during or after other maintenance activity:
 - * *Compliance test*. Test used to show whether or not a characteristic or a property of the equipment complies with the stated specification,
- *Monitoring*. Activity performed either manually or automatically intended to observe the actual state of the equipment. Monitoring is distinguished from inspection in that it is used to evaluate any changes in the parameters of the equipment with time. Monitoring may be continuous, over an interval of time, or after a given number of operations. Monitoring is usually carried out in the operating state,
- *Routine maintenance*. Regular or repeated elementary maintenance activities which usually do not require special qualification, authorization(s) or tools. Routine maintenance may include, for example, cleaning, tightening of connections, checking liquid level, lubrication, etc.;
- *Overhaul*. A comprehensive set of examinations and actions carried out in order to maintain the required level of availability and safety of the equipment. An overhaul may be performed at prescribed intervals of time or number of operations, and may require a partial or complete dismantling of the item,
- *Rebuilding*. Action following the dismantling of the equipment and the repair or replacement of those components that are approaching the end of their useful life and/or should be regularly replaced. The objective of rebuilding is normally to provide the equipment with a useful life that may be greater than the lifespan of the original equipment. Rebuilding differs from overhaul in that the actions may include improvements and/or modifications, understood as follows:
 - * *Improvement*. Combination of all technical, administrative and managerial actions intended to ameliorate the dependability of the equipment, without changing its required function;
 - * *Modification*. Combination of all technical, administrative and managerial actions intended to change the required function of the equipment. Modification, in fact, is not a maintenance action but concerns changing the required function of the equipment to a new required function. The changes may have an influence on the dependability or on the performance of the equipment, or both,
- *Repair*. Physical action taken to restore the required function of faulty equipment. Within a repair we can normally find the following actions:
 - * *Fault diagnosis*. Actions taken for fault recognition, fault localization at the appropriate indenture level and cause identification;
 - * *Fault correction*. Actions taken after fault diagnosis, to put the equipment into a state in which it can perform a required function,
 - * *Function check-out*. Action taken after maintenance actions to verify that the equipment is able to perform the required function.
 - * Function check is usually carried out after down state.

1.1.4 The Indenture level

Many of the modern industrial systems are complicated in their structure which consists of many interconnected elements. The cause and effect relationships between these elements will normally be difficult to capture because of their extent, their time delay, or simply because of their rare impact in system behavior patterns. Also, the history of these systems will be important for their behavior analysis. If we try to carry out complex systems maintenance, we have to take into account the considerations above before starting the implementation of our maintenance strategy. When trying to understand causes of equipment functional failure, we need to describe the different parts of the equipment structure, the different sub-functions and the possible causes of the function loss. Maintenance is always trying to eliminate these causes of functional failures that will be located at different levels of the equipment structure. The level of subdivision of an item from the point of view of the maintenance action is called the indenture level. Examples of indenture level could be a system, a subsystem, a component (Figure 1.2). There are several factors that may influence the equipment indenture level:

- The complexity of the equipment construction,
- The accessibility to the different subsystems.
- The required skill level of the maintenance personnel,
- The requirements for test equipment facilities,
- The need for specific safety considerations,
- *Etc.*

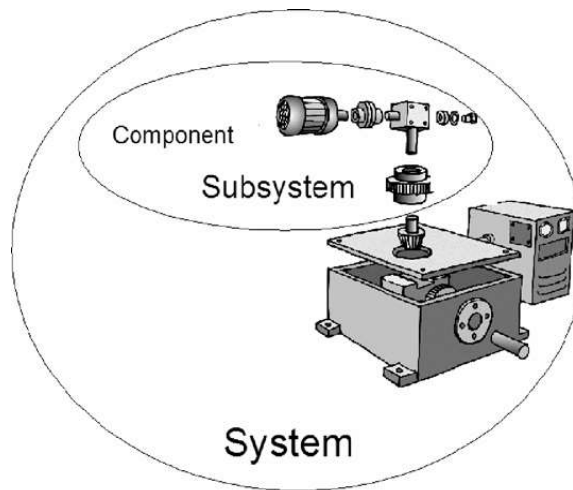


Figure 1.2: Equipment indenture level

1.1.5 The Maintenance Level

European standard defines a level of maintenance as the set of maintenance actions to be carried out at a specific indenture level. With this in mind, examples of maintenance actions at different indenture level would be replacing a system, a subsystem or a component.

However, in many real plants and factories, the levels of maintenance are not necessarily related to the indenture levels (item subdivisions) and this may, sometimes, induce confusion. The level of maintenance is commonly characterized by the complexity of the maintenance task. Therefore, different maintenance levels are not necessarily related to actions at different indenture levels but to actions of different technical complexity.

To illustrate this point, let us see the following example, where the maintenance levels of a real assembly plant are defined. This plant belongs to a well known multinational company that considers maintenance development to be a clear driver of their business competitive advantage. The plant started a TPM program several years ago with considerable success, and the current definition of the maintenance levels is as follows:

- Level 1: Autonomous management:
 - * Cleaning, inspection and lubrication standards,
 - * Simple repairs and replacements,
 - * Adjustments and format changes,
- Level 2: Corrective maintenance:
 - * Equipment cards removal (solving equipment anomalies);
 - * Fault diagnosis,
 - * Repairs,
- Level 3. Preventive maintenance:
 - * Preventive (including predictive) maintenance;
 - * Overhauls,
 - * Training and standardization,
- Level 4. Maintenance prevention:
 - * Improvements,
 - * Early equipment management,
 - * New equipment, techniques and systems,
- Level 5. Contracted Maintenance:
 - * Maintenance providers interventions,
 - * Important supplier's activities.

In this example, as the reader may perceive, maintenance levels seem to be more related to technical and/or managerial complexity than to indenture levels. However, it is obvious that preventive operations at level 3, or corrective operations at level 2, may deal with different indenture levels than those carried out at level 1.

In industry it is also common to assign higher maintenance levels to more complex maintenance tasks. In our example, maintenance task in levels 2 or 3 would require higher maintenance skills than those in level 1. However, this could not be applicable for levels 3 and 5.

1.1.6 The Maintenance Line or Echelon

The line of maintenance is a concept that links the level of maintenance to the existing maintenance organization. Note that the maintenance level concept is not related to the maintenance organization, but

to the item maintenance complexity, through the indenture level concept. The maintenance line concept, however, establishes the position in an organization where specified levels of maintenance are to be carried out on an item. Examples of line of maintenance are: field repair shop, maintenance provider shop or manufacturer.

The lines of maintenance are characterized by their location and their maintenance support, that is to say, the place where the maintenance is carried out and the resources, services and management necessary to carry out a certain level of maintenance activities. Support may include, for example, personnel, test equipment, work rooms, spare parts, documentation, tools, *etc.*

When maintenance is carried out at the location where the equipment is used we refer to this maintenance as *on-site maintenance*. Other maintenance activities will be off-site, for instance at the shop of a certain manufacturer. But it is also possible that, with the equipment on-site, maintenance is carried out off-site, *i.e.* without the physical access to the item — *remote maintenance*.

Regardless of the number of maintenance lines defined by a certain organization, the maintenance terminology standard defines *maintenance supportability* as the ability of a maintenance organization to have the right maintenance support at the necessary place to perform the required maintenance activity at a given instant of time during a given time interval. Maintenance supportability is therefore concerned with the effectiveness of an organization to provide the correct maintenance support, but an organization has to provide the right support in an efficient manner. The same standard defines the term *maintenance support efficiency* as the ratio between the planned or expected resources necessary to fulfill the required maintenance task and the resources actually used.

1.1.7 The Maintenance Policy

Maintenance actions at different indenture levels can then be classified in different maintenance levels. Maintenance levels will be then carried out at different positions of the maintenance organization named maintenance lines or echelons.

A maintenance policy is defined as the interrelationship between its maintenance echelons or lines, the items indenture levels and the maintenance levels to be applied for the maintenance of an item.

Figure 1.3 presents the maintenance lines where actions of the different maintenance levels. As we can see in that figure, the first level of maintenance is accomplished by operators of the production lines or cells. They are the first maintenance line. The second maintenance line is the maintenance department of each production unit. They are responsible for the corrective activities within the second level of maintenance. A maintenance department at a higher level, common support for all production units, is the third maintenance line which is responsible for the other three levels of maintenance: preventive maintenance, maintenance improvement and contracted maintenance.

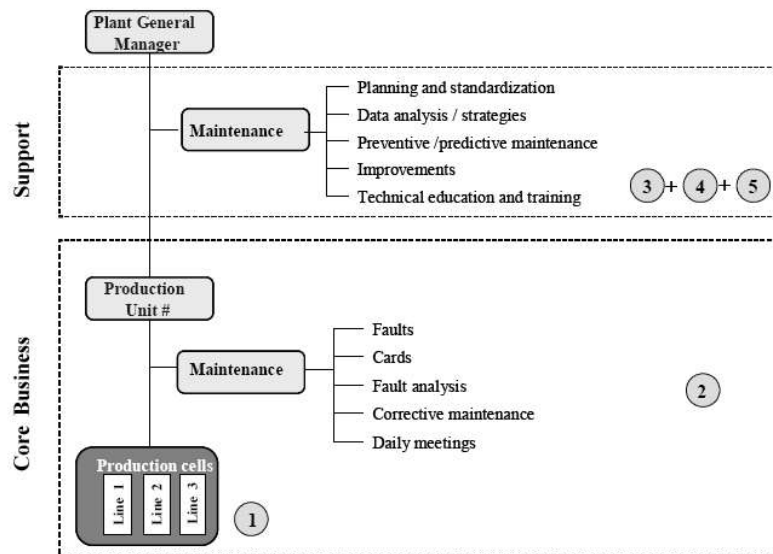


Figure 1.3: Example of a maintenance policy definition

The definition of the maintenance policy is important for an organization. The maintenance policy develops the maintenance concept within the organization and sets up solid foundations for the excellence in maintenance management.

1.2 Meantime Between Failure (MTBF), Meantime To Repair (MTTR) Maintenance Policy

Mean Time Between Failure (MTBF) is a reliability term used loosely throughout many industries and has become widely abused in some. Over the years the original meaning of this term has been altered which has led to confusion and cynicism. MTBF is largely based on assumptions and definition of failure and attention to these details are paramount to proper interpretation. Here we will explain the underlying complexities and misconceptions of MTBF and the methods available for estimating it.

1.2.1 Introduction

Mean Time Between Failure (MTBF) has been used for over 60 years as a basis for various decisions. Over the years more than 20 methods and procedures for lifecycle predictions have been developed. Therefore, it is no wonder that MTBF has been the daunting subject of endless debate. One area in particular where this is evident is in the design of mission critical facilities that house IT and telecommunications equipment.

1.2.2 What is a Failure? What are the Assumptions?

These questions should be asked immediately upon reviewing any MTBF value. Without the answers to these questions, the discussion holds little value. MTBF is often quoted without providing a definition of failure. This practice is not only misleading but completely useless. A similar practice would be to advertise

the fuel efficiency of an automobile as “miles per tank” without defining the capacity of the tank in liters or gallons. To address this ambiguity, one could argue there are two basic definitions of a failure:

- 1) The termination of the ability of the product as a whole to perform its required function.
- 2) The termination of the ability of any individual component to perform its required function but not the termination of the ability of the product as a whole to perform.²

The following two examples illustrate how a particular failure mode in a product may or may not be classified as a failure, depending on the definition chosen.

Example 1: If a redundant disk in a RAID array fails, the failure does not prevent the RAID array from performing its required function of supplying critical data at any time. However, the disk failure does prevent a component of the disk array from performing its required function of supplying storage capacity. Therefore, according to definition 1, this is not a failure, but according to definition 2, it is a failure.

Example 2: If the inverter of a UPS fails and the UPS switches to static bypass, the failure does not prevent the UPS from performing its required function which is supplying power to the critical load. However, the inverter failure does prevent a component of the UPS from performing its required function of supplying conditioned power. Similar to the previous example, this is only a failure by the second definition.

If there existed only two definitions, then defining a failure would seem rather simple. Unfortunately, when product reputation is on the line, the matter becomes almost as complicated as MTBF itself. In reality there are more than two definitions of failure, in fact they are infinite. Depending on the type of product, manufacturers may have numerous definitions of failure. Manufacturers that are quality driven track all modes of failure for the purpose of process control which, among other benefits, drives out product defects. Therefore, additional questions are needed to accurately define a failure.

Is customer misapplication considered a failure? There may have been human factors that designers overlooked, leading to the propensity for users to misapply the product. Are load drops caused by a vendor’s service technician counted as a failure?

Is it possible that the product design itself increases the failure probability of an already risky procedure? If an LED (Light Emitting Diode) on a computer were to fail is it considered a failure even though it hasn’t impacted the operation of the computer? Is the expected wear out of a consumable item such as a battery considered a failure if it failed prematurely? Are shipping damages considered failures? This could indicate a poor packaging design. Clearly, the importance of defining a failure should be evident and must be understood before attempting to interpret any MTBF value. Questions like those above provide the bedrock upon which reliability decisions can be made.

It is said that engineers are never wrong; they just make bad assumptions. The same can be said for those who estimate MTBF values. Assumptions are required to simplify the process of estimating MTBF. It would be nearly impossible to collect the data required to calculate an exact number. However, all assumptions must be realistic.

1.2.3 Reliability, Availability, MTBF, and MTTR Defined

MTBF impacts both reliability and availability. Before MTBF methods can be explained, it is important to have a solid foundation of these concepts. The difference between reliability and availability is often unknown or misunderstood. High availability and high reliability often go hand in hand, but they are not interchangeable terms.

Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE 90].

In other words, it is the likelihood that the system or component will succeed within its identified mission time, with no failures. An aircraft mission is the perfect example to illustrate this concept. When an aircraft takes off for its mission, there is one goal in mind: complete the flight, as intended, safely (with no catastrophic failures).

Availability, on the other hand, is the degree to which a system or component is operational and accessible when required for use [IEEE 90].

It can be viewed as the likelihood that the system or component is in a state to perform its required function under given conditions at a given instant in time. Availability is determined by a system's reliability, as well as its recovery time when a failure does occur. When systems have long continuous operating times (for example, a 10-year data center), failures are inevitable. Availability is often looked at because, when a failure does occur, the critical variable now becomes how quickly the system can be recovered. In the data center example, having a reliable system design is the most critical variable, but when a failure occurs, the most important consideration must be getting the IT equipment and business processes up and running as fast as possible to keep downtime to a minimum.

MTBF, or Mean Time Between Failure, is a basic measure of a system's reliability. It is typically represented in units of hours. The higher the MTBF number is, the higher the reliability of the product. Equation 1 illustrates this relationship.

$$\text{Reliability} = e^{\left(\frac{\text{Time}}{\text{MTBF}}\right)}$$

A common misconception about MTBF is that it is equivalent to the expected number of operating hours before a system fails, or the "service life". It is not uncommon, however, to see an MTBF number on the order of 1 million hours, and it would be unrealistic to think the system could actually operate continuously for over 100 years without a failure. The reason these numbers are often so high is because they are based on the rate of failure of the product while still in their "useful life" or "normal life", and it is assumed that they will continue to fail at this rate indefinitely. While in this phase of the products life, the product is experiencing its lowest (and constant) rate of failure. In reality, wear-out modes of the product would limit its life much earlier than its MTBF figure. Therefore, there should be no direct correlation made between the service life of a product and its failure rate or MTBF. It is quite feasible to have a product with extremely high reliability (MTBF) but a low expected service life. Take for example, a human being:

There are 500,000 25-year-old humans in the sample population.

Over the course of a year, data is collected on failures (deaths) for this population.

The operational life of the population is 500,000 x 1 year = 500,000 people years.

Throughout the year, 625 people failed (died).

The failure rate is 625 failures / 500,000 people years = 0.125% / year.

The MTBF is the inverse of failure rate or 1 / 0.00125 = 800 years.

So, even though 25-year-old humans have high MTBF values, their life expectancy (Service life) is much shorter and does not correlate.

The reality is that human beings do not exhibit constant failure rates. As people get older, more failures occur (they wear-out). Therefore, the only true way to compute an MTBF that would equate to service life would be to wait for the entire sample population of 25-year-old humans to reach their end-of-life. Then, the average of these life spans could be computed. Most would agree that this number would be on the order of 75-80 years.

So, what is the MTBF of 25-year-old humans, 80 or 800? It's both! But, how can the same population end up with two such drastically different MTBF values? It's all about assumptions!

If the MTBF of 80 years more accurately reflects the life of the product (humans in this case), is this the better method? Clearly, it's more intuitive. However, there are many variables that limit the practicality of using this method with commercial products such as UPS systems. The biggest limitation is time. In order to do this, the entire sample population would have to fail, and for many products this is on the order of 10- 15 years. In addition, even if it were sensible to wait this duration before calculating the MTBF, problems would be encountered in tracking products. For example, how would a manufacturer know if the products were still in service if they were taken out of service and never reported?

Lastly, even if all of the above were possible, technology is changing so fast, that by time the number was available, it would be useless. Who would want the MTBF value of a product that has been super ceded by several generations of technology updates?

MTTR, or Mean Time to Repair (or Recover), is the expected time to recover a system from a failure. This may include the time it takes to diagnose the problem, the time it takes to get a repair technician onsite, and the time it takes to physically repair the system. Similar to MTBF, MTTR is represented in units of hours. As Equation 2 shows, MTTR impacts availability and not reliability. The longer the MTTR, the worse off a system is. Simply put, if it takes longer to recover a system from a failure, the system is going to have a lower availability. The formula below illustrates how both MTBF and MTTR impact the overall availability of a system. As the MTBF goes up, availability goes up. As the MTTR goes up, availability goes down.

$$\text{Availability} = \frac{MTBF}{(MTBF + MTTR)}$$

For Equation 1 and Equation 2 above to be valid, a basic assumption must be made when analyzing the MTBF of a system. Unlike mechanical systems, most electronic systems don't have moving parts. As a result, it is generally accepted that electronic systems or components exhibit constant failure rates during the useful operating life. Figure 1.4, referred to as the failure rate "bathtub curve", and illustrates the origin of this constant failure rate assumption mentioned previously. The "normal operating period" or "useful life period" of this curve is the stage at which a product is in use in the field. This is where product quality has leveled off to a constant failure rate with respect to time. The sources of failures at this stage could include undetectable defects, low design safety factors, higher random stress than expected, human factors, and natural failures. Ample burn-in periods for components by the manufacturers, proper maintenance, and proactive replacement of worn parts should prevent the type of rapid decay curve shown in the "wear out period". The discussion above provides some background on the concepts and differences of reliability and availability, allowing for the proper interpretation of MTBF. The next section discusses the various MTBF prediction methods.

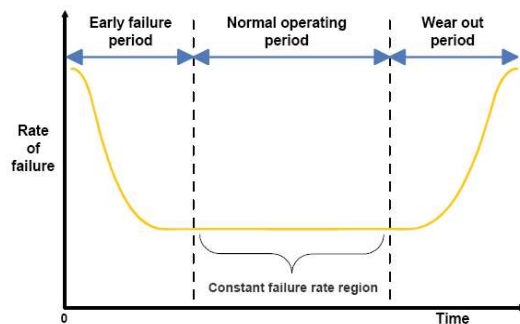


Figure 1.4: Bathtub curve to illustrate constant rate of failures

1.2.4 Methods of Predicting and Estimating MTBF

Oftentimes the terms “prediction” and “estimation” are used interchangeably, however this is not correct. Methods that *predict* MTBF, calculate a value based only on a system design, usually performed early in the product lifecycle. Prediction methods are useful when field data is scarce or non-existent as is the case of the Space Shuttle or new product designs. When sufficient field data exists, prediction methods should not be used. Rather, methods that *estimate* MTBF should be used because they represent actual measurements of failures. Methods that *estimate* MTBF, calculate a value based on an observed sample of similar systems, usually performed after a large population has been deployed in the field. MTBF estimation is by far the most widely used method of calculating MTBF, mainly because it is based on real products that are experiencing actual usage in the field.

All of these methods are statistical in nature, which means they provide only an approximation of the actual MTBF. No one method is standardized across an industry. It is, therefore, critical that the manufacturer understands and chooses the best method for the given application. The methods presented below, although not a complete list, illustrate the breadth of ways MTBF can be derived.

1.2.4.1 Reliability Prediction Methods

The earliest methods of reliability prediction came about in the 1940’s with a German scientist named Von Braun and a German mathematician named Eric Pieruschka. While trying to improve numerous reliability problems with the V-1 rocket, Pieruschka assisted Von Braun in modeling the reliability of his rocket thereby creating the first documented modern predictive reliability model. Subsequently, NASA along with the growth of the nuclear industry prompted additional maturation in the field of reliability analysis. Today, there are numerous methods for predicting MTBF.

MIL-HDBK 217: Published by the U.S. military in 1965, the Military Handbook 217 was created to provide a standard for estimating the reliability of electronic military equipment and systems so as to increase the reliability of the equipment being designed. It sets common ground for comparing the reliability of two or more similar designs. The Military Handbook 217 is also referred to as Mil Standard 217, or simply 217. There are two ways that reliability is predicted under 217: Parts Count Prediction and Parts Stress Analysis Prediction.

Parts Count Prediction is generally used to predict the reliability of a product early in the product development cycle to obtain a rough reliability estimate relative to the reliability goal or specification. A failure rate is calculated by literally counting similar components of a product (i.e. capacitors) and grouping

them into the various component types (i.e. film capacitor). The number of components in each group is then multiplied by a generic failure rate and quality factor found in 217. Lastly, the failure rates of all the different part groups are added together for the final failure rate. By definition, Parts Count assumes all components are in series and requires that failure rates for non-series components be calculated separately.

Parts Stress Analysis Prediction is usually used much later in the product development cycle, when the design of the actual circuits and hardware are nearing production. It is similar to Parts Count in the way the failure rates are summed together. However, with Parts Stress, the failure rate for each and every component is individually calculated based on the specific stress levels the component is subjected to (i.e. humidity, temperature, vibration, voltage,). In order to assign the proper stress levels to each component, a product design and its expected environment must be well documented and understood. The Parts Stress Method usually yields a lower failure rate than the Parts Count Method. Due to the level of analysis required, this method is extremely time consuming compared to other methods.

Today, 217 is rarely used. In 1996 the U.S. Army announced that the use of MIL-HDBK-217 should be discontinued because it “has been shown to be unreliable, and its use can lead to erroneous and misleading reliability predictions”. 217 has been cast off for many reasons, most of which have to do with the fact that component reliability has improved greatly over the years to the point where it is no longer the main driver in product failures. The failure rates given in 217 are more conservative (higher) than the electronic components available today. A thorough investigation of the failures in today’s electronic products would reveal that failures were most likely caused by misapplication (human error), process control or product design.

Telcordia: The Telcordia reliability prediction model evolved from the telecom industry and has made its way through a series of changes over the years. It was first developed by Bellcore Communications Research under the name Bell core as a means to estimate telecom equipment reliability. Although Bellcore was based on 217, its reliability models (equations) were changed in 1985 to reflect field experiences of their telecom equipment. The latest revision of Bellcore was TR-332 Issue 6, dated December 1997. SAIC subsequently bought Bellcore in 1997 and renamed it Telcordia. The latest revision of the Telcordia Prediction Model is SR-332 Issue 1, released in May 2001 and offers various calculation methods in addition to those of 217. Today, Telcordia continues to be applied as a product design tool within this industry.

HRD5 HRD 5: is the Handbook for Reliability Data for Electronic Components used in telecommunication systems. HRD5 was developed by British Telecom and is used mainly in the United Kingdom. It is similar to 217 but doesn’t cover as many environmental variables and provides a reliability prediction model that covers a wider array of electronic components including telecom.

RBD (Reliability Block Diagram): The Reliability Block Diagram or RBD is a representative drawing and a calculation tool that is used to model system availability and reliability. The structure of a reliability block diagram defines the logical interaction of failures within a system and not necessary their logical or physical connection together. Each block can represent an individual component, sub-system or other representative failure. The diagram can represent an entire system or any subset or combination of that system which requires failure, reliability or availability analysis. It also serves as an analysis tool to show how each element of a system functions, and how each element can affect the system operation as a whole.

Markov Model: Markov modeling provides the ability to analyze complex systems such as electrical architectures. Markov models are also known as state space diagrams or state graphs. State space is defined as a collection of all of the states a system can be in. Unlike block diagrams, state graphs provide a more accurate representation of a system. The use of state graphs accounts for component failure dependencies as well as various states that block diagrams cannot represent, such as the state of a UPS being on battery. In addition to MTBF, Markov models provide various other measures of a system, including availability, MTTR, the probability of being in a given state at a given time and many others.

FMEA/FMECA: FMEA (Failure Mode and Effects Analysis) is a process used for analyzing the failure modes of a product. This information is then used to determine the impact each failure would have on the product, thereby leading to an improved product design. The analysis can go a step further by assigning a severity level to each of the failure modes in which case it would be called a FMECA (Failure Mode, Effects and Criticality Analysis). FMEA uses a bottom to top approach. For instance, in the case of a UPS, the analysis starts with the circuit board level component and works its way up to the entire system. Apart from being used as a product design tool, it can be used to calculate the reliability of the overall system. Probability data needed for the calculations can be difficult to obtain for various pieces of equipment, especially if they have multiple states or modes of operation.

Fault Tree: Fault tree analysis is a technique that was developed by Bell Telephone Laboratories to perform safety assessments of the Minuteman Launch Control System. It was later applied to reliability analysis. Fault trees can help detail the path of events, both normal and fault related, that lead down to the component-level fault or undesired event that is being investigated (top to bottom approach). Reliability is calculated by converting a completed fault tree into an equivalent set of equations. This is done using the algebra of events, also referred to as Boolean algebra. Like FMEA, the probability data needed for the calculations can be difficult to obtain.

HALT: Highly Accelerated Life Testing (HALT) is a method used to increase the overall reliability of a product design. HALT is used to establish how long it takes to reach the literal breaking point of a product by subjecting it to carefully measured and controlled stresses such as temperature and vibration. A mathematical model is used to estimate the actual amount of time it would have taken the product to fail in the field. Although HALT can estimate MTBF, its main function is to improve product design reliability.

1.2.4.2 Reliability Estimation Methods

a) Similar Item Prediction Method

This method provides a quick means of estimating reliability based on historical reliability data of a similar item. The effectiveness of this method is mostly dependent on how similar the new equipment is to the existing equipment for which field data is available. Similarity should exist between manufacturing processes, operating environments, product functions and designs. For products that follow an evolutionary path, this prediction method is especially useful since it takes advantage of the past field experience. However, differences in new designs should be carefully investigated and accounted for in the final prediction.

b) Field Data Measurement Method

The field data measurement method is based on the actual field experience of products. This method is perhaps the most used method by manufacturers since it is an integral part of their quality control program. These programs are often referred to as Reliability Growth Management. By tracking the failure rate of

products in the field, a manufacturer can quickly identify and address problems thereby driving out product defects. Because it is based on real field failures, this method accounts for failure modes that prediction methods sometimes miss. The method consists of tracking a sample population of new products and gathering the failure data. Once the data is gathered, the failure rate and MTBF are calculated. The failure rate is the percentage of a population of units that are expected to “fail” in a calendar year. In addition to using this data for quality control, it also is used to provide customers and partners with information about their product reliability and quality processes. Given that this method is so widely used by manufacturers, it provides a common ground for comparing MTBF values. These comparisons allow users to evaluate relative reliability differences between products, which provide a tool in making specification or purchasing decisions. As in any comparison, it is imperative that critical variables be the same for all systems being compared. When this is not the case, wrong decisions are likely to be made which can result in a negative financial impact.

1.2.5 Conclusions

MTBF is a “buzz word” commonly used in the IT industry. Numbers are thrown around without an understanding of what they truly represent. While MTBF is an indication of reliability, it does not represent the expected service life of the product. Ultimately an MTBF value is meaningless if failure is undefined and assumptions are unrealistic or altogether missing.

1.3 Potential Problems of Preventive Maintenance and Corrective Maintenance

Maintenance is the last stage in the system development life cycle and, consequently, is affected by everything that happens in the previous stages. Errors made during the analysis and design stages can significantly impact maintenance. More specifically, maintenance relies on the documentation created during the analysis, design, testing, and implementation stages, and the system maintenance life cycle parallels the system development life cycle.

Maintenance begins when the system is released and continues for the life of the system. Over a period of years, it is not unusual for the cost of maintaining a system to significantly exceed the cost of developing it, so a primary objective is controlling maintenance costs. When the cost of maintaining and operating an obsolete or inefficient system exceeds the cost of replacing it, the system life cycle ends and a new life cycle begins.

The key to controlling maintenance costs is to design systems that are easy to change, so the link between development and maintenance is very strong. Using such tools as database management software, data normalization, program generators, fourth-generation languages, structured techniques, and object-oriented techniques forces the system designer to create independent modules, to separate the logic from the data, and to avoid programming “tricks.” Coding standards can help to enforce a consistent software style that helps to minimize the maintenance programmer’s learning time. Walkthroughs and inspections are excellent tools for enforcing standards and also help to familiarize personnel with the work of others.

Many of the analysis and design methodologies, tools, and techniques employed during system development can be applied to system maintenance, but there are significant differences between development and maintenance. System development (typically) focuses on new systems and considers such issues such as functional productivity, flexibility, integrity, and user friendliness. Maintenance, in contrast, is concerned with refining and improving the operational efficiency and effectiveness of an existing system and, consequently, is constrained by the existing system’s scope, boundaries, and platform,

and often must be performed in a short time frame and with a limited budget. Development is a one-time activity, so outsourcing is a viable option. Maintenance is a continuing activity more appropriately performed by in-house personnel. Finally, such resources as test data and test cases, program code, and documentation must be created by the system developers, but are available to the maintenance personnel.

Maintenance is divided into preventive and corrective categories to permit separation of skill levels and training in the design tradeoff analyses. Where preventive maintenance of the entire site can be performed by one trained individual, corrective maintenance involves several different skills, including electrical, electronics, engine mechanics, and at times, construction training. Corrective maintenance also requires spare parts, test equipment, and documentation.

Corrective maintenance may be required occasionally in order to rectify problems that have developed with system and sub-system performance. Some potential problems and their possible causes are:

Problems	Possible Causes
Battery electrolyte specific gravity low (lead-acid batteries)	• Corrosion or mechanical failure of connection. • Load current exceeds design limits. • Array output varies from design. • Blocking diodes malfunctioning. • High battery self-discharge
Array open circuit voltage to zero	• Module failure (single module array). • Defective or loose module contacts. • Array shaded. • Loose terminal block connections. • Defective blocking diode. • Battery cable loose or defective.
Array open circuit voltage low	• Array not properly oriented toward sun. • Array shaded. • Module failure. • Loose or defective cables.
Array short circuit current low	• Array shaded. oArray not oriented properly toward sun. • Module failure. • Defective or loose cables.
Excessive difference between array short circuit and battery charging current	• Corrosion at battery terminals. • Corrosion within junction box. • Defective module.

Maintenance actions are not complete until the repaired system has been tested and the effectiveness of the repair has been verified. This may be accomplished automatically by built-in fault-sensing circuitry, or it may require special provisions such as a light source to verify that a replaced circuit breaker will trip on over-load.

1.3.1 Relationship to Preventive Maintenance to Corrective Maintenance

When establishing an effective maintenance program, one must determine not only which preventive maintenance (PM) routines to accomplish, but how often they should be done. On the surface, the answer to this question would seem to be quite simple. Is it really?

One proven theory is that the PM to corrective maintenance (CM) work order ratio should be about 6 to 1. This theory assumes that PM inspections reveal some type of corrective work that should be completed on an asset on average every six times it is performed. The assumption is that, if the ratio is greater than 6:1, you are performing the PM too often, if the ratio is less than 6:1, you are not performing it often enough. (*The “6 to 1 Rule” was proven by John Day, Jr., manager of Engineering and Maintenance at Alumax of South Carolina, during the period when Alumax of South Carolina was certified as the first “World-Class” maintenance organization.*)

How effective?

Preventive maintenance is that activity performed in some routine or regularly scheduled fashion designed to keep equipment in an existing state, prevent deterioration or failure and identify work of a corrective nature to keep equipment from causing non-productive time in any capacity. This is the detection phase of the PM investment— *the conditions that we identify and correct prior to failure are the return for this investment.*

Each PM that we develop and implement in our Maintenance organization will require some definite period of time for a Maintenance or Operations person to accomplish. How many PMs, how often, can we accomplish with our workforce, reserving a certain percentage of each day for emergencies, unplanned work and planned corrective work? Should we attempt to implement some type of control over how often we conduct PMs? You may realize, as we continue on this path, that the frequency assigned to many PMs has as much to do with effective manpower utilization as it does with discovery of potential asset problems.

All too often, our organization sees Maintenance departments being overwhelmed by the number of PMs required on a daily and weekly basis. It's not that these clients have so many PMs that all cannot be completed. It's because so many PMs must be accomplished, that there is little time allowed for emergency work and NO time for either solid corrective work to prevent emergencies (which capitalizes on the payback for our investment) or to perform other unplanned work. We also must consider the potential to “PM the equipment to DEATH!” Such a scenario—*performing more PMs than we should*—creates more problems than it solves.

The obvious question is: “How effective is your PM program?” The short answer is: “If your PM program isn't finding problems, it isn't effective.”

How often?

How often should we perform any one PM procedure? It occurs to me that the frequency of performing a PM should be based on asset failure rate, or Mean Time Between Failure (MTBF) rather than on the NON-failure rate.

If I run a particular piece of equipment to failure, fix it, and then run it to failure again, what is the MTBF? Knowing that number, I should be able to calculate a realistic time frame where, if I perform some routine checks and preventive measures on this asset, I have the opportunity to identify potential problems and fix them, significantly extending the MTBF. Is this not our primary goal in maintenance? More does not necessarily equal better in preventive maintenance.

Let's consider the air compressor PM that is scheduled once every month. It requires that you observe the compressor in normal operation and look for any obvious signs of potential problems, such as air leaks, knocking in cylinder areas and improper operation of the automatic drain on the accumulator. It also requires that you shut down the compressor and check the condition of the air filter and oil level.

This air compressor PM is estimated to take one hour to complete. If you accomplish it as scheduled for six months and do not note any problems, or do not have to change the air filter or replenish the oil, what can you say about this PM?

First, you have used at least five man-hours of valuable craft labor performing a PM that you did not need to do after the first time, and the compressor was "off-line" for five hours during this PM activity. What other work could you have completed with those five man-hours?

Second, you can make a logical assumption that once per month is simply too often to schedule this PM. What to do? Should you change the PM frequency to "Annual" right away? If you did not generate a CM work order in six months, perhaps three or four months would be a good place to start. In this case, extending the length of time between PMs by a factor of 12 (to Annual) might result in missing an indicator of a potential problem and prove more costly in the long run.

Work into the appropriate frequency carefully. If by extending the periodicity of the compressor PM to three months, you identify corrective work every fifth or sixth time you accomplish the PM, you are in the right neighborhood for an effective PM program for the compressor. If not, keep adjusting the frequency until it gives you the outcome you need for an effective, proactive PM program. Good PM work order history will point exactly to the right frequency as you continue to experiment with periodicity for the PM.

How proactive?

When first implementing a proactive preventive maintenance program, you should establish frequency of PMs with a conservative view. Many sites implement their programs using manufacturer-suggested PM frequencies which, although usually on the conservative side, are a good starting point. Adjusting the frequency of PMs as good history develops is a benchmarking exercise driven by the desire to identify deficiencies and correct them before they become emergencies—*while at the same time striving for the best possible use of your available Maintenance resource hours.*

Consider the types of maintenance actually being performed at your facility. There is *preventive, predictive, condition monitoring, corrective and emergency work* in your basket, with every type of facility and industry expending certain percentages of Maintenance resources on each type.

- **Predictive maintenance (PdM)** technology uses some proven testing method, such as thermograph, tribology or ultrasonic's, to trend equipment performance and "predict" when certain preventive maintenance activity should be performed, thereby heading off a potential failure.
- **Condition monitoring** is the practice of closely monitoring equipment on a continuous basis to provide early detection of symptoms that could cause problems or failure, then performing some corrective actions to preclude the problem or failure.
- **Corrective maintenance (CM)** is the act of performing some repair or adjustment for a condition that was identified during the accomplishment of a PM or PdM evolution (and cannot reasonably be corrected within the allowed labor time for accomplishing the PM or PdM).

- *Emergency* work requires little definition; it is work performed in direct response to a failure that causes process downtime or imminent hazard to assets or personnel.

This is the appropriate time to note that, with the exception of emergency work, all of the other types of work are predicated on finding and fixing a problem before it becomes a “downtime” event. Perhaps we could categorize all maintenance except “emergency” under the umbrella of “*preemptive*” maintenance.”

How close are you?

We have taken a “long, strange trip” around the Maintenance horn. Are we any closer to determining the proper ratio of PMs to CMs in a proactive Maintenance organization?

Two true statements that can be found in nearly every maintenance-related publication on the market are that:

1. You must evaluate the ratio of preventive maintenance actions to corrective maintenance actions to determine the effectiveness of your PM program.
2. In a proactive Maintenance environment, PM activities should account for approximately 30% of total Maintenance resource time.

The real answer could be that the ratio of PM to CM is dependent on several variables, including:

1. **Asset criticality**—If the asset fails, what is the impact on production or safety.
2. **Asset age**—Equipment histories will prove that most failures occur during infancy (newly installed or overhauled) and old-age (self-explanatory).
3. **Asset history**—How many times has the asset failed in the past (MTBF)? Answer the what, how, why, when and how much.
4. **Asset technology**—Do you need to PM a state-of-the-art digital measuring device as often as the analog one installed next to it?
5. **Trust**—How much do you trust the asset to perform as designed when scheduled to run?
6. What percentage of your total Maintenance resources is expended on PMs? On CMs? On emergencies?
7. Can you change PM frequencies within the guidelines you have established for yourself (ref: ISO, CFR, MILSTD, etc.)?

1.4 Circuit Tracing techniques

Circuit Tracing is the copper lines (sometimes aluminum) on a printed circuit board (PCB) that allow electricity to flow between electronic components. A wire trace is a conductive line (pathway) in a printed circuit board that allows electricity to flow from one electronic device to another. In a chip, wire traces are typically called “tracks.”

The PCB is a Component of the Op Amp Design

Op amp circuitry is analog circuitry, and is very different from digital circuitry. It must be partitioned in its own section of the board, using special layout techniques.

Printed circuit board effects become most apparent in high-speed analog circuits, but common mistakes described in this chapter can even affect the performance of audio circuits. The purpose of this

section is to discuss some of the more common mistakes made by designers and how they degrade performance, and provide simple fixes to avoid the problems.

In all but very rare cases, the PCB layout for analog circuitry must be designed such that the effect of the PCB is transparent to the circuit. Any effect caused by the PCB itself should be minimized, so that the operation of the analog circuitry in production will be the same as the performance of the design and prototype.

Prototype!

Normal design cycles, particularly of large digital boards, dictate layout of the PCB as soon as possible. The digital circuitry has been simulated, but in most cases, the production PCB itself is the prototype, and may even be sold to a customer. Digital designers can correct small mistakes by implementing *cuts and jumpers*, reprogramming gate arrays or flash memories, and go on to the next project. This is not the case with analog circuitry. Some of the common design mistakes discussed in this section cannot be corrected by the cut and jumper method. They can and will render the entire PCB unusable.

Noise Sources

Noise is the primary limitation on analog circuitry performance. Other types of noise include:

- **Conducted Emissions** — noise that the analog circuitry generates through its connections to other circuits. This is usually negligible in analog circuitry, unless it is high power (such as an audio amplifier that draws heavy currents from its power supply).
- **Radiated Emissions** — noise that the analog circuitry generates, or transmits, through the air. This is also usually negligible in analog circuitry, unless it is high frequency such as video.
- **Conducted Susceptibility** — noise from external circuitry that is conducted into the analog circuit through its connections to other circuits. Analog circuitry must be connected to the “outside world” by at least a ground connection, a power connection, an input, and an output. Noise can be conducted into the circuit through all of these paths, as well as any others that are present.
- **Radiated Susceptibility** — noise that is received through the air (or transmitted into the analog circuitry) from external sources. Analog circuitry, in many cases, resides on a PCB that may have high-speed digital logic including DSP chips. High-speed clocks and switching digital signals create considerable radio frequency interference (RFI). Other sources of radiated noise are endless: the switching power supply in a digital system, cellular telephones, broadcast radio and TV, fluorescent lighting, nearby PCs, lightning in thunderstorms, and so on. Even if the analog circuitry is primarily audio in frequency, RFI may produce noticeable noise in the output.

PCB Mechanical Construction

It is important to choose a PCB with the right mechanical characteristics for the application.

Materials — Choosing the Right One for the Application

PC Board materials are available in various grades, as defined by the National Electrical Manufacturers Association (NEMA). It would be very convenient for designers if this organization was closely allied with the electronics industry — controlling parameters such as resistivity and dielectric constant of the material. Unfortunately, that is not the case. NEMA is an electrical safety organization, and the different PCB grades primarily describe the flammability, high temperature stability, and moisture absorption of the board. Therefore, specifying a given NEMA grade does not guarantee electrical parameters of the

material. If this becomes critical for an application, consult the manufacturer of the raw board stock. Laminated materials are designated with *FR* (flame resistant) and *G* grades. FR-1 is the least flame resistant, and FR-5 is the most. G10 and G11 have special characteristics as described in Table below.

GRADE DESIGNATION	MATERIAL/COMMENTS
FR-1	Paper/phenolic: room temperature punchable, poor moisture resistance.
FR-2	Paper/phenolic: suitable for single-sided PCB consumer equipment, good moisture resistance.
FR-3	Paper/epoxy: designed for balance of good mechanical and electrical characteristics.
FR-4	Glass cloth/epoxy: excellent mechanical and electrical properties.
FR-5	Glass cloth/epoxy: high strength at elevated temperatures, self-extinguishing.
G10	Glass cloth/epoxy: high insulation resistance, highest bond strength of glass laminates, high humidity resistance.
G11	Glass cloth/epoxy: high flexural strength retention at high temperature, extreme resistance to solvents.

PCB Materials

After the board substrate material has been selected, the next decision is how thick to make the copper foil laminated to it. For most applications, 1-ounce copper is sufficient. If the circuit consumes a lot of power, 2-ounce may be better. Avoid 1/2-ounce copper, because it tends to break between the trace and the pad.

How Many Layers are the Best?

Depending on the complexity of the overall circuitry being designed, a designer must decide how many layers the PCB should be.

Single-Sided

Very simple consumer electronics are sometimes fabricated on single-sided PCBs, keeping the raw board material inexpensive (FR-1 or FR-2) with thin copper cladding. These designs frequently include many jumper wires, simulating the circuit routing on a double-sided board. This technique is only recommended for low-frequency circuitry. For reasons described below, this type of design is extremely susceptible to radiated noise. It is harder to design a board of this type, because of the many things can go wrong. Many complex designs have been successfully implemented with this technique, but they require a lot of forethought. An example is a television set that puts all of the analog circuitry on a single-sided board at the bottom of the case, and uses the metalized CRT itself to shield the board from a separate digital tuning board near the top of the set. Be prepared to get creative if the design demands high volume, low cost PCBs.

If a single-sided PCB is a requirement, remember the trace resistance! The op amp is not a 3-terminal device (inverting input, non-inverting input, and output). It is a 7-terminal device as shown in Figure below.

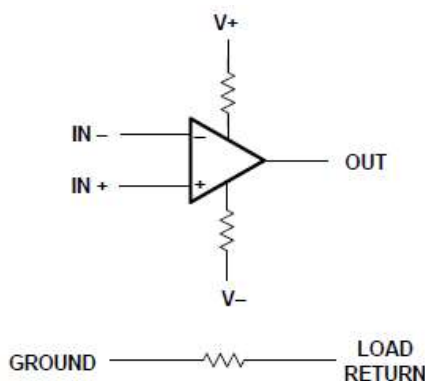


Fig 1.5

Op Amp terminal model

Resistance in the power leads of the device must be taken into account, as well as resistance between the return for the inputs and the load. Both the input and load must return somewhere. If these are at different potentials due to trace resistance, there can be problems.

Double-Sided

The next level of complexity is double-sided. Although there are some double-sided FR-2 boards, they are more commonly fabricated with FR-4 material. The increased strength of FR-4 material supports vias better. Double-sided boards are easier to route because there are two layers of foil, and it is possible to route signals by crossing traces on different layers. Crossing traces, however, is not recommended for analog circuitry. Wherever possible, the bottom layer should be devoted to a ground plane, and all other signals routed on the top layer. A ground plane provides several benefits:

- Ground is frequently the most common connection in the circuit. Having it continuous on the bottom layer usually makes the most sense for circuit routing.
- It increases mechanical strength of the board.
- It lowers the impedance of all ground connections in the circuit, which reduces undesirable conducted noise.
- It adds a distributed capacitance to every net in the circuit — helping to suppress radiated noise.
- It acts a shield to radiated noise coming from underneath the board.

Multi-Layer

Double-sided boards, in spite of their benefits, are not the best method of construction, especially for sensitive or high-speed designs. The most common board thickness is 1.5 mm. This separation is too great for full realization of some of the benefits listed above. Distributed capacitance, for example, is very low due to the separation. Critical designs call for multi-layer boards. Some of the reasons are obvious:

- Better routing for power as well as ground connections. If the power is also on a plane, it is available to all points in the circuit simply by adding vias.
- Other layers are available for signal routing, making routing easier.

- There will be distributed capacitance between the power and ground planes, reducing high frequency noise. There are other reasons for multi-layer boards, however, that may not be obvious or intuitive.
- Better EMI/RFI rejection. There is due to the *image plane effect*, which has been known since the time of Marconi. When a conductor is placed close to a parallel conductive surface, most of the high frequency currents will return directly under the conductor, flowing in the opposite direction. This mirror image of the conductor within the plane creates a transmission line. Since currents are equal and opposite in the transmission line, it is relatively immune to radiated noise. It also couples the signal very efficiently. The image plane effect works equally well with ground and power planes, but they must be continuous. Any gap or discontinuity causes the beneficial effects to quickly vanish. There is more on this in the following paragraphs.
- Reduced overall project cost for small production runs. Although multi-layer boards are more expensive to manufacture, EMI/RFI requirements from the FCC or other agencies may require expensive testing of the design. If there are problems, it can force a complete redesign of the PCB, leading to additional rounds of testing. A multi-layer PCB can have as much as 20-dB better EMI/RFI performance over a 2-layer PCB. If production volumes are going to be small, it makes sense to make a better PCB to begin with, than try to cut costs and take the risk of failing \$25,000 to \$50,000 tests.

Board Stack-Up — The Order of Layers

There has been a lot of confusion in the past over what is the optimum order for PCB layers. Take, for example, a 4-layer board consisting of two signal layers, a power plane, and a ground plane. Is it better to route the signal traces between the layers, thus providing shielding for the signal traces – or is it better to make the ground and power planes the two inner planes?

In considering this question, it is important to remember that no matter what is decided, there will still be signals exposed on one or both of the top and bottom planes. The leads of the op amp PCB package, and the traces on the board leading to nearby passive components and feed-throughs will be exposed. Therefore, any shielding effects are compromised. It is far better to take advantage of the distributed capacitance between the power and ground plane by making them internal.

Another advantage of placing the planes internally is that the signal traces are available for probing and modification on the top and bottom layers. Anyone who has had to change connections on buried traces will appreciate this feature.

For more than four layers, it is a general rule to shield higher speed signals between the ground and power planes, and route slower signals on the outer layers.

Grounding

Good grounding is a system-level design consideration. It should be planned into the product from the first conceptual design reviews.

The Frequency Characteristics of Passive Components

Choosing the right passive components for an analog design is important. In most cases, a *right* passive component will fit on the same pads as a *wrong* passive component, but not always. Start the design process by carefully considering the high frequency characteristics of passive components, and putting the correct part outline on the board from the start.

Most designers are totally ignorant of the frequency limitations of the passive components they use in analog circuitry. Passive components have limited frequency ranges, and operation of the part outside of that range can have some much unexpected results. One might think that this discussion only applies to high-speed analog circuits. But high frequencies that are radiated or conducted into a low-speed circuit will affect passive components as well. For example: a simple op amp low-pass filter may well turn into a high-pass filter at RF frequencies.

Resistors

High-frequency performance of resistors is approximated by the schematic shown in Figure below:

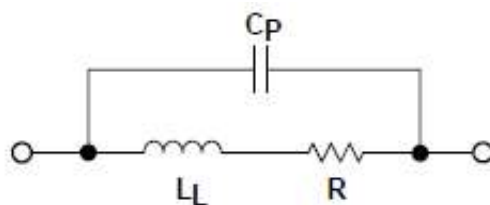


Fig 1.6

Resistor high frequency performance

Resistors are typically one of three types: wire-wound, carbon composition, and film. It does not take a lot of imagination to understand how wire-wound resistors can become inductive because they are coils of resistive wire. Most designers are not aware of the internal construction of film resistors, which are also coils of thin metallic film. Therefore, film resistors are also inductive at high frequencies. The inductance of film resistors is lower, however, and values under 2 k Ω are usually suitable for high frequency work.

The end caps of resistors are parallel, and there will be an associated capacitance. Usually, the resistance will make the parasitic capacitor so “leaky” that the capacitance does not matter. For very high resistances, the capacitance will appear in parallel with the resistance, lowering its impedance at high frequencies.

Capacitors

High-frequency performance of capacitors is approximated by the schematic shown in

Figure below:

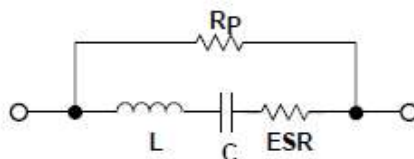


Fig 1.7

Capacitor high-frequency performance

Capacitors are used in analog circuitry for power supply decoupling and as filter components. For an ideal capacitor, reactance decreases by the formula:

$$X_C = \frac{1}{(2\pi fC)}$$

Where:

X_C capacitive reactance in Ohms

f frequency in Hz

C capacitance in microfarads

Therefore, a 10- μ F electrolytic capacitor has a reactance of 1.6 Ω at 10 kHz, and 160- $\mu\Omega$ at 100 MHz.

Inductors

High frequency performance of inductors is approximated by the schematic shown in Figure below:

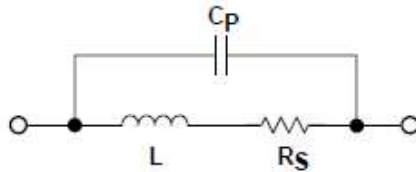


Fig 1.8

Inductor High-Frequency Performance

Inductive reactance is described by the formula:

$$X_L = 2\pi fL$$

Where:

X_L inductive reactance in Ohms

f frequency in Hz

L inductance in Henrys

Therefore, a 10-mH inductor has a reactance of 628 Ω at 10 kHz, which increases to 6.28 M Ω at 100 MHz.

Unexpected PCB Passive Components

In addition to the obvious passive components above, the PCB itself has characteristics that form components every bit as real as those discussed previously — just not as obvious.

PCB Trace Characteristics

The layout pattern on a PCB can make it susceptible to radiated noise. A good layout is one that minimizes the susceptibility of analog circuitry to as many radiated noise sources as possible. Unfortunately, there is always a level of RF energy that will be able to upset the normal operation of the circuit. If good design techniques are followed, that level will be one that the circuit never encounters in normal operation.

Trace Antennas

A board is susceptible because the pattern of traces and component leads form antennas. Antenna theory is a complex subject, well beyond the scope of this book. Nevertheless, a few basics are presented

here. One basic type of antenna is the whip, or straight conductor. This antenna works because a straight conductor has parasitic inductance, and therefore can concentrate flux from external sources. The impedance of any straight conductor has a resistive and an inductive component:

$$Z = R + j\omega L \quad (17-3)$$

For dc and low frequencies, resistance is the major factor. As the frequency increases, however, the inductance becomes more important. Somewhere in the range of 1 kHz to 10 kHz, the inductive reactance exceeds the resistance, so the conductor is no longer a low resistance connection, but rather an inductor. The formula for the inductance of a PCB trace is:

$$L(\mu H) = 0.002X \left[\ln \left(\frac{2X}{W+H} \right) + 0.2235 \left(\frac{W+H}{X} \right) + 0.5 \right] \quad (17-4)$$

Where:

X length of the trace

W width of the trace

H thickness of the trace

The inductance is relatively unaffected by the diameter, since it varies as the logarithm of the circumference. Common wires and PCB traces vary between 6 nH and 12 nH per centimeter.

For example, a 10 cm PCB trace has a resistance of 57 mΩ and an inductance of 8 nH per cm. At 100 kHz, the inductive reactance reaches 50 mΩ. At frequencies above 100 kHz, the trace is inductive — not resistive.

A rule of thumb for whip antennas is that they begin to couple significant energy at about 1/20 of the wavelength of the received signal, peaking at $\frac{1}{10}$ the wavelength. Therefore, the 10-cm conductor of the previous paragraph will begin to be a fairly good antenna at frequencies above 150 MHz. Remember that although the clock generator on a digital PCB may not be operating at a frequency as high as 150 MHz, it approximates a square wave. Square waves will have harmonics throughout the frequency range where PCB conductors become efficient antennas. If through-hole components are mounted in a way that leaves significant lead length, those component leads also become antennas, particularly if they are bent.

Another major type of antenna is the loop. The inductance of a straight conductor is dramatically increased by bending it into partial or complete loops. Increased inductance lowers the frequency at which the conductor couples radiated signals into the circuit. Without realizing it, most digital designers are well versed in loop antenna theory. They know not to make loops in critical signal pathways. Some designers, however, that would never think of making a loop with a high speed clock or reset signal will turn right around and create a loop by the technique they use for layout of the analog section of the board. Loop antennas constructed as loops of wire are easy to visualize. What is not as obvious is that slot antennas are just as efficient. Consider the three cases shown in Figure below:

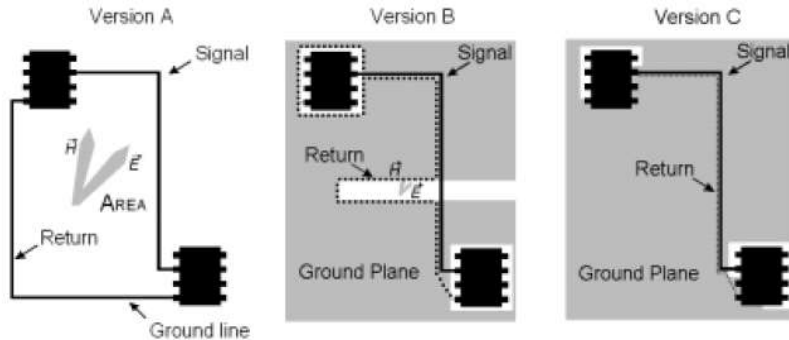


Fig 1.9

Loop and Slot Antenna Board Trace Layouts

Version **A** is a poor design. It does not use an analog ground plane at all. A loop is formed by the ground and signal traces. An electric field E and perpendicular magnetic field H are created, and form the basis of a loop antenna. A rule of thumb for loop antennas is that the length of each leg is equal to half the most efficiently received wavelength. Remember, however, that even at $1/20$ of the wavelength, the loop will still be a fairly efficient antenna.

Version **B** is a better design, but there is intrusion into the ground plane, presumably to make room for a signal trace. A much smaller slot antenna is formed by the difference in pathways between signal and return. A second loop is created by the cutout for the IC.

Version **C** is the best design. Signal and return are coincident with each other, eliminating loop antenna effects completely. Note that there is still a cutout for the IC, but it is located away from the return path for the signal.

Trace Reflections

Reflections and matching are closely related to loop antenna theory, but different enough to warrant their own discussion. When a PCB trace turns a corner at a 90° angle, a reflection can occur. This is primarily due to the change of width of the trace. At the apex of the turn, the trace width is increased to 1.414 times its width. This upsets the transmission line characteristics, especially the distributed capacitance and self-inductance of the trace — resulting in the reflection. It is a given that not all PCB traces can be straight, and so they will have to turn corners.

Most CAD systems give some rounding effect on the trace. Sharp 90° corners in traces are a relic of the *tape up* days of PCB layout. The rounding effects of CAD programs, however, still do not necessarily maintain constant width as the trace rounds the corner. Figure below shows progressively better techniques of rounding corners. Only the last example maintains constant trace width and minimizes reflections. Most CAD programs now support these methods, but they can entail a little more work to master.

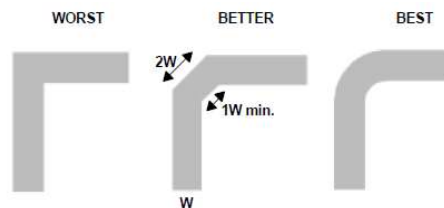


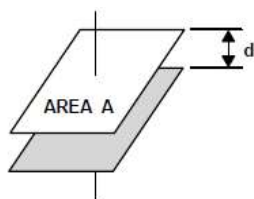
Fig 1.10

PCB Trace Corners

A suggestion for the advanced PCB layout engineer: leave rounding to the last step before tear-dropping and flood-filling. Otherwise, the CAD program will slow down doing numerical calculations as the traces are moved around during routing.

Trace-to-Plane Capacitors

PCB traces, being composed of foil, form capacitance with other traces that they cross on other layers. For two traces crossing each other on adjacent planes, this is seldom a problem. Coincident traces (those that occupy the same routing on different layers), form a long, skinny capacitor. The formula for capacitance is shown in Figure below:



$$C = 0.0085 \times \epsilon_R \times \frac{A}{d}$$

where:

C = capacitance (pF)

ϵ_R = dielectric constant

A = area of plate (mm^2)

d = separation of plates (mm)

Fig 1.11

PCB Trace-to-Plane Capacitance Formula

Trace-to-Trace Capacitors and Inductors

PCB traces are not infinitely thin. They have some finite thickness, as defined by the *ounce* parameter of the copper clad foil. The higher the number of ounces, the thicker the copper will be. If two traces run side-by-side, then there will be capacitive and inductive coupling between them (Figure below). The formulas for these parasitic effects can be found in transmission line and/or micro-strip references, but are too complex for inclusion here.

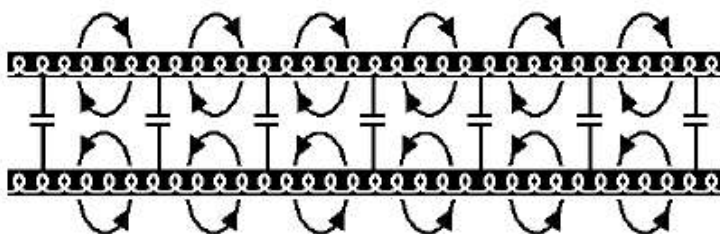


Fig 1.12

Coupling Between Parallel Signal Traces

Signal lines should not be routed parallel to each other, unless transmission line or micro-strip effects are desired. Otherwise, a gap of at least three times the signal trace width should be maintained.

Capacitance between traces in an analog design can become a problem if fixed resistors in the design are large (several MΩ). Capacitance between the inverting and non-inverting inputs of an op amp could easily cause oscillation.

Inductive Vias

Whenever routing constraints force a *via* (connection between layers of a PCB, Figure below), a parasitic inductor is also formed. At a given diameter (d) the approximate inductance (L) of an via at a height of (h) may be calculated as follows:

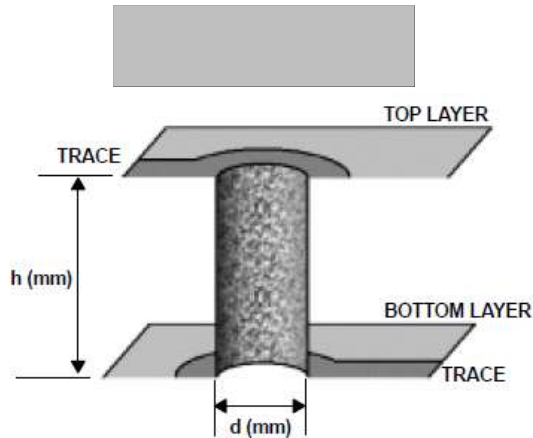


Fig 1.13

Via Inductance Measurements

For example, a 0.4-mm diameter via through a 1.5-mm thick PCB has an inductance of 1.1 nH.

Keep in mind that inductive vias combined with parasitic capacitance can form resonant circuits. The self-inductance of a via is small enough that these resonances are in the GHz range, but inductors add in series, lowering the resonant frequency. Do not put several vias on a critical trace of a high-speed analog circuit! Another concern is that the vias put holes in ground planes, potentially creating ground loops. They should be avoided — the best analog layout is one that routes all signal traces on the top layer of the PCB.

Through-Hole Considerations

The older technology for op amps and other components is through-hole. Components are constructed with leads that insert through holes in the board — hence the name. Through-hole components, due to their size, are more suited to applications where space is not an issue. The components themselves are frequently lower in cost, but the PCB is more expensive due to the fact that the PCB fabrication house has to drill holes for component leads. PCBs are primarily a mechanical fabrication — the number of holes and number of different drills have a big impact on the price.

The leads on a through-hole op amp are arranged on a 0.1-inch grid. Many PCB layout people like to maintain the 0.1-inch grid for the rest of the components as well. Resistors and other passive components can even be purchased with leads pre-bent to land on a 0.1 inch grid. Some electrolytic capacitors have leads that are on a 0.025-inch grid.

These component sizes may force a lot of wasted area on the PCB. Components that ideally should be placed close to the op amp itself may be forced several tenths of an inch away, due to intervening components. Therefore, through hole circuitry is not recommended for high speed analog circuitry, or for analog circuitry in proximity to high speed digital.

Some designers attempt to overcome the long trace length caused by resistors by placing the resistors on the board vertically, one lead of the resistor bent close to the body of the part. This is common in older consumer electronics. This allows for denser placement of parts, and may help some with trace length — but each resistor exposes almost 1 cm of one component lead to radiated signals, and lead self-inductance.

An advantage of the through-hole approach of PCB layout is that the through-holes themselves can serve as feed-throughs, reducing the number of vias in complex circuits.

Surface Mount

Surface-mount circuitry does not require a hole for each component lead. Automated testing, however, may require vias on every node. The holes were never an issue with through-hole circuitry, because every component lead made a hole in the board. The PCB layout designer, who is used to designing a board with a minimum number of vias, now has to put a via on EVERY node of the circuit. This can make a Swiss cheese out of a nice continuous ground plane — negating many of the advantages it provides.

Fortunately, there is a close variation of the “via on every node” requirement. This requirement can often be met by putting a test pad on every node. The automated test station can then access the analog circuitry from the top of the board. A *clamshell* test fixture is significantly more expensive than one that accesses only one side of the board. The extra cost can be justified if there is documentation that circuit performance will be unacceptable with vias.

Signal connections to ground or the power supply may have to be made through a small fixed resistor instead, so the automated equipment can access that pin of the IC and test its function.

1.5 Concept of Shielding, Grounding and Power Supply requirements

To the instrument engineer, grounding and shielding probably do not generate the interest enjoyed by more academic and less practical pursuits. It would seem preferable if grounding and shielding could be reduced to a few simple rules. Certainly, continually revisiting an issue on which safety is so dependent would have its drawbacks. In practice, an engineer with a few years of experience is likely to run across not only a good deal of variability in grounding and shielding application, but also a good deal of confusion. In fact, all too often it is simply accepted that there is a trade-off between safety and noise reduction. Getting it right seems more of an art than a science. However, when one starts with the laws of physics and tacks on knowledge of codes and standards, one will be pleasantly surprised to find complete compatibility between what sometimes seem conflicting goals.

1.5.1 Power Grounding Basics

Power Grounding practices for electrical safety, static electricity management, shielding, and noise reduction are inter-related and do not conflict with one another. Grounding practices for safety and signal integrity purposes are rooted firmly in the fields of electro-statistics, magnetism, and radiation. Grounding has many purposes including:

- *Providing a low impedance path for fault currents back to over current protection devices.* When a fault to ground occurs, it is desirable to interrupt and isolate the offending circuit and equipment. An over-current device needs to see a much larger current than it does during normal operation to perform this function. When all equipment is low impedance bonded back to the grounding electrode via the equipment grounding conductor, current due to line faults to equipment or ground will cause momentarily high currents back at the over-current protection device.

- *Reducing shock hazards to personnel.* When a circuit faults to conductive equipment, the equipment becomes part of the circuit. If the equipment is grounded, the current flows at “zero” voltage and is therefore not a shock hazard. When all equipment is low impedance bonded back to the over-current device, such faults should not persist and should be immediately obvious.
- *Providing fire protection.* If a low impedance path back to circuit over-current protection is provided, fault currents will not radiate heat energy and can readily be isolated. Because 100 A flowing in 0.1 W produces 1 kW of heat, if the over-current device is designed to trip at 120 A, current will continue flowing until the conductor melts, possibly causing a fire.

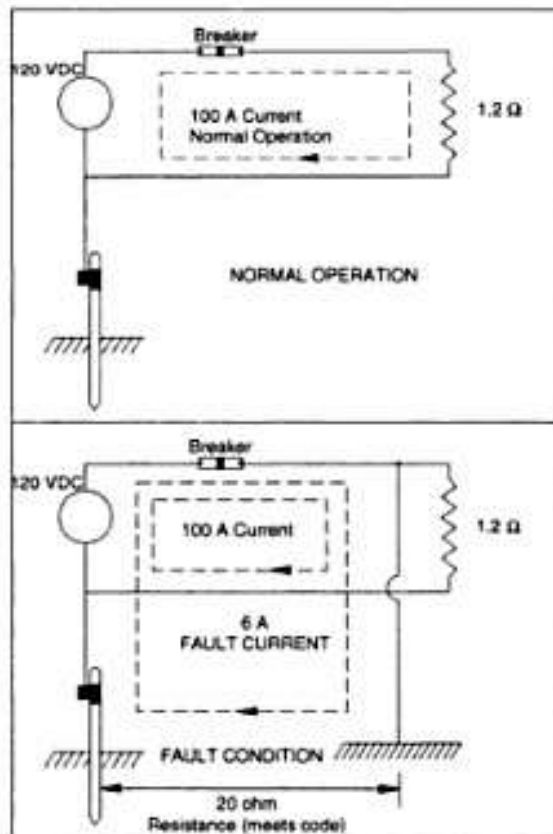


Fig 1.14

1.5.2 Grounding, Bonding and Overload Protection

One of the fundamental protections of safety grounding and bonding is to provide low impedance current paths when normal ungrounded conductors fault to ground. If a fault current travels through high impedance, the over-load protection device cannot distinguish the fault condition from normal operation. Furthermore,

the impedance can radiate heat. When low impedance paths are provided via grounding and bonding, sudden high currents will trip the over-load device causing the faulted circuit to be quickly isolated by the over-current device (breaker). For example, from the relationship $V = IR$, resistance in a 120-V, 100-A load is 1.2W. Were the ungrounded conductors in this circuit to fault, the fault circuit would require much lower resistance for the current to rise much above 100 A and trip the breaker. In fact, 10 to 15 times more current is required for quick action. This suggests a need for less than 0.12-W resistance in the grounding and bonding system. Figure 1.1 demonstrated this principle schematically. Here the ground resistance meets code requirements of less than 25W. The circuit breaker only senses a 6-A increase in current.

NEC code strictly prohibits relying on earth as an equipment grounding conductor. This is because earth's resistance and voltage can vary not only from location to location and depending on depth of an electrode, but also from time to time in the same location.

1.5.2.1 Grounding Electrode Resistance

Much research has focused on identifying techniques for achieving low resistance grounding rods. Many problems encountered with communications reliability can be traced to high grounding electrode resistance. The standard method of measuring soil resistivity is known as the four-probe Werner method.

Lightening, in particular, places stringent requirements on grounding electrode resistance. Radio tower and telecommunications hub installations are particularly affected. Often expensive boards and the like can be destroyed leading to long downtimes. The lower the resistance of the electrode system (and the better the bonding), the more likely all of the lightening energy will be dissipated in the ground. Lightening energy has been shown to dissipate horizontally across the ground. Thus horizontal electrodes have been shown to be preferable to vertical ones. In the past, salt solutions were injected around grounding rods to decrease electrode resistance. Maintenance and environmental issues have led to a decrease in popularity of this technique. More and more, conductive concrete backfill is used effectively to increase electrode surface area, soil contact, and grounding system capacitance. It has also been shown that long, deep electrodes can greatly lower resistance. Deep electrodes also offer a stabler ground over time.

1.5.2.2 Power Grounding Definitions

Accepting that the NFPA NEC provides the most in-depth, authoritative, and widely accepted set of guidelines on grounding, it is important to understand the specific terms. Some of these terms include:

- **Bonding (Bonded):** Bonding is the practice of providing electrical continuity among all conducting equipment in a facility. It has implications for over-current protection as well as static electricity management.
- **Bonding Jumpers:** The conductors used to bond equipment together and to certain conductors.
- **Branch Circuits:** Circuits after a final over-current protection device.
- **Circuit Breaker:** Device used to open circuits manually or automatically based on a maximum current trip point.
- **Effectively Grounded:** Intentionally connected to earth through a low impedance conductor of sufficient capacity. Also called *solidly grounded*.
- **Equipment:** General term for fittings, devices, appliances, fixtures and apparatus used in electrical installations.

- **Equipment Grounding Conductor:** The conductor used to connect non-current-carrying conductive equipment to be grounded conductor, grounding electrode, or both at the service equipment and at the source of a separately derived system if desired.
- **Ground:** An intentional or accidental connection between electrical circuits or equipment and earth. In marine and aviation appliances ground refers to a substitute for earth.
- **Grounded:** Connected to earth or its substitute.
- **Grounded Conductor:** A circuit conductor that is intentionally grounded. Also called a neutral in AC applications.
- **Grounding Conductor:** A conductor used to connect equipment to the grounded conductor and hence the grounding electrode.
- **Grounding Electrode:** The primary ground point, located at the service entrance, in a facility. Although there can only be one grounding electrode in a facility, local grounding electrodes are permitted.
- **Grounding Electrode Conductor:** Conductor used to connect grounding electrode to equipment grounding conductor and the grounded conductor.
- **Listed:** Certified for its purpose by an organization whose authority is accepted by enforcement bodies with appropriate jurisdiction.
- **Plenum:** Air duct.
- **Raceway:** General term for enclosed equipment that houses wires, cables or bus bars.
- **Separately Derived System:** A wiring system whose power is derived from a battery, generator or transformer not directly connected electrically to supply conductors originating in another system. In instrumentation, a UPS (Uninterruptible Power Supply) or an isolation transformer usually demarcates a separately derived system.
- **Service:** The conductors and equipment for delivering electric energy from the serving utility to the wiring system of a facility.

1.5.2.3 Separately derived Instrumentation Power System

A key safety function of power grounding is to provide a low impedance path for returning faults back to over-current protection devices. Fortunately, this safety function can be maintained while still providing common mode noise attenuation. To provide isolation and common mode noise reduction, instrumentation power networks warrant use of an isolation transformer. NEC defines such a system as “separately derived.”

Separately derived systems derived from transformers require that the primary power source be properly grounded at the service entrance. The secondary of the transformer must be regrounded as well. Grounding of the secondary of a transformer always involves a three step process. First, one sizes the bonding jumper between the center tap or neutral of the secondary and the transformer case. Next, one sizes the grounding electrode conductor using NEC Table 250-66. Finally, one selects the grounding electrode.

NEC requires that a single grounding electrode have less than 25W of resistance or that two be used (250-66). Instrumentation systems have more stringent requirements. For example, an intrinsic safety ground must have 1W or less resistance to ground. The IEEE Green Book recommends ground resistances of 2 to 5W for industrial systems.

Equipment grounding conductor and equipment bonding concepts demonstrated in the example all still hold. Figure 1.15 demonstrates a preferred method of grounding an instrumentation power system consisting of the following:

- 1) Single UPS module.
- 2) Non-isolated UPS bypass.
- 3) Distribution panel with Delta-Wye isolation transformer.

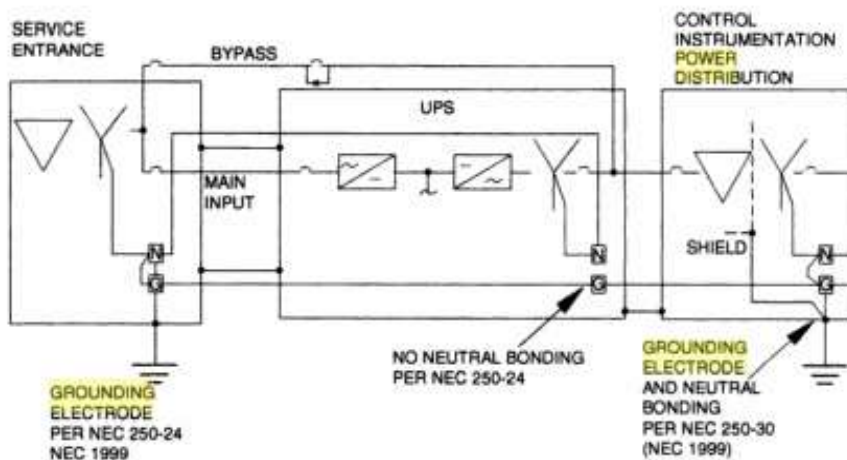


Figure 1.15: Grounding of separately derived instrumentation and control power.

Here the UPS is not separately derived source because its neutral is bonded to the grounding conductor at the service entrance. Keeping in mind that sub-panels should not be bonded to neutrals, the neutral in the UPS is isolated from its equipment grounding conductor. Because the isolation transformer is a separately derived system, its neutral is bonded to the grounding conductor. Keep in mind that the grounding conductor refers to the main one at the service entrance. Also note that NEC 250-30(3) allows one to use the grounding electrode in place of a local grounding electrode at the transformer. NEC 250-30(2) requires, in either case, that the grounded conductor of the transformer be connected to the grounding electrode. It also requires that the grounded conductor of the derived system and the equipment grounded conductor be bonded. Thus, the service and separately derived systems will always be bonded.

In this arrangement, the service entrance power can be supplied at 208 or 480 V. a 480-V input/480-V output UPS is recommended to reduce the cost of feeder wire and to reduce voltage drop. Stepping down to 120 V is accomplished in the isolation transformer.

Note that for this configuration, noise elimination effectiveness is dependent on how close the transformer is located to the loads. One of the benefits of placing the transformer after the UPS is that the UPS does not have to be located close to the loads to attenuate noise properly.

1.5.2.4 Single-Point Grounding of Power Supplies

It is desirable to “isolate” control system and instrumentation power from other power sources in a facility. Figure 1.2 demonstrates the preferred method of obtaining this goal while meeting code requirements. Note that all equipment is grounded to a single point. What figure 1.15 does not show is how

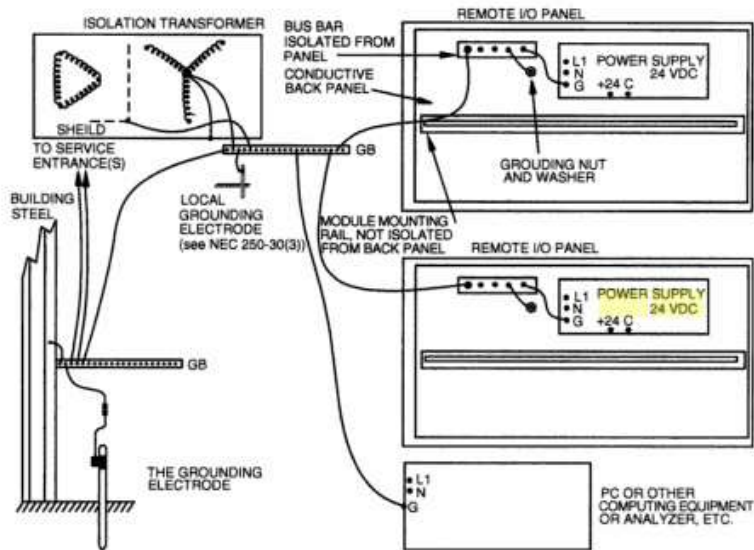


Figure 1.16: Single-point grounding of power supplies, computing equipment and signal cabinetry

this single point grounding concept is carried over to the numerous points where grounding is required in a typical control system and instrumentation network. Although safety may seem to be less of a concern at the low voltages normally encountered, single-point grounding has implications for noise elimination as well. For one, if connections are made haphazardly along a very long ground bus, potential differences develop at the various points due to bus resistance.

These potential differences would then lead to current loops. Although it is not possible to connect every ground to a single point, Figure 1.16 suggests an approximate method that is widely accepted. Note that only equipment grounding conductors are shown. Power conductors, conduit, cable tray, and the bonding thereof are not shown.

Although the input/output (I/O) modules are not shown, it is assumed that they are powered by the power supply or by a grounded neutral plus ungrounded conductor circuit derived from the transformer. Discrete signal neutral wiring is not shown because the neutral can come from a variety of sources. It is further assumed the I/O modules provide connections for cable shields at grounded terminals adjacent to the signal terminals and that all signals are grounded either at the modules (analog) or via their neutral conductors (discrete). This implies that analog modules provide grounding via their connection to the mounting rail. Grounding of signals at the I/O module is the most common method of signal grounding. Still, not all I/O modules confirm to this approach.

1.5.2.5 The Ungrounded System

NEC code allows for use of ungrounded systems in certain situations. Usually, the idea is to eliminate unexpected equipment outages. In such facilities, a single fault to ground will not cause overload protection to operate. Ground fault indicators are thus necessary to alert maintenance staff when and where a fault has occurred so it can be cleared. Otherwise, the purpose of not grounding, i.e., avoidance of unexpected outages, would not be met once a second fault causes unexpected tripping of over-current protection. Ground fault detectors are basically current switches placed around ground conductors or ground all the

phases in a power line. Although, it seems simple enough, it is often very difficult to design a ground fault detection network that makes locating the fault a trivial matter. With a grounded system, fault location is obvious. One should evaluate other techniques for increasing availability, such as redundancy, prior to deciding on an ungrounded system.

No matter what the reason for not grounding, one is still required to detect ground faults. This is usually accomplished using what NEC and IEEE call “relays”. Relays are current switches that detect:

- 1) Unbalanced current flow in an AC circuit (the faulted conductor experiences more flow than the other) or
- 2) Current flow in the grounding electrode system.

1.5.2.6 Resistance Grounding

The magnetic field component of very high fault currents can produce mechanical stresses beyond what some machinery is designed to handle. Motor and generator frames can be torn apart by a magnetic field associated with a fault current. Grounding through a carefully sized resistance counteracts this problem. Ground fault and ground resistance monitoring is employed in such systems as well.

1.5.2.7 Shielding Theory

Good topological planning during the design phase is absolutely essential to ensure electromagnetic compatibility (EMC) in electronic equipment and installations. Topology may be likened to a geometric hierarchy of EM zones, ranging from an utterly unprotected environment to a completely “clean” one, such as a computer room or a rack in which all sensitive electronic circuitry has been enclosed within a tight metallic shield. Barriers installed between zones prevent unwanted disturbances from passing into protected areas, whether they be electromagnetic fields generated by intentional or unintentional radio transmitters, transients induced on power lines, electrostatic discharges, or other EM threats (see Figure below).

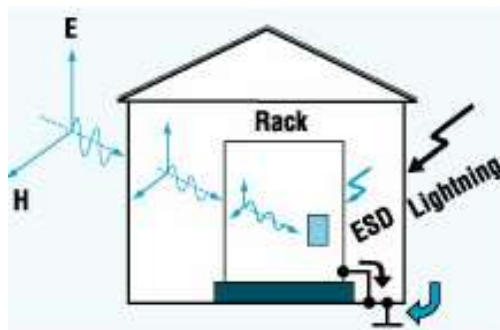


Fig 1.17

Figure: Shields are used to prevent unwanted EH-fields and other electro-magnetic disturbances from entering a protected electromagnetic zone.

The Topological Approach

The EM topology approach requires the identification of the various electromagnetic zones created by an apparatus or installation, each of which must be separated by a geometrical or physical barrier (see

Figure a below). A geometrical barrier is essentially an open area in which existing electromagnetic fields will decay to an acceptable level, similarly, between two conductive elements, it may also be a distance that represents a capacitive coupling small enough to neglect the coupling path for transient disturbances. A physical barrier, in contrast, typically takes the form of a metallic shield that will either keep electromagnetic fields from penetrating into electronic circuitry or, conversely, keep radiated emissions produced by electronic circuitry from polluting the environment. Such shields can also protect against electrostatic discharges, as well as currents in the grounding system—provided, that is, that they are connected to ground/earth in such a way that any disturbances are shunted away from the sensitive electronics to be protected, as in Figure below. Because shielding and grounding go hand in hand, it is vital that the latter be taken into account when the electromagnetic topology is configured (see Figure b below). A few specific guidelines may be helpful here:

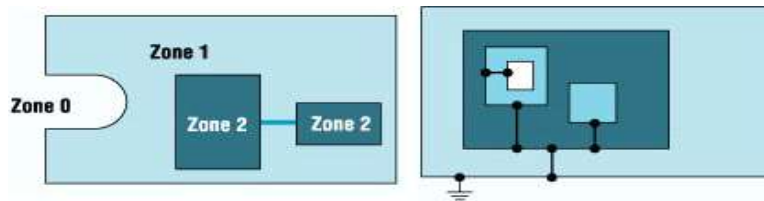


Fig 1.18 (a)

Figure a: Electromagnetic topology can be seen as a series of zones separated by geometrical or physical barriers. **b:** An inner screen should be connected with a ground reference to the surrounding screen. Screens between zones that are not adjacent should not be connected.

If EMI filters or transient-suppression components are used as a barrier to prevent conducted disturbances originating in one zone from propagating into another, they should always be placed at the border of the protected zone.

- A shielded cable must be carefully grounded in order to do its job effectively.
- Whenever a metallic screen separates two zones, all other barriers should be located as close as possible to that screen.
- A power-line filter with a shielded enclosure must be mounted in direct contact with the screen in order to provide adequate attenuation.

Screened rooms, metallic racks, and conductive chassis all constitute barriers designed to separate a “clean” electromagnetic zone from a more polluted one. Inner zones are often thought of as the cleaner ones, used to protect sensitive electronic circuitry, but the opposite may also be the case, as when a screened cover is employed to prevent emissions from a circuit with very high internal clock frequencies. Similarly, a frequency converter mounted in a rack may require a separate enclosure combined with filters to prevent interference that might disturb other apparatus in the rack.

Shielding Effects

The shielded room and the screened enclosure both exemplify Faraday’s principle. To gain some insight into this physical effect without having to resort to field theory, let’s take the example of a thin, conductive, spherical shell placed in an electric field (see Figure a below). According to Faraday, we can expect the field inside the sphere to be almost zero. Why? Not because the shell has absorbed the field, but because the E-field has caused electrical charges of different polarity along the screen. These charges will, in

turn, generate an electrical field that will tend to cancel the original field inside the shell. Because electrons can move easily along any conductive surface, the thickness of the shield is not in itself a significant factor.

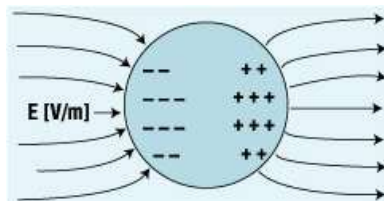


Fig 1.18 (b)

Figure b: Faraday's cage. A metallic spherical shell of good conductivity will eliminate the internal electrical field because induced charges tend to generate a second electrical field that cancels the original one.

When it comes to magnetic fields, Faraday's effect has no relevance, since there is no such thing as a magnetic charge. Magnetic-field attenuation can, however, be achieved by means of a screen made of a magnetic material combining high permeability ($\mu \gg 1$) with sufficient thickness to attract the material's magnetic field by providing a low-reluctance path (see Figure b below). Alternatively, as Figure c shows below, a thin shield made of a conductive material with low permeability can also provide effective shielding for magnetic fields because an alternating magnetic field will induce so-called eddy currents in the screen (assuming, that is, that the shield has adequate conductivity). These eddy currents will themselves create an alternating magnetic field of the opposite orientation inside the shell. The effect will increase as frequency increases, resulting in high shielding effectiveness at high frequencies.

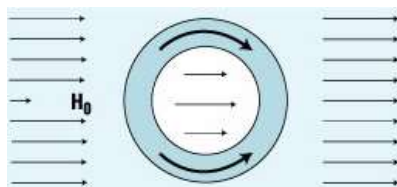


Fig 1.18 (c)

Figure c: A spherical shell of magnetic material with good permeability will reduce the field inside because the field tends to remain in the magnetic layer as it offers a low-reluctance path.

Low-frequency magnetic fields are more difficult to shield against. However, whereas absorption shielding typically calls for the installation of thick shields constructed of fairly expensive magnetic materials, shields based on the induced-current principle may be reasonably effective at power-line frequencies. Consequently, aluminum screens are commonly used to protect against 50- and 60-Hz magnetic fields generated by transformers and other sources.

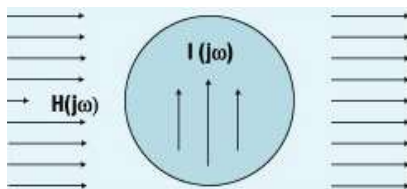


Fig 1.18 (d)

Figure d: A thin metallic shell of good conductivity will reduce an alternating magnetic field (ac) inside because the currents induced by the field tend to generate a field of opposite direction from the original.

Any apertures or breaks in a shield will limit its effectiveness. Since the theory behind magnetic-field shielding via induced currents presumes that such currents will flow as long as there are no obstacles in their path, it is essential that any and all apertures be arranged in such a way as to minimize their effect on the currents (see Figures a and b below). Note, too, that apertures have HF resonances, so an (induced) HF current flowing on the screen can cause the aperture to act as a transmitting antenna.

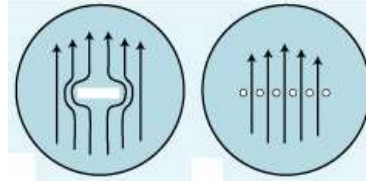


Fig 1.18 (e)

Figure e: Apertures may prevent induced currents from promoting shielding effectiveness. They can also act as transmitters for certain HF frequencies related to their resonance frequencies.

Closed screening is one kind of electromagnetic barrier. Another kind may consist of a sort of open generalized screening representing the attenuation of the electromagnetic coupling between two zones. For example, a vertical metallic plane positioned in the path of a horizontally propagating electromagnetic field will provide a generalized screening effect for electronics located in the “shadow” on the other side. Yet another example is the ground plane on a printed circuit board or on the ground floor in a computer room. Both will reduce the coupling of an environmental electromagnetic field into any cables and/or strips placed close to them, creating a protective zone extending some distance above the plane or floor. This generalized screening may yield an attenuation of up to about 30 dB per 10 dB shielding effectiveness for electronic circuitry mounted on a printed circuit board or for a computer system with cables placed close to the computer room floor. The reason for this is that the E-field tends to “hit” a conductive ground plane at right angles, rendering it impossible for the field to induce an electric potential along cables running parallel to the screen. Likewise, because an H-field located near a metallic surface tends to have its predominant field component parallel to the surface, it will be unable to induce currents into a cable loop placed close to the shield. Keeping cabling as close as possible to a reference ground plane is therefore a very effective means of achieving a generalized screen.

Shielding theory is based on two fundamental mechanisms, reflection loss and absorption loss. Figures (10) and (12) illustrate the principle involved in placing a metallic barrier in the path of an electromagnetic plane wave propagating with orthogonal E and H vectors. The E- and H-field components are related by the wave impedance, which is defined by the ratio of the tangential field components, so that

$$Z = E / H$$

In free space, the wave impedance is

$$Z_0 = \sqrt{\mu_0 / \epsilon_0} = 120 \pi = 377 [\Omega]$$

Where,

$$\mu_0 = 4\pi 10^{-7} / \epsilon_0 = 10^{-9} / 36\pi$$

A metallic screen however has much lower impedance

$$[Z_s] = \sqrt{j\omega\mu / \sigma}$$

$\mu = \mu_r \mu_0$ is the Permeability

$\epsilon = \epsilon_r \epsilon_0$ is the dielectric constant;

σ is the conductivity, $[1/\Omega\text{m or "mhos/m"}]$, and

$$\omega = 2\pi f = 2\pi c_0 / \lambda$$

Where

f is the frequency [Hz],

$c_0 = 3 \cdot 10^8$ is the speed of light [m/s];

and $\lambda = c_0 / f = 300/f_{\text{MHz}}$ is the wavelength [m]

This implies an impedance mismatch for the wave, which therefore causes reflections. The remaining field is transmitted through the barrier after partial absorption by the metal. The electric-field component is reflected predominantly when it has to pass into a medium with lower impedance (at the first surface), while the magnetic component is reflected when it must pass into a medium with higher impedance (the second surface). Between the two surfaces there will be multiple reflections, which may be overlooked if the absorption loss in the barrier is at least 10 dB.

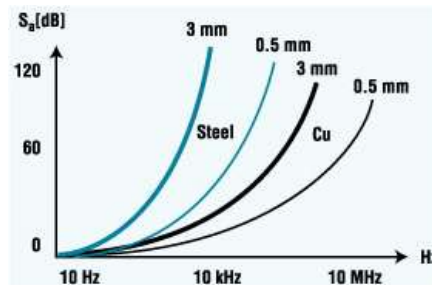


Fig 1.19

Figure: Absorption loss for an EH-wave as a function of frequency for steel and copper shield, respectively of 0.5 and 3mm thickness.

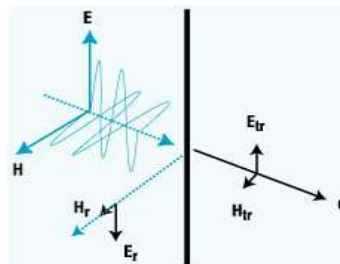


Fig 1.19

Figure: The reflection loss for an EH wave will depend on the ratio of the free space impedance Z^0 to the impedance in the screen Z_s .

Figure above shows that the shielding effectiveness for a plane wave is typically no less than 100 dB in the MHz region. For a large metal screen of thickness t , the total loss can thus be calculated as:

$$S = S_a S_r \approx 0.35 \cdot (\lambda / 2\pi\mu_r\delta) \cdot e^{t/\delta} \quad (t > \delta)$$

$$S = S_a S_r \approx (t/\delta) \cdot (\lambda / 2\pi\mu_r\delta) \quad (t < \delta)$$

A thin spherical shield, in contrast, will produce a loss of:

$$S = S_a S_r \approx (t/\delta) \cdot (2r/3\mu_r\delta) \quad (t > \delta)$$

(Where r = equivalent radius and t = thickness)

In the case of a multiple-laminated shield, the total reflection and absorption losses may be seen as, respectively, the sum of reflection losses at each surface and the sum of attenuation losses in each layer.

Near-Field Conditions

Plane-wave conditions assume that the field is fully developed ($E/H = Z_0 = 377\Omega$), which is the case if the distance from the radiation source is great enough. This is called the far-field region. The amplitude of the E-field and H-field, respectively, decreases in the far-field region as $1/r$ —that is, the E- and H-field is reduced 20 dB (10 dB) if the distance r is increased 10 times (3.3 times).

In the near-field region, by contrast, the ratio between E and H is complex and varies with the distance from the source. A high-impedance source antenna (e.g., a dipole antenna) will produce a near field dominated by E ($E/H \gg Z_0$), while a low-impedance antenna (e.g., a current loop) will yield a near field dominated by H ($E/H \ll Z_0$). At a distance of $1/2$, the wave impedance will approach Z_0 and the field will start to decrease linearly with distance when $r = 1/2$.

In the near field, the shielding effectiveness must be regarded separately for the electric and the magnetic fields.

1.5.2.8 Power Supply Shielding

Proper use of a floating power supply to power instrumentation loops varies depending on the type of signal generator and whether differential or single-ended instrumentation is being employed. With resistance bridge signal generators, it is important to ground the bridge and shield(s) appropriately if either differential or single-ended equipment is used.

Guidelines for shielding, grounding and physical separation from power circuits are provided. The general rules set forth are guidelines only and should be tempered by specific manufacturer's recommendations, particularly for computer applications.

Definitions

- a) Normal mode noise (transverse). The noise appearing between the signal wires caused by one of the following:
 - i. Electro-static induction due to disturbed capacitance between the signal wires and the surroundings.
 - ii. Electromagnetic induction due to magnetic, fields linking with the signal wires.

- iii. Junction or thermal potentials due to improper connections.
- b) Common mode noise (longitudinal). The noise appearing between each signal wire and ground caused by:
 - i. Incorrect location of signal, ground
 - ii. Multiple grounding of shield.
- c) Cross talk. The noise caused by AC and pulse type signals in adjacent circuits.

Recommendations for Noise Reduction

- a) Electrostatic normal mode noise can best be minimized by shielding.
- b) Electromagnetic normal mode noise can effectively be reduced by twisting signal conductor pairs, and physical separation between power and instrumentation cables.
- c) Common mode noise caused by ground potential differences can best be minimized by grounding a shield at only one point and by the correct location of that ground point.
- d) Cross talk can best be reduced by using cables with twisted pair conductors and individually insulated shields over each pair.

***Note:** The length and direction(s) of lay (right or left hand twists per inch) may depend on the cable design and are optimized in relation to performance requirements and good construction practices.*

Shielding Recommendations

- a) Aluminum or copper backed tape, 100% coverage, with a copper drain wire (tinned copper should be used with aluminum) is a more effective electrostatic shield than a braid or served wire armor.
- b) At a minimum, low-level analog signal cables should be made up of twisted pairs with an overall shield.
- c) Digital signal cables and pulse type circuits should be wired with individually twisted and shielded pairs. In multi-pair cables, the shields should be isolated and an overall shield should also be provided.
- d) Except where specific reasons dictate otherwise, cable shields should be electrically continuous. When two lengths of shielded cable are connected together at a terminal block, a point on the terminal block should be used for connecting the shields.
- e) The shield of each cable should be covered with an insulating tape or jacket in order to prevent stray and multiple grounds to the shield.

Grounding Recommendations

- a) All shields should be grounded.
- b) Shields should be grounded at only one point.
- c) Digital signal circuits should not be grounded at any point external to the power supply.
- d) The shields on grounded as well as ungrounded thermocouple circuits should be grounded at the thermocouple well.
- e) Multi-pair cables used with thermocouples must have individual isolated shields so that each shield may be maintained at the particular couple ground potential.

- f) The low or negative potential side of a signal pair should be grounded at the same point where the shield is grounded. Where a common power supply is used, the low side of each signal and its shield should be grounded at the power supply.

1.6 Considerations of Computers and its Peripherals

This service involves the design, installation and configuration of networks without an existing network. By installing a network, IT resources can be shared and managed more efficiently.

Computers and Peripherals Service and Maintenance

This undertakes the diagnosing and troubleshooting of faulty computers and peripherals; the preventive maintenance of computers (on a quarterly basis) through a yearly preventive maintenance contract or the client is required.

Data Management – Data Backup, Data Storage and Data Recovery

The implementation of a suitable data backup process for the clients is required. This service covers the purchase, set-up and management of the data backup process. The physical storage of the backup media including offsite scheduling and test runs.

Benefits of Preventive Maintenance of Computers and Printers

Generally the benefits of regular preventive maintenance of computers and peripheral are huge. When you take into consideration the initial cost of purchase of the hardware, the cost of repairs, when the systems breakdown due to lack of regular maintenance and the actual cost of being without the particular computer or an essential printing device in an organization. Notwithstanding the cost of the repairs or replacement.

Computers and printers by design will only perform efficiently if they are being regularly maintained. Let us start with the computer, during daily usage, the system builds up data from downloads in the temp file, allocated for temporary storage of such downloads and since the folder size is fixed it has to be emptied from time to time.

The recycle bin which stores all deleted files also needs to be occasionally emptied to free up space on the hard disk. You need to delete cookies from time to time in Internet explorer to make Internet access faster and allow explorer to work properly.

The above may well be minor issues compared to the need for regular scanning of the hard disk surface to repair any bad sectors or clusters that may eventually lead to loss of data or corruption of the operating system. As we install data and programs on the hard disk, the data fragments on the surface of the disk thereby causing the system to spend more time in accessing the data. By defragging the disk the data is re-arranged in a manner that makes it easier to access, therefore reducing access time and increasing the speed of the computer.

Most organizations these days have constant access or connection to the Internet, in as much as this is a blessing to all businesses given the savings to be made by e-commerce and communications it does also open a permanent channel to viruses, worms and Trojans constantly streaming in from the Internet. Regular maintenance will ensure the security protection is adequate and up-to-date.

Irrespective of the fact that most organizations use air-conditions in their offices over time dust still

clogs up on the surface of the electronic circuits in the computer. The dust reduces the effect of the system fans in reducing the heat generated by the high-speed circuits; the heat then goes to damage the systems components. Dust build up on processor fans can also reduce the speed of the fan over a period of time and cause the processor to overheat leading to damage to the processor.

In the case of printers every print generates an amount of print residue resulting from the use of toner and paper through the printing device. Ink Jet printers even have tanks or holding area for the ink residue, which needs to be occasionally emptied. The residue does not just settle in this location provided but also builds up on the print path, which needs to be vacuumed from time to time. Some of the parts of the printers do have a definite life span and HP does sell service kits for the replacement of these parts at the end of their projected life span.

Taking all of the above issues into consideration, it is therefore imperative for every organization to make provision for such preventive maintenance services to be carried out regularly to extend the life span of their investment in computers and peripheral for their equipments to function efficiently, work faster, prevent loss of valuable data, prevent or limit virus infections and intrusions, save on the repair or replacement cost and the real cost of system down time.

EXERCISE

1. What is maintenance? Explain different types of maintenance.
2. Explain the activities required to do in maintenance. What are different maintenance levels?
3. What are the factors that influence the equipment indenture level?
4. Explain the terms:
Shielding, Grounding, Meantime Between Failure (MTBF) and Meantime to Repair (MTTF).
Explain the causes of these policies failures.
Explain circuit tracing techniques.

Fundamental Troubleshooting Procedures

Instructional Objectives

- 2.1 Troubleshooting Process
- 2.2 Fault Location
- 2.3 Fault Finding Aids
- 2.4 Service Manuals
- 2.5 Testing and Measuring Instruments
- 2.6 Special Tools

2.1 Troubleshooting Process

The process of troubleshooting comprises the following steps:

2.1.1 Fault Establishment

Before any other action is taken, it is important to establish the presence of a fault in equipment. In some cases, a system may be reported faulty, but it may be a case of a faulty operation or a system failure may be reported with either very little or misleading information. It is essential that a functional test be made for checking the system's actual performance against its specification, and that all fault symptoms be noted.

It is also important to check with the equipment operator the history of the equipment and the repair and servicing work carried out earlier by any other person. Sometimes, incomplete work or mishandling of the equipment by an inexperienced worker could prove disastrous and defy all efforts to repair the equipment.

2.2 Fault Location

The fault location procedure will comprise a study of the literature relevant to servicing, maintenance and repairs, and pinpointing the cause of the fault, first to a sub-system and finally to a single component within the sub-system. The fault location methods are discussed later in this chapter.

2.2.1 Fault Correction

Fault Correction consists of replacing and repairing the faulty component. This must always be followed by a thorough functional check of the whole system.

2.2.2 Fault Location Procedure

For fault location, it is advisable to follow systematic and logical approach as it is often easy to reach the trouble-spot by proceeding step by step. However, the degree of success in locating a particular fault will depend upon the technician's knowledge of the equipment and his ability to troubleshoot. It must be clearly understood that there is no substitute for familiarity with the equipment when it comes to troubleshooting a system. For example, if you are not familiar with a micro-computer to the extent that you can analyze its operation, interprets its indications, read its printouts, and analyze its programs, you will certainly have a tough time in isolating a failure within that equipment.

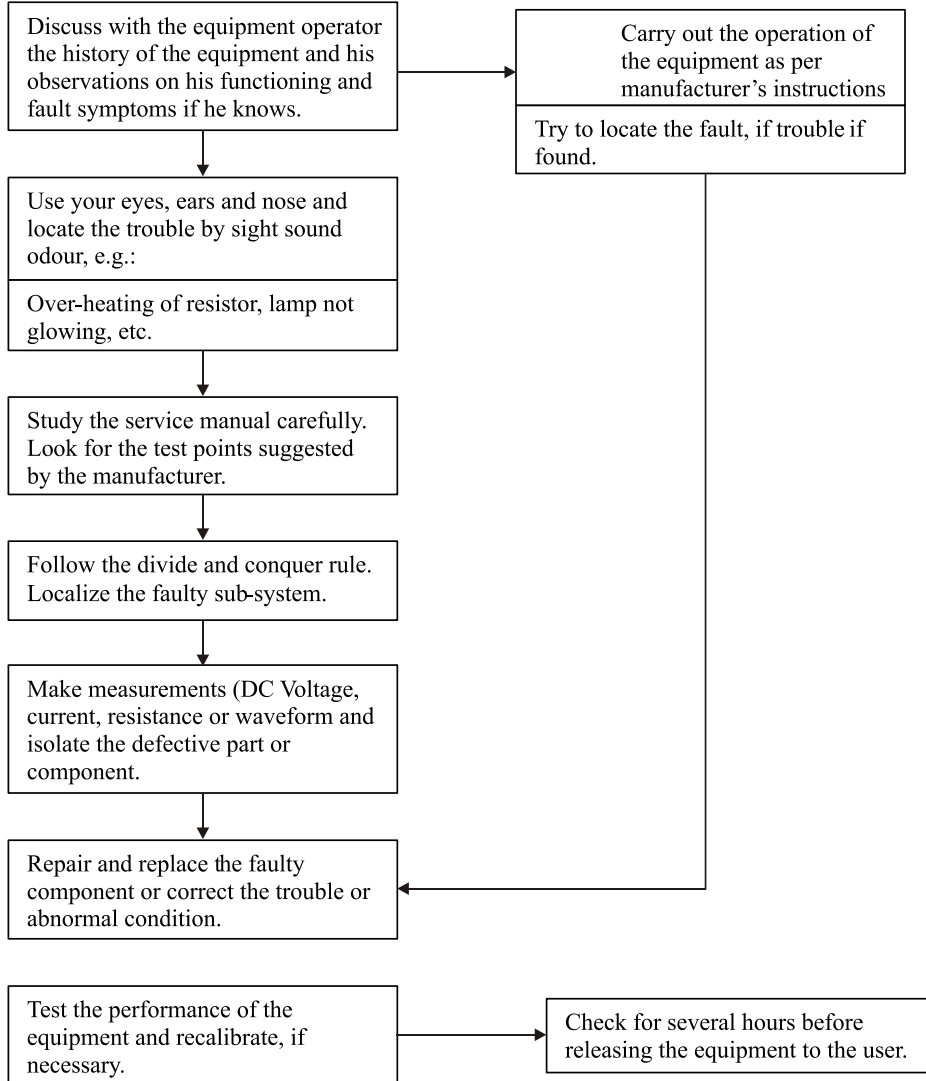


Figure 2.1: Fault Diagnosis Tree – generalized troubleshooting procedure

Troubleshooting procedure must always start with a preliminary analysis of the trouble symptoms, from which various possibilities of malfunction are deduced. These are analyzed in order of probability and various quick checks are usually made to eliminate or verify mutual deductions. Figure 2.1 gives a summary of the suggested generalized troubleshooting procedure.

The following questions should be asked and facts ascertained before proceeding with troubleshooting:

- i. Has this ever happened before? If the device has been historically known to fail in a certain particular way, check for this first.
- ii. If a system has been having problems immediately after some kind of maintenance or other change, the problems could be linked to those changes.
- iii. If a system is not producing the desired end-result, look for what it is doing correctly. In other words, identify where the problem is not present, and focus your efforts elsewhere.
- iv. On the basis of your knowledge of how a system works, think of what kind of failures would cause this problem or phenomenon to occur.

Effective troubleshooting requires a blend of both art and science. There is always a safe way and a technical accurate way to do something, but the precise choice of techniques and strategies used to fix the problem is largely decided by the technician's own experience and background.

2.3 Fault Finding Aids

In order to achieve rapid fault localization and its subsequent repair, the technician will obviously look for certain aids to supplement his technical skills. The most commonly needed aids are:

- a. Service and maintenance manuals and instruction manuals;
- b. Test and measuring instruments; and
- c. Special tools (instruments, mechanical tools).

2.4 Service Manuals

Reputed manufacturers usually supply a service and maintenance manual along with the equipment sold. If properly prepared, the manual provides information on:

- a. List of test instruments and special tools;
- b. Method of dismantling;
- c. Safety procedures to be observed while dismantling and while carrying out tests;
- d. Test points with DC voltages and operating waveforms;
- e. Fault location tree or tables showing typical symptoms for various fault conditions, together with the most probable causes and suggested course of action;
- f. Block diagram description;
- g. Circuit diagrams;
- h. Spare parts list, with component values, rating and tolerances;
- i. Printed circuit board layouts for various components identified by means of callouts; and
- j. Mechanical layout, line diagrams, photographs and exploded views of various mechanical parts.

After checking the obvious things, if you do not find a clue about the fault, it is time to consult the service manual and to try to understand, firstly, the result that you should be getting and secondly, the result that you are getting. By doing this, either by measurement or observation, the technical performing the fault finding is guided to the faulty component.

Sometimes, the service manuals are not available. No doubt, based on the experience of other similar systems, the technician can attempt to repair the fault. However, if the system is unknown, proceeding with tests without knowing exactly how the system performs can often lead to incorrect conclusions and in some cases, in causing extra faults. Therefore, it is wise to procure the service manual, as far as possible, before trying to locate a serious fault in the system. However, if you are not able to get the schematic diagram, in some cases, some reverse engineering will be necessary in drawing the circuit diagram. The time will be well-spent as you would have learnt something in the process that can be applied to other equipment problems. Your success in finding and repairing the fault will be much more likely when you understand how a device works.

The instruction manual or user manual or operator's manual provides necessary information for operating the equipment, start-up and shut down instructions, general design concepts, specifications and the installation procedure. Operator level maintenance instructions including preventive maintenance manuals are useful for preliminary diagnostics establishing preventive maintenance schedules.

2.5 Testing and Measuring Instruments

The task of troubleshooting is essentially carried out by using numerous test instruments in various areas of electronic servicing. Leaving aside any special instrument that may be required for working on digital and communication equipment, a majority of the system faults can be located and rectified by using the following three instruments:

- a. Multi-meter
 - i. Analog
 - ii. Digital
- b. Oscilloscope
- c. Signal generator or pulse generator or function generator.

The type of measurements usually carried out in electronic circuits is basically DC and AC voltage measurements. Besides these, a variety of measurements in terms of amplitude, frequency and phase, and a detailed waveform analysis are needed to be performed on complex circuit functions in order to aid the troubleshooting procedure.

2.6 Special Tools

However, a few hardware diagnostic tools can be very helpful in isolating defective hardware components. These tools include:

- Software diagnostic disk
- Multimeter
- Cable tester
- POST card

1). Software Diagnostic Packages

Several commercially available disk-based diagnostic routines can check the system by running predetermined tests on different areas of its hardware. The diagnostic package evaluates the response from each test and attempts to produce a status report for all of the system's major components. Like the computer's self-tests, these packages produce visual and beep-coded error messages.

This menu is the gateway to information about the system's makeup and configuration, as well as the entryway to the program's Advanced Diagnostic Test functions. You can find utilities for performing low-level formats on older hard drive types and for managing small computer system interface (SCSI) devices through this menu. In addition, options to print or show test results are available here, as is the exit point from the program.

The most common software-troubleshooting packages test the system's memory, microprocessor, keyboard, display monitor, and the disk drive's speed. If at least the system's CPU, disk drive, and clock circuits are working, you might be able to use one of these special software-troubleshooting packages to help localize system failures. They can prove especially helpful when trying to track down non-heat-related intermittent problems.

If a diagnostic program indicates that multiple items should be replaced, replace the units one at a time until the unit starts up. Then replace any units removed prior to the one that caused the system to start. This process ensures that there are not multiple bad parts. If you have replaced all the parts, and the unit still does not function properly, the diagnostic software is suspect.

2). Using a Multimeter in a PC

A number of test instruments can help you isolate computer hardware problems. One of the most basic pieces of electronic troubleshooting equipment is the multimeter. These test instruments are available in both analog and digital readout form and can be used to directly measure electrical values of voltage (V), current in milliamperes (mA) or amperes (A), and resistance in ohms. Therefore, these devices are referred to as VOMs (volt-ohm-milliammeters) for analog types, or DMMs (digital multimeters) for digital types.

With a little finesse, you can use this device to check diodes, transistors, capacitors, motor windings, relays, and coils. This particular DMM contains facilities built in to the meter to test transistors and diodes. These facilities are in addition to its standard functions of current, voltage, and resistance measurement; however, in computer repair work, only the voltage and resistance functions are used extensively.

The first step in using the multimeter to perform tests is to select the proper function. For the most part, you never need to use the current function of the multimeter when working with computer systems; however, the voltage and resistance functions can be very valuable tools.

In computer troubleshooting, most of the tests are DC voltage readings. These measurements usually involve checking the DC side of the power-supply unit. You can make these readings between ground and one of the expansion-slot pins, or at the system board power-supply connector. It is also common to check the voltage level across a system board capacitor to verify that the system is receiving power. The voltage across most of the capacitors on the system board is 5V (DC). The DC voltages that can normally be expected in a PC-compatible system are +12V, +5V, -5V, and -12V. The actual values for these readings might vary by 5% in either direction.

Caution

It is normal practice to first set the meter to its highest voltage range to be certain that the voltage level being measured does not damage the meter.

The DC voltage function is used to take measurements in live DC circuits. It should be connected in parallel with the device being checked. This could mean connecting the reference lead (black lead) to a ground point and the measuring lead (red lead) to a test point to take a measurement,

As an approximate value is detected, you can decrease the range setting to achieve a more accurate reading. Most meters allow for overvoltage protection; however, it is still a good safety practice to decrease the range of the meter after you have achieved an initial value.

The second most popular test is the resistance, or continuity test.

Caution

Unlike voltage checks, resistance checks are always made with power removed from the system.

Failure to turn off the power when making resistance checks can cause serious damage to the meter and can pose a potential risk to the technician. Resistance checks require that you electrically isolate the component being tested from the system. For most circuit components, this means desoldering at least one end from the board.

The resistance check is very useful in isolating some types of problems in the system. One of the main uses of the resistance function is to test fuses. You must disconnect at least one end of the fuse from the system. You should set the meter on the 1k ohm resistance setting. If the fuse is good, the meter should read near 0 ohms. If it is bad, the meter reads infinite.

The resistance function also is useful in checking for cables and connectors. By removing the cable from the system and connecting a meter lead to each end, you can check the cable's continuity conductor by conductor to verify its integrity.

You also use the resistance function to test the system's speaker. To check the speaker, simply disconnect the speaker from the system and connect a meter lead to each end. If the speaker is good, the meter should read near 8 ohms (although a smaller speaker might be 4 ohms). If the speaker is defective, the resistance reading should be 0 for shorts or infinite for opens.

Only a couple of situations involve using the AC voltage function for checking microcomputer systems. The primary use of this function is to check the commercial power being applied to the power-supply unit. As with any measurement, it is important to select the correct measurement range; however, the lethal voltage levels associated with the power supply call for additional caution when making such measurements.

The second application for the AC voltage function is to measure ripple voltage from the DC output side of the power-supply unit. This particular operation is very rarely performed in field-service situations.

3). Cable Testers

The most frequent hardware-related cause of network problems involves bad cabling and connectors. Several specialized, handheld devices designed for testing the various types of data communication cabling are available. These devices range from inexpensive continuity testers, to moderately priced data cabling testers, to somewhat expensive time domain reflectometers (TDR).

Although inexpensive continuity testers can be used to check for broken cables, data cabling testers are designed to perform a number of different types of tests on twisted-pair and coaxial cables. These wiring testers normally consist of two units—a master test unit and a separate load unit,

The master unit is attached to one end of the cable and the load unit is attached to the other. The master unit sends patterns of test signals through the cable and reads them back from the load unit. Many of these testers feature both RJ-45 and BNC connectors for testing different types of cabling. When testing twisted-pair cabling, these devices can normally detect such problems as broken wires, crossed-over wiring, shorted connections, and improperly paired connections.

TDRs are sophisticated testers that can be used to pinpoint the distance to a break in a cable. These devices send signals along the cable and wait for them to be reflected. The time between sending the signal and receiving it back is converted into a distance measurement. The TDR function is normally packaged along with the other cable testing functions just described. TDRs used to test fiber-optic cables are known as optical time domain reflectometers (OTDRs).

4). POST Cards

A POST card is a diagnostic device that plugs into the system's expansion slot and tests the operation of the system as it boots up. These cards can be as simple as interrupt and direct memory access (DMA) channel monitors, or as complex as full-fledged ROM BIOS diagnostic packages that carry out extensive tests on the system.

POST cards are normally used when the system appears to be dead, or when the system cannot read from a floppy or hard drive. The firmware tests on the card replace the normal BIOS functions and send the system into a set of tests. The value of the card lies in the fact that the tests can be carried out without the system resorting to software diagnostics located on the hard disk or in a floppy drive.

The POST routines located in most BIOS chips report two types of errors—fatal and nonfatal. If the POST encounters a fatal error, it stops the system. The error code posted on the indicator corresponds to the defective operation.

If the POST card encounters a nonfatal error, however, it notes the error and continues through the initialization routine to activate as many additional system resources as possible. When these types of errors are encountered, the POST card must be observed carefully because the error code on its indicator must be coordinated with the timing of the error message or beep code produced by the BIOS routines.

Simple POST cards come with a set of light-emitting diodes (LEDs) on them that produce coded error signals when a problem is encountered. Other cards produce beep codes and seven-segment LED readouts of the error code

EXERCISE

1. Explain the process of troubleshooting with all the steps.
2. What is the information included in service manual? Why service manual is helpful?
3. What are different types of testing instruments? Why are testing instruments helpful?
4. What are the special tools required to efficiently carry out troubleshooting process?
5. What are the most commonly fault finding aids needed?

Hardware and Software Faults

Chapter

3

Instructional Objectives

- 3.1 Troubleshooting Techniques
- 3.2 Different Troubleshooting Techniques and Methods
- 3.3 Functional Area Approach
- 3.4 Split Half Method
- 3.5 Divergent, Convergent and Feedback Path Circuits
- 3.6 Analysis measured Techniques

3.1 Troubleshooting Techniques

3.1.1 Preliminary Observations

When equipment is received from repairs, it is essential to carry out some preliminary checks on it before the actual work is started. These checks are necessary for your safety and often help in quickly approaching the trouble spot. The checks are as follows:

- a. Carefully examine the equipment on all sides for pertinent information given by the manufacturer on the panels. Safety precautions are generally printed on the panels with the following nomenclature:
 - i. Caution – indicates a personal injury hazard not immediately accessible as one reads the marking, or a hazard to property including the equipment itself.
 - ii. Danger – indicates a personal injury hazard immediately accessible as one reads the marking. Danger sign will be normally marked at places where high voltages exist on the equipment.
 - iii. Protective ground (earth terminal).
 - iv. Refer to manual.
- b. Be sure about the power supply requirements of the equipment. Some equipment is battery-operated while others may be operating on the mains power supply. Identify the mains power supply voltage, i.e. whether 110 volts, 60 Hz or 220 volts, 50 Hz and the maximum voltage that can be applied from the power source. Determine the supply conductors (if the plug is not present or if it is suspected to be weird wrongly) and the ground lead. A protective ground connection by way of the grounding conductor on the power cord is essential for safe operation.
- c. Almost all modern electronic equipment which is mains-operated is grounded through the grounding conductor of the power cord. In order to avoid electrical shock, the power cord must be plugged into a properly wired receptacle before connecting to the product input or output terminals.

- d. Before switching on the equipment for preliminary examination, study the 'Service Manual' thoroughly and look for the following terms in the manual:
 - i. Caution statements specify conditions or practices that could result in damage to the equipment or other property.
 - ii. Warning statements specify conditions or practices that could result in personal injury or loss of life.
 - iii. Check for applicable cautionary or other information.
- e. The service manuals usually provide information for removing the equipment panels and to gain access to various circuit boards and individual components. Such instructions must be followed to the letter, otherwise by opening the wrong screws; the internal assemblies sometimes get dislodged resulting in damage to the fragile parts.
- f. Disconnect power to the equipment before attempting to remove the cabinet panels in order to avoid electric shock hazard.
- g. In some equipment, dangerous potentials exist at several points throughout the equipment. When the equipment is operated with the covers removed, do not touch exposed connections or components. Some transistors have voltages present on their cases. Always disconnect power before cleaning the equipment or replacing parts.
- h. Do not try to break open potted assemblies or components about which you have limited information. You would end up in further spoiling the equipment in case something gets damaged during this process.
- i. As far as possible, do not perform internal service or adjustment with dangerous voltages unless another person capable of rendering first aid resuscitation is present.
- j. The painted metal panels of equipment are generally vulnerable to scratching. Avoid rough handling of the panels.
- k. When the equipment cover is removed from the chassis of the equipment, bare metal edges are exposed which can scratch the work surface. Be careful that the sharp edges and corners of the chassis do not scratch the work surface area.
- l. The CMOS logic family of integrated circuits used in some equipment can be damaged by an uncontrolled static electricity discharge. Before handling any of the circuit boards, firmly grasp the equipment chassis to eliminate any static charge difference between your body and the equipment.
- m. Handle all circuit boards by the edges. CMOS circuits operate with currents in the nano-ampere range and leakage paths caused by skin oils, dirt, dust, etc. can cause inaccurate circuit performance in some equipment.
- n. After removing the cover of the equipment, inspect all exposed screws for tightness. Check that all printed circuit boards are firmly seated in their connectors or are in position. Check the conditions of all external cables, especially for splits or cracks and signs of twisting. If any serious damage is evident, the cable should be replaced immediately.

To summarize, an effective system of troubleshooting should be quite logical and it is useful to remember the following three points:

1. **Know your equipment:** Without familiarity with the equipment to the extent that one can analyze its operation, interpret its indicators and read and decipher printouts, one will have difficulty in isolating problems.
2. **Think before you act:** Do not straight away start replacing parts, disassembling various parts, etc. without thinking and analyzing for possible causes of trouble. Unorganized way of troubleshooting leads to more trouble and can take an unusually long time.
3. **Establish a general troubleshooting procedure:** Depending upon your knowledge of equipment, the availability of proper tools, test equipments, spare parts and time, a general troubleshooting procedure needs to be developed. It could be component level repair or board level maintenance. In the latter case, the defective boards are then repaired at a later time or sent back to the manufacturer for repairs.

3.2 Different Troubleshooting Techniques and Methods

The various troubleshooting techniques given below are representative of those used in troubleshooting in a majority of electronic systems. The type of system you are handling, along with your personal abilities, will decide the troubleshooting technique or techniques you adopt.

3.3 Functional Area Approach

An electronic system may comprise several functional parts which may include power supplies, amplification, generation, transmission, conversion, logical manipulation, and storage of signal voltages. Obviously, when the system fails to give the expected performance, the trouble could lie in any of the functional areas. This implies that it is essential to troubleshoot the system in an effort to isolate the fault to the failing functional area and then to the failing component within the functional area. The logical approach to isolating a fault is through a process of elimination of the functional areas that are performing properly. Once a failure is isolated to a specific functional area, further analysis of the circuitry within this area is carried out to isolate malfunction to the faulty component. This functional area approach is also called the block diagram approach to troubleshooting. The service manuals normally carry a block diagram description of the equipment which assists in a proper understanding of the performance of the electronic system. It is often more useful than the full circuit diagram, particularly when a system is handled for the first time.

3.4 Split-Half Method

In this technique of troubleshooting, once the absence of an output has been established, the circuit is split into half and the output is checked at the half-way point. It will help to isolate the failing circuit in the first or second half. After determining the faulty half, the circuit is split into half for further isolation of the failure. The process is continued until the failure is isolated to one function or component. The half-split method is extremely useful when the system is made up of a large number of blocks in series. A typical example is that of the division of frequency of an oscillator by decade counters for generating various timing pulses. Figure 3.1 shows one such scheme.

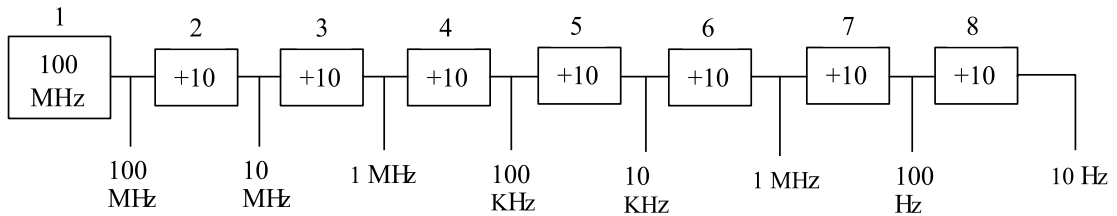


Figure 3.1: Split-Half method for isolating trouble in a circuit

Suppose that in this circuit, the expected output (100 Hz pulses) is not present. Let us suppose that the fault is in block 4. The sequence of carrying out tests would be as follows:

- Split the circuit into half (mentally) and measure the output of block 4. The output will not be present. So the fault lies anywhere in the first half (blocks 1 to 4).
- Split the circuit further into half and measure the output of block 2. The output will be found to be correct as 10 MHz. The fault thus lies in blocks 3 and 4.
- Measure the output of block 3. It will be found to be correct as 1 MHz. Therefore, the fault lies in block 4.

The example given here and the number of tests indicated may be an over-simplification. In practice, more measurements would be necessary to localize a fault, in case there are multiple faults in the system.

Unfortunately, most electronic systems do not involve only series of connected blocks. They may have feedback loops or parallel branches in a part of the circuit. Such situations will make the task of localizing faults complicated, but the half-split rule still remains applicable. The following situations may be carefully watched and fault analysis systematically carried out:

3.5 Divergent, Convergent and Feedback path circuits

3.5.1 Divergent Paths

In divergent paths (Fig. 3.2), the output from one block feeds two or more blocks. The most common example is that of the power supply circuit which supplies DC power to various sub-system in equipment.

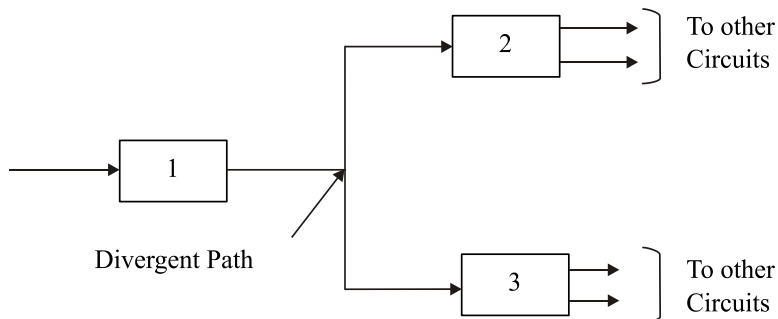


Figure 3.2: Troubleshooting circuits with divergent paths

In such a scheme, it is best to start by checking the common feedpoint. Alternatively, if one output (say at A or B) is normal, check after the divergent point. Conversely, if one output is abnormal, check before the common point.

3.5.2 Convergent Paths

In convergent paths, two or more input lines feed a circuit block (Figure 3.3). To check the performance of such a scheme, all inputs at the point of convergence must be checked one by one. If all are found to be correct, the fault lies beyond the convergent point. However, if any of the input is incorrect (at C, D) then the fault lies in that particular input circuit. For example, if C and D are correct, and there is no output at E, the fault lies in Unit 3. But if the input at C is incorrect, the fault lies in Block 1 or before that.

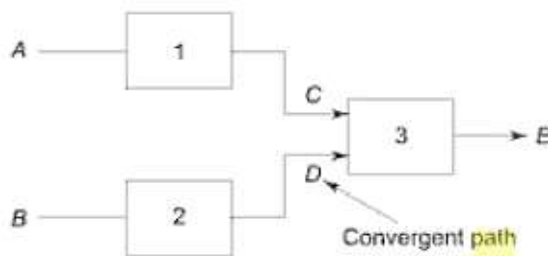


Figure 3.3: Isolating faults in convergent paths

3.5.2 Feedback Paths

The presence of a feedback loop in a circuit presents one of the more difficult problems in fault location. The feedback loop normally corrects the output of some block with the input of an earlier block via some network, known as the feedback network (Figure 3.4). Since the circuit behaves as a closed loop, any fault within the loop will appear as if the outputs of all blocks within the system are at fault.

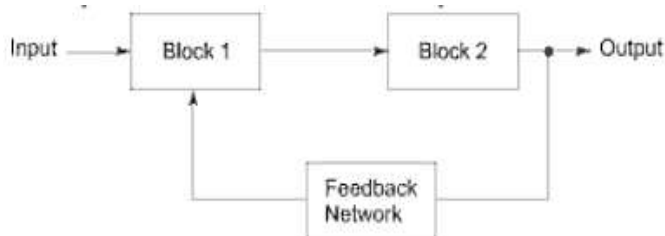


Figure 3.4: Feedback network circuit fault location

Feedback paths are provided basically for the following functions:

- Sustaining circuit function: In this case, the feedback is totally essential for an output to exist. For example, an oscillator circuit.
- Modification of circuit function: The feedback loop is provided to modify the characteristics of a system, for example, an automatic gain control circuit in a superhet radio receiver.

Before attempting repairs on a faulty system having a feedback loop, it will be essential to understand the type of feedback used and its purpose. Having done so, proceed as follows to locate the fault.

With modifying feedback, it may be possible to break the feedback loop and convert the system to a straight linear data flow. Each block can then be tested separately without the fault signal to be fed around the loop. In some cases, instead of completely breaking the feedback loop, it may be preferable to modify the feedback at or near the point where the feedback path rejoins the main forward path. If the output appears normal, check the feedback circuitry. If not, check the forward path.

In case of the sustaining path, feedback is disconnected from the input and a suitable test signal is injected to check the performance of various circuit blocks. Due to a wide variety of feedback circuits, it is difficult to suggest a rule of thumb for fault location in this type of feedback.

3.5.2.1 Switching Paths

In a system which has switchable parts (Figure 3.5) and if the circuit function is found to be faulty in one position of the switch, throw the switch to another position. If the trouble persists, check after the switch in the common circuitry. If the trouble disappears with this action, check that the circuitry is switched out.

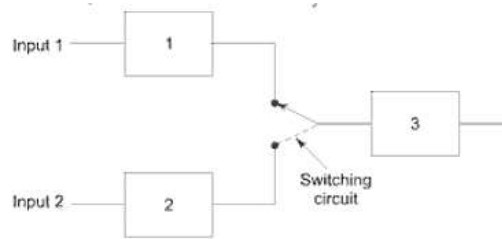


Figure 3.5: Fault location in switching circuits

3.6 Analysis Measured techniques

The analysis of simple circuits was carried by employing Kirchhoff's laws and Ohm's law. This approach can be used for all circuits. However, for circuits with more elements and structurally more complicated a systematic approach is preferable. The techniques of circuit analysis studied here provide an aid in the analysis of more complex circuits.

Techniques of circuit analysis

The purpose of circuit analysis is to determine the current in each of the b branches where the current is unknown. The formulation of b independent equations with these currents as variables is achieved by applying Kirchhoff's laws. In a circuit with n nodes, $n-1$ equations are formulated by applying Kirchhoff's current law (KCL) to any set of $n-1$ nodes and the remainder $b - (n-1)$ equations can be written by applying Kirchhoff's voltage law (KVL) to that number of meshes in the circuit. In general, $ne \leq n$ and $be \leq b$, where ne and be are the number of essential nodes and essential branches, respectively. Therefore, the formulation of the independent equations is achieved in terms of essential nodes and branches. However, by introducing new variables (*node voltages* and *mesh currents*), the circuit can be described with just $ne-1$ equations or just $be - (ne-1)$ equations.

Node-Voltage Method: The node-voltage method permits the description of a circuit in terms of $ne-1$ equations. Figure 3-1 shows a circuit suitable for analysis with the node-voltage method. In this circuit three essential nodes can be identified ($ne = 3$), therefore two ($ne - 1$) node-voltage equations describe the circuit. To select the set of $ne-1$ nodes to perform the analysis, one of the essential nodes is

selected as a reference node. The node with the most branches is usually chosen. The equations are then written by applying KCL to each non-reference node expressing the branch currents in terms of the node voltages. Once the equation system is solved and the node voltages are known, all the branch currents can be calculated.

Mesh-Current Method: The mesh-current method permits the description of a circuit in terms of $be - (ne - 1)$ equations. Figure 3-2 shows a circuit suitable for analysis with the mesh-current method. In this circuit four essential nodes ($ne = 4$) and six essential branches ($be = 6$) can be identified, therefore three ($be - (ne - 1)$) mesh-current equations describe the circuit. The equations are formulated by applying KVL to each mesh, expressing the voltages across the elements on the mesh in terms of the mesh currents. Once the equation system is solved and the mesh currents are known, all the branch currents (and any other parameter of interest) can be calculated.

Techniques for circuit simplification

Here, source transformations and Thevenin and Norton equivalent circuits are discussed as additional methods to simplify the circuit analysis.

Source transformations

A *source transformation*, shown in Fig. 3-3, allows the replacement of a voltage source in series with a resistor by a current source in parallel with the same resistor, or vice versa. In order for these two circuits to be equivalent, the voltage drop and the current drawn by any load at nodes a and b must be the same. The relationship between V_s and I_s is simply:

$$I_s = \frac{V_s}{R}$$

The above equation holds for the special cases when there is a resistor R_p in parallel with the voltage source or a resistor R_s in series with the current source. In both cases the resistance has no effect on the equivalent circuit (see Fig. 3-4). It can be shown that by applying source transformations on the circuit of Fig. 3-5, an equivalent circuit with respect to the voltage v_o consisting of a current source and a resistor can be found.

Thevenin and Norton equivalents

For purpose of analysis, it is often desirable to replace, at a specific pair of terminals (nodes) of a circuit, the set of interconnected elements (resistors and power sources) “behind” the pair of terminals, by a single resistor and a single power source. Thevenin and Norton equivalents are techniques of circuit simplification that describe the behavior of a circuit at a specific pair of terminals.

Thevenin equivalent

A Thevenin equivalent circuit is composed by an independent voltage source V_{Th} in series with a resistor R_{Th} , which replaces an interconnection of sources and resistors. The value of V_{Th} is the *open circuit voltage* at the pair of terminals in the original circuit. R_{Th} is given by the ratio of V_{Th} and the *short circuit current* observed at the pair of terminals when a short circuit is placed across them. Thus, $R_{Th} = V_{Th}/I_{sc}$. Fig. 3-6 shows a circuit that can be replaced by its Thevenin equivalent at terminals a and b . Determination of V_{Th} and R_{Th} can be simplified by applying source transformations.

Norton equivalent

A Norton equivalent circuit is composed by an independent current source I_N in parallel with a resistor R_N . The Norton equivalent can be derived from the Thevenin equivalent simply by making a source transformation. Therefore, the Norton current equals the short-circuit current at the terminals of interest, $I_N = i_{sc}$, and the Norton resistance is identical to the Thevenin resistance, $R_N = R_{Th}$. The circuit shown in Fig. 3-7 can be easily replaced by its Norton equivalent at terminals a and b . Notice that source transformations can be applied to calculate I_N and R_N .

Preparation

In preparation for the lab compute the required quantities.

1. **Node-voltage method.** Consider the circuit and the component values. Use the node-voltage method to complete the entries corresponding to the theoretical values. Do not use source transformations. Include your calculations in a separate sheet.
2. **Mesh-current method.** Consider the circuit and the component values. Use the mesh-current method to complete the entries corresponding to the theoretical values. Include the calculations in a separate sheet.
3. **Source transformations.** Consider the circuit and the component values. Use a series of source transformations to find an equivalent circuit (with respect to v_o) consisting of a current source and a resistor. Complete the entries in Table corresponding to the theoretical values. Use R_{01} and R_{03} for the calculation of v_{0o} . Include the calculations and circuit simplifications in a separate sheet.
4. **Thevenin equivalent.** Consider the circuit and the component values. Find the Thevenin equivalent and complete the entries corresponding to the theoretical values. Include the calculations in a separate sheet.
5. **Norton equivalent.** Consider the circuit and the component values. Find the Norton equivalent and complete the entries corresponding to the theoretical values. Include the calculations in a separate sheet.

Procedure

This part of the experiment requires assembling the resistive circuits presented in the previous section and measuring data from all of them. Set the current compliance value of the voltage source to 20 mA. The default voltage compliance value (21 V) for the current source is appropriate for this experiment.

1. **Node-voltage method.** Assemble the circuit with the component values shown in Table. Take measurements to complete the entries corresponding to the experimental values.
2. **Mesh-current method.** Assemble the circuit with the component values shown in Table. Take measurements to complete the entries corresponding to the experimental values.
3. **Source transformations.** Assemble the circuit with the component values shown in Table. Take measurements to complete the entries corresponding to the experimental values. Replace R_1 by R_{01} and R_3 by R_{03} to measure v_{0o} .
4. **Thevenin equivalent.** Assemble the circuit with the component values shown in Table. Take measurements to complete the entries corresponding to the experimental values. Connect the DMM in current measurement mode across terminals a and b in order to measure i_{sc} .

5. **Norton equivalent.** Assemble the circuit with the component values shown in Table. Connect the DMM in current measurement mode across terminals a and b in order to measure I_N . Measure V_{Th} in order to determine R_N .

Param	Unit	Theor	Param	Unit	Theor	Exper	%Error
R_1	k Ω	1.0	V_{R_1}	V			
R_2		2.2	V_{R_2}				
R_3		5.6	V_{R_3}				
R_4		6.8	V_{R_4}				
R_5		8.2	V_{R_5}				
V_s	V	10	v				
I_s	mA	10					

Fig 3.6 Node-Voltage Method

Param	Unit	Theor	Param	Unit	Theor	Exper	%Error
R_1	k Ω	1.0	V_{R_1}	V			
R_2		2.2	V_{R_2}				
R_3		5.6	V_{R_3}				
R_4		6.8	V_{R_4}				
R_5		8.2	V_{R_5}				
V_s	V	10					

Fig 3.7 Mesh-current method

Param	V_s	I_s	R_1	R_2	R_3	R_4	R_5	R'_1	R'_3	Param	Unit	Theor	Exper	%Error
Units	V	mA				k Ω				v_o	V			
Theor	10	3	1.0	2.2	5.6	6.8	8.2	2.4	4.7	v'_o	V			

Fig 3.8 Mesh-current method

Param	V_s	I_s	R_1	R_2	R_3	Param	Unit	Theor	Exper	%Error
Units	V	mA			k Ω	V_{Th}	V			
Theor	10	10	1.0	2.2	5.6	i_{sc}	mA			
						R_{Th}	k Ω			

Fig 3.9 Thevenin equivalent

Param	I_s	R_1	R_2	R_3	R_4	Param	Unit	Theor	Exper	%Error
Units	mA				k Ω	V_{Th}	V			
Theor	10	1.0	2.2	5.6	6.8	I_N	mA			
						R_N	k Ω			

Fig 3.10 Norton equivalent

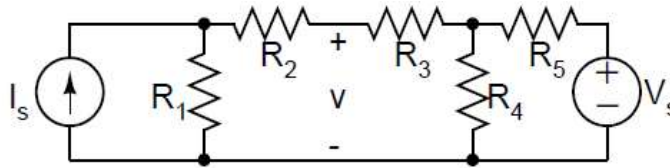


Fig 3.11 Test circuit for Node-voltage method

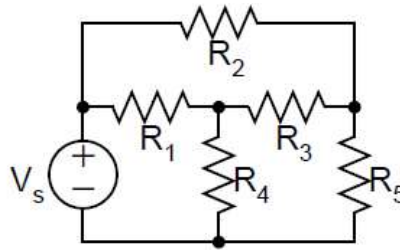


Fig 3.12 Test circuit for Mesh-current method

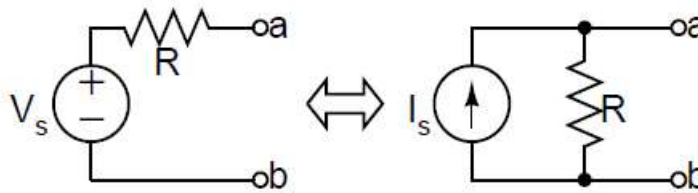


Fig 3.13 Source transformations

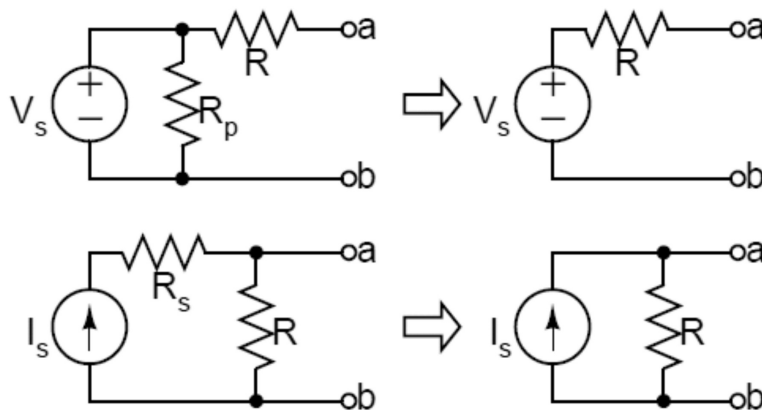


Fig 3.14 Equivalent circuits containing a resistor in parallel with a voltage source or in series with a current source

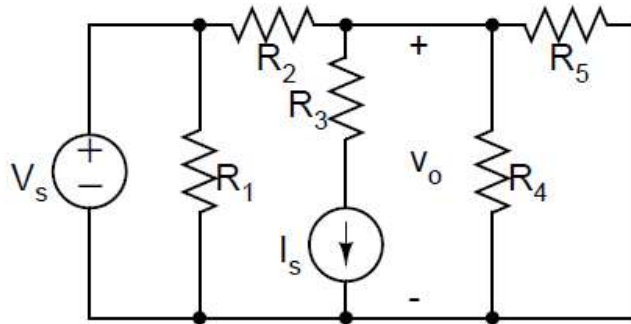


Fig 3.15 Test circuit for Source transformations

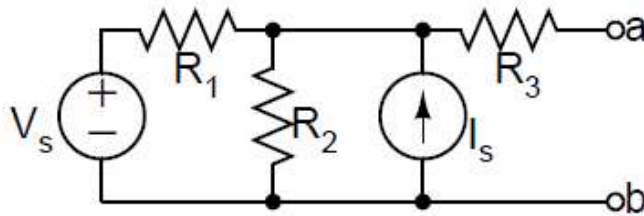


Fig 3.16 Test circuit for Thevenin equivalent

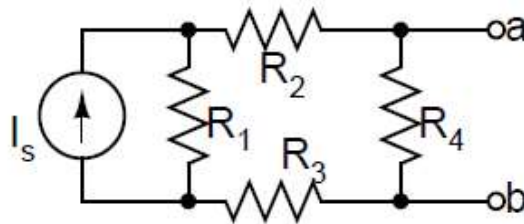


Fig 3.17 Test circuit for Norton equivalent

3.6.1 Software Test Techniques for System Fault-Tree Analysis

System fault-tree analysis is a technique for modeling dependability that is in widespread use. For systems that include software, the integration of software data into fault trees has proved problematic. In this section we discuss a number of techniques that can be used to make the assessment of software dependability by testing both more tractable and more suitable for use in system fault-tree analysis.

Introduction

Computers are introduced into applications for the many advantages that they provide.

But these advantages do not come without a price. The price is the complexity that the computer system brings with it. In addition to providing several advantages, the increased complexity has the potential for decreasing the dependability of the overall system. This can be dangerous in safety-critical systems where incorrect computer operation can be catastrophic.

For safety-critical systems, it is essential that various aspects of the dependability of the complete system, e.g., probability of failure per unit time, either be assessed or predicted before deployment. Assessment is usually performed by observing the system operating in a test environment. Predictions are usually obtained from mathematical models. The treatment of software has been a source of difficulty in the development of predictive models of computer-based systems. Acceptable quantification of a system's software components has proved elusive. In this section, we consider the problem of making system dependability predictions using system fault-tree models that include appropriate analysis of software. We focus in particular on how the results of software testing can be made a practical source of probabilistic data for fault-tree analysis. By employing a variety of techniques including restricting software's functionality and a very rigid software architecture, we show how various limitations in previous models can be overcome, and useful dependability predictions of complex systems produced.

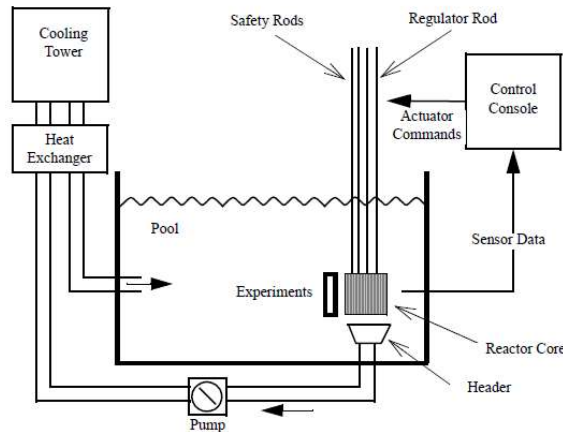


Fig 3.18 Reactor System

Fault Tree Analysis

System-fault-tree analysis is an important and widely used safety analysis technique, and is also the subject of active research. Using the design of a system and the failure probabilities (due to degradation faults) of its components, a system fault tree model is constructed and used to estimate the probability of occurrence of the various hazards that are of interest to the systems' designers.

The failure probabilities of a system's components are either measured or estimated.

The probability is estimated when it cannot be easily measured using life testing. An estimate is developed by viewing the component itself as a system made up of simpler components whose failure probabilities can be measured by life testing. These probabilities are then used in a model (frequently a Markov model) of the component of interest to produce the required estimate.

Fault-tree analysis of systems that include computers can treat the computer hardware much like other components. Computer systems can fail, however, as a result of software defects as well as hardware defects, and this raises the question about how the software "components" of a system can be included in a fault-tree model. In practice, this has proved difficult.

Fault-tree analysis is an important technology in the overall assessment of safety-critical systems. For it to be applied to computer based systems, however, software must be included in the fault-tree models. With software excluded or not treated appropriately, the results of fault-tree analysis are conditional on the system's software always working correctly—an assumption that is unwarranted.

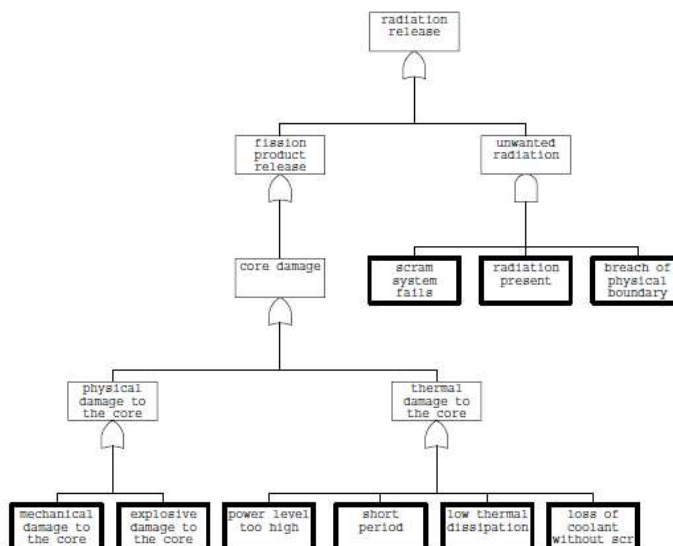


Fig 3.19

Top level reactor fault tree.

The upper part of the fault tree is used to show the hazards and some of the events that can cause them is shown in Figure above. The portion of the fault tree that is shown is just a small part of the whole model.

Extensive sub-trees are associated with the lowest level nodes shown in the figure, and within these sub-trees are many nodes—*many* nodes—whose proper analysis is critical to safe operation. The solid borders on the fault-tree nodes indicate that the associated node is not a leaf node.

The quantification associated with these nodes requires parametric information from software (in our experimental digital control system only) because the associated events occur as a result of software failure. The sub-tree associated with the event “loss of coolant without scram” (see Figure 2), for example, has an event that arises because of failures in the software that implements the following: *the scram logic, management of several sensors, sensor signal processing, shutdown logic, and shutdown device control.*

Software in System Fault Trees

In order to obtain the probabilistic data needed for fault-tree analysis, it is tempting to analyze software in the same way that hardware is analyzed—either as a black-box component whose failure probability can be measured by sampling the input space, i.e., life testing, or as a component whose structure permits modeling of its failure probability from its design.

Unfortunately, the quantification of software dependability by life testing has been shown to be infeasible in general for safety-critical systems. The reason is that an infeasible number of tests are

required to establish a useful bound on the probability of failure in the ultra-dependable range. The large number of tests derives from the number of combinations of input values that can occur. It is quite literally the case that for most realistic systems the number of tests required would take thousands of years to complete even under the most optimistic circumstances.

Also unfortunate is the fact that there are no general models that predict software dependability from the software's design—the type of Markov models used in hardware analysis do not apply in most cases. The reason for this is that the basic assumptions underlying Markov analysis of hardware systems do not apply to software systems. In particular the assumption that independent components in a system fail independently does not apply.

Faced with this situation, there are three directions that can be followed. The first is to somehow limit the effect that software can have on a system so that the system is less dependent on software for meeting its safety goals. We refer to this technique as *robust design*. If this could be done, satisfactory fault-tree analysis could be performed and satisfactorily safe systems developed without requiring that software meet extreme dependability goals and without having to show that such goals have in fact been met.

The second technique is to obtain the parameters needed for fault-tree analysis by some means other than testing or modeling. Many techniques exist, usually within the field of *formal methods*, that can show that a particular software system possesses useful properties without executing the software. If these properties could be used to establish the parameters necessary for fault-tree analysis, then the requirement of using testing and Markov models would be avoided.

Finally, the third technique to dealing with the problems of quantifying software performance for fault-tree analysis is to try to modify the test process in some way (or ways) so that what is now infeasible becomes feasible by changing the details of what has to be quantified by testing. We refer to this technique as *restricted testing*. We are developing a comprehensive approach to the treatment of software in system fault trees that exploits all three of these techniques—each in several ways.

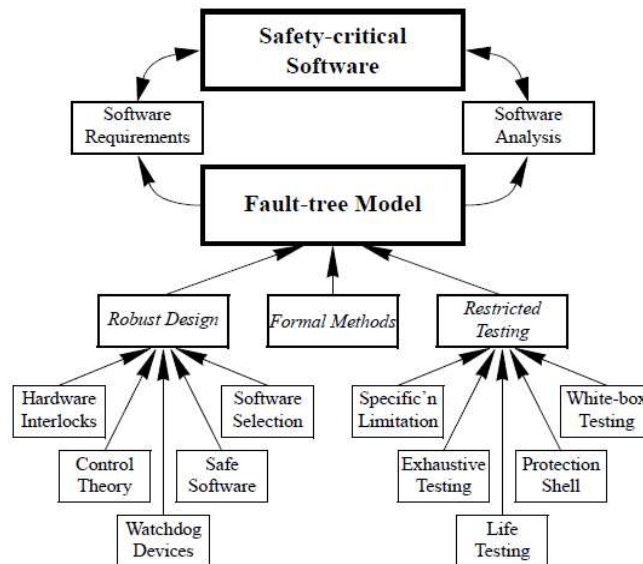


Fig 3.20

The overall approach is illustrated in the next Figure, and the various methods used within the three techniques are shown beneath them. We examine two of the three techniques that make up the approach in the following sections. Robust design is discussed only for completeness and therefore only briefly, and formal methods are omitted for the sake of brevity.

Comprehensive system fault-tree analysis

Robust Design

Refinement of a system's overall design is often undertaken with fault-tree analysis. If the hazard probabilities computed using a system fault tree are determined to be unacceptably high, system design changes or component replacements can be undertaken until the predicted probabilities are acceptable. The goal that we have with robust design is to use the *system-level* design to minimize the importance of software in the dependability analysis of the system. We illustrate this point using the following aspects of robust design:

Software selection: The process of design refinement includes the determination of which aspects of a system will be implemented in software. Although it is stating the obvious, we observe that where a function can be implemented satisfactorily using some technology other than software, the analytic challenges that software presents are reduced. In other words, step one is not to use software to the extent that this makes sense.

Avoidance of software-only nodes: Requiring that both a software failure and some other failure occur before a hazard can arise introduces an AND operator into a fault tree. This structure ensures that a software failure alone cannot lead to a hazard and reduces the dependability requirement on the software correspondingly. Various ways of introducing such conditions exist including hardware interlocks, watchdog devices such as timers, and various types of control-theory techniques that are stable even in the face of various types of implementation failure.

Safe programming: Changing the specification of a software element from requiring correct functionality to requiring either correct functionality *or no action* is a powerful tool in robust design. This technique is known as Safe Programming, and it permits software to be designed to be self checking rather than correct. Safe programming is far easier to implement and verify than full functionality.

EXERCISE

- 1) What are different troubleshooting techniques used in a majority of electronic systems?
- 2) Differentiate between divergent and convergent paths with diagram.
- 3) What are feedback paths? Explain the functions of feedback paths.
- 4) What are switching paths?
- 5) What preliminary checks should be carried out when equipment is received from repairs?

Troubleshooting of Computers: Components and Peripherals

Chapter

4

Instructional Objectives

- 4.1 Mother Board
- 4.2 Floppy Disk
- 4.3 Hard Disk Drive
- 4.4 CD ROM/DVD
- 4.5 Printers
- 4.6 Modems
- 4.7 Monitors
- 4.8 SMPs

4.1 Motherboard

A **motherboard** is the central **printed circuit board (PCB)** in some complex electronic systems, such as modern personal computers. The motherboard is sometimes alternatively known as the **main board**, **system board**, or, on Apple computers, the logic board. It is also sometimes casually shortened to **mobo**.

Modern motherboards include, at a minimum:

- **Sockets** (or slots) in which one or more microprocessors are installed.
- **Slots** into which the system's main memory is installed (typically in the form of DIMM modules containing DRAM chips).
- A **chipset** which forms an interface between the CPU's front-side bus, main memory, and peripheral buses.
- **Non-volatile memory chips** (usually Flash ROM in modern motherboards) containing the system's firmware or BIOS.
- A **clock generator** which produces the system clock signal to synchronise the various components.
- **Slots for expansion cards** (these interface to the system via the buses supported by the chipset).
- **Power connector flickers**, which receive electrical power from the computer power supply and distribute it to the CPU, chipset, main memory and expansion cards.

4.1.1 Troubleshooting of Mother Board

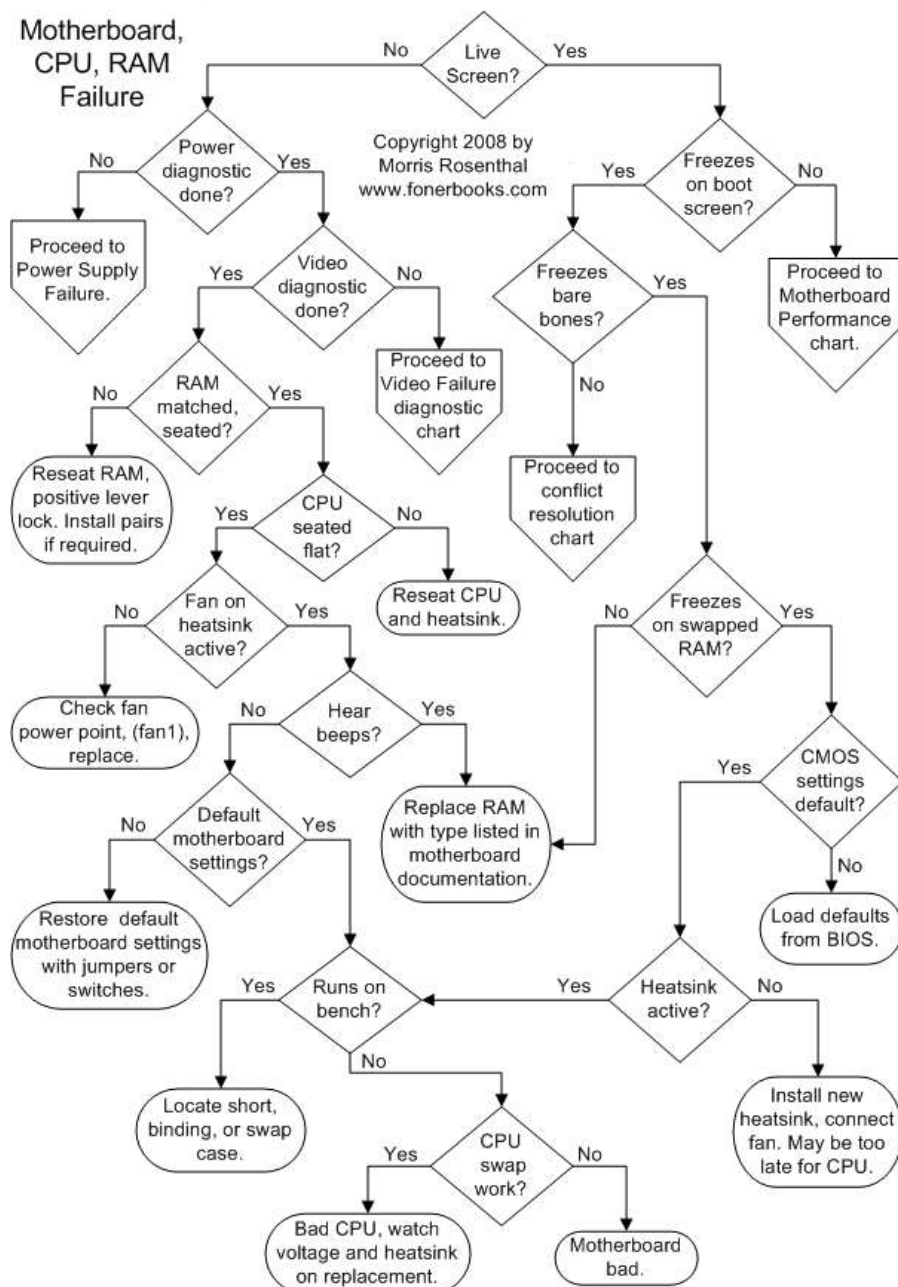


Fig: 4.1 Steps of Troubleshoot to Motherboard

Do you get a live screen? A message saying “No Video Signal” or anything similar doesn’t count as a live screen in this case. You need to get at least as far as a BIOS screen, either the system BIOS or an adapter BIOS loading.

Does the system power up? Do you hear any beeps, drives spinning up, fans, etc. If the power isn’t coming on, proceed to power supply failure. If the power supply diagnostics sent you back here, follow through these diagnostics as a double-check before giving up on the motherboard.

If you haven’t performed the video failure diagnostics for a dead screen yet, do so now. Don’t ignore the obvious steps, like checking the power cord and the outlet. If you skip the video diagnostics and continue with the motherboard flowchart, you could easily end up buying replacement parts for hardware that’s not bad.

One of the most common failures following motherboard or RAM upgrades is improper insertion of memory modules. The levers should be lowered before inserting the memory module, and should raise themselves up and lock in place when the module is correctly seated. If you’re using RIMM (Rambus Inline Memory Module) memory, the modules in a bank must be matched, and you must install CRIMMs (Continuity RIMMs) in the empty sockets. If you’re using older SIMM (Single Inline Memory Modules), each bank needs a matched pair. In both cases, matched doesn’t just mean capacity and speed, it also means manufacturer. I have a new page up for upgrading laptop memory with SODIMMs. For replacing regular DIMM memory, see the illustrated replacing RAM.

There are a number of reasons for a system with a good power supply to refuse to power up which were covered in the power supply diagnostics. Another reason is a failed CPU insertion, whether it’s a slot or socket CPU. With good lighting, using a flashlight if necessary, make sure that any socket CPU is sitting dead flat in the socket, which means that the heat sink should be perfectly parallel to the motherboard surface; the CPU may be so totally hidden beneath some heat sinks that you can’t see the edges. This problem should really only be relevant if you just upgraded your CPU or installed a new motherboard, because the CPU socket locks the CPU in firmly and the heat sink adds another level of clamping. If a socket CPU is a new install, you have to remove the heat sink and CPU to visually inspect it for damage such as crushed or bent legs. A CPU will not seat correctly if the socket locking arm wasn’t raised all the way up before the CPU was inserted, or wasn’t lowered all the way down after. If your CPU won’t sit down in the socket properly, either the socket is faulty or you have the wrong CPU for the motherboard! I haven’t seen a CPU creep out of a socket due to thermal shock for over a decade.

It’s pretty tough to tell if slot type CPUs are seated by visual inspection, so when in doubt, I reseat them. On the plus side, you can remove and reseat a slot CPU without removing the heat sink, since they form an integral unit. Make sure you correctly identify release levers on a slot CPU package, which are normally located at the top of the CPU package, to the inside of the motherboard support structure.

A **stone dead CPU** is another reason for a system to fail. All modern CPUs require a heat sink, and most of these are an active heat sink, with a fan on top. You may encounter a heat sink without a fan in mass-manufactured brand-name systems where the manufacturer had the engineering talent in-house to do a thorough thermal analysis and determined that the airflow over a passive finned heat sink was enough to keep the CPU within the operating temperature range. When there is a fan on the heat sink, it must be hooked up to the correct power point on the motherboard for the BIOS to monitor its condition and turn it off and on. If you just installed a new CPU and powered the system up with no heat sink, it may have failed already. If the fan on your active heat sink isn’t spinning up, replace it and

hope for the best. Make sure you see the new heat sink fan operating since it could be the power point on the motherboard that's failed.

If you have a system that powers up, the next question is, do you hear any beeps coming from the motherboard speaker. If your motherboard doesn't have an integrated piezoelectric speaker but does have a speaker connection next to the power and reset connections (usually the front, left-hand corner of the motherboard) attach a case speaker. If you hear an unending string of beeps, it's often bad RAM, while a repeated sequence can be RAM or video. Other beep codes have been largely abandoned since they pertained to non-user replaceable surface mount components. Beeps or no beeps, I always reseal the video adapter and the RAM, paying special attention to the locking levers on the memory sockets.

Are your motherboard settings on the defaults? Whether you just put in a new motherboard or have been fooling around with overclocking, restore the default settings. This is often accomplished with a single jumper or switch setting, but sometimes it involves moving several jumpers or switches. Get the default values from the motherboard documentation. If you can't find the original manual or locate the equivalent documentation on the Internet, you may have to skip this procedure. Sometimes, the silk screens on the motherboard are sufficiently detailed to work out the defaults, but you need really good eyes to figure it out.

Although we're repeating a little of the power supply diagnostics here, stripping down the system is the next step in a "no power-up" scenario. Unplug the power cord before each change in the case. Disconnect drives, once at a time, reconnecting power and trying power up after each. Next start removing adapters, saving the video adapter for last, reconnecting power and retrying after each change to ensure you discover which component is causing the failure.

Running the motherboard without a case is a common technique used by technicians to eliminate any weird grounding and shorting issues or mechanical stresses. It also makes it much easier to swap the CPU if that's required. I normally do my bench testing on top of a cardboard box, with a static free bag or foam between the bottom of the motherboard and the cardboard. You don't walk away from a test like this or you might come back to find the box on fire! If your motherboard powers up on the bench with the same power supply that you used in the case, you have a geometry problem. Ideally, you should have a spare power supply for bench testing if you're going to do regular repair and testing work.

Make sure some standoffs aren't higher than others, putting unacceptable stress on the motherboard. Check that every standoff appears under a screw hole. The easiest way to be sure is to count the standoffs, count the screws, and make sure there are no screws leftover after you install the motherboard. There could be a short caused by a misplaced standoff, a loose screw, metal chips from shoddy materials. I've encountered standoff shorts that produce an endless string of beeps like RAM failure, without damaging the motherboard. There's also the possibility that the case geometry is so messed up (out of square or level when the cover is forced on) that it's putting an unacceptable mechanical stress on the motherboard resulting in an open circuit. If you can't find the cause of the problem, don't hesitate to try another case and power supply.

If you still have a "no power" situation with the motherboard running out of the case, there's always the last refuge of a scoundrel. Swap in a known good CPU not forgetting to install a good heat sink and to connect the fan, even just for a quick test. I try to keep around some cheap old CPUs for this purpose, just in case the motherboard is a CPU eater. It's another good reason to leave all the motherboard settings on the default "Automatic" setting, so you don't have to fool around with them at this stage. If your old CPU is bad and the heat sink fan is dead, it's a pretty sure bet that the dead fan caused the CPU

failure. If the heat sink fan is working, determining whether the CPU failure was due to poor heat sink contact, improper motherboard settings, or lousy power regulation from the motherboard is a guessing game. If the motherboard is an older make and you have a couple bucks to spare, replace the CPU and the motherboard together. Replacing just the CPU, even if the motherboard tests out OK, is kind of risky and usually tough to justify from a price/performance standpoint unless the system was practically new, say less than a half a year old.

If you still have a no power situation, not to mention no beeps and no video, you're probably looking at a bad motherboard. Again, this diagnosis assumes that you went through the Video Failure diagnostics, which would have forced you through the Power Supply Failure diagnostics as well. I still wouldn't be in a hurry to take a gun to the motherboard. Get your system operating with a replacement motherboard and all the identical parts that the old motherboard failed with before you make the trash can decision. I just added some illustrated instructions for replacing a motherboard to this site, including installing a new motherboard.

Does the system power right up, give a happy beep or two, then freeze on the BIOS screen? This can occur on an all text screen, during or after memory count, while checking for drives, or the feared "Verifying DMI Data Pool." The problem is very likely due to a conflict, most like between the adapters but also possibly between incompatible drives sharing a bus.

Strip the system down to bare-bones, just a power supply, motherboard, minimum RAM, CPU and heat sink, and video adapter. If the system no longer freezes when it's stripped down, but complains about the lack of a boot device, proceed to Conflict Resolution.

Try swapping the RAM around, reordering the banks if you have more than one bank of RAM installed, or moving the only module installed to a neighboring slot. If this doesn't cure the freeze-up, and you have some suitable known good RAM from another system, try it. If the RAM currently installed doesn't meet the motherboard manufacturer specs, you shouldn't be using it; even if it seemed to work until this point. Improperly selected RAM can be the cause of problems ranging from no-boot to intermittent lock-ups. Is the RAM seated correctly and in the proper quantities? (i.e., number of modules, addition of continuity modules, or CRIMMs, if you are using RIMMs). Also make sure that the system didn't use tinned (silver colour) contacts against gold contacts, or the dissimilar metals will cause corrosion over time due to a constant electrical current when the power is off. Replacing RAM at this point isn't a guaranteed proposition, but it's a good item to eliminate. Don't toss out the RAM you remove because you may find out later that it's actually good.

If you aren't using the default **CMOS** settings, try restoring them all at this point. You can usually restore these from a major CMOS menu item like "Restore Default Settings" or "BIOS Default Settings." The default settings usually put everything on autodetect and use the recommended timing for the RAM. This means if you're overclocking, stop it, at least until you get the system running again. It doesn't matter whether or not overclocking the exact same CPU or RAM in a friend's system worked without a hitch, you're exceeding the manufacturers recommendations so it's a gamble.

An overheating will cause the system to quickly lock up. Remove the existing heat sink and fan, make sure that the fan is working properly and that the geometry of the bottom of the heat sink will bring it in full contact with the exposed CPU die or the top of the CPU package. See my illustrated guide for how to replace a CPU. Apply an approved thermal grease or thermal tape before reinstalling the heat sink. Don't put on too much thermal grease or you'll just make a mess. The thermal media is only there to fill the microscopic gaps between the die surface and the heat sink. Don't improvise your thermal

material, go to a computer or electronics store and buy some. Installing heat sinks can be frustrating, but this isn't a "bash away at it" process. You can damage the CPU if you start cracking the heat sink against it in an attempt to get the heat sink to sit right. Be patient, study the mechanical connections, make sure you aren't hitting some poorly placed component on the motherboard and check that your heat sink isn't so oversized it just won't fit on the particular motherboard.

Make sure the fan on that heat sink spins up the second that power comes on. If it doesn't, despite being connected to the correct power point (see the motherboard manual), replace it with a new active heat sink unit. Make sure the bottom surface of the new unit will make full contact with the exposed CPU die or the top of the CPU package. The only problem with replacing an active heat sink is it may be too late for your CPU. CPUs have an unfortunate tendency to damage themselves when they overheat. Some CPUs can go into thermal runaway and destroy themselves in a matter of seconds without proper cooling.

4.2 Floppy Disk Drive (FDD)

A **floppy disk** is an obsolete data storage medium that is composed of a disk of thin, flexible (floppy) magnetic storage medium encased in a square or rectangular plastic shell. Floppy disks are read and written by a **floppy disk drive** or **FDD**, the initials of which should not be confused with "fixed disk drive," which is another term for a (non-removable type of) hard disk drive. Invented by IBM, floppy disks in 8-inch (200 mm), 5¼-inch (131¼ mm), and the newest and most common 3½-inch (87½ mm) formats enjoyed many years as a popular and ubiquitous form of data storage and exchange, from the mid-1970s to the late 1990s. They have now been superseded by USB flash drives, CD-ROMs and DVD-ROMs.

Floppy sizes are almost universally referred to in imperial measurements; even in countries where metric is the standard, and even when the size is in fact defined in metric (for instance the 3½-inch floppy, which is actually 87½ mm). Formatted capacities are generally set in terms of binary kilobytes (as 1 sector is generally 512 bytes).

Historical sequence of floppy disk formats, including the last format to be generally adopted — the "High Density" 3½-inch HD floppy, introduced 1987.			
Disk format	Year introduced	Formatted Storage capacity (in kB = 1024 bytes if not stated)	Marketedcapacity
8-inch - IBM 23FD (read-only)	1971	79.7	?
8-inch - Memorex 650	1972	175 kB	1.5 megabit [unformatted]
8-inch – SSSD IBM 33FD / Shugart 901	1973	237.25	3.1 Mbits unformatted
8-inch – DSSDIBM 43FD / Shugart 850	1976	500.5	6.2 Mbits unformatted

5¼-inch (35 track)	1976 Shugart SA 400	89.6 kB	110 kB
8-inch DSDD IBM 53FD / Shugart 850	1977	980 (CP/M)- -1200 (MS-DOS FAT)	1.2 MB
5¼-inch DD	1978	360 or 800	360 KB
3½-inch HP single sided	1982	280	264 kB
3-inch	1982	360	125 kB (SS/SD), 500 kB (DS/DD)
3½-inch (DD at release)	1984	720 (400 SS, 800 DS on Macintosh, 880 DS on Amiga)	1 MB
5¼-inch QD		720	720 KB
5¼-inch HD	1982 YE Data YD380	1,182,720 bytes	1.2 MB
3-inch DD	1984	720	?
3-inch Mitsumi	1985	128 to 256	?
2-inch	Quick Disk 1985	720	?
5¼-inch Perpendicular	1986	100 MB	?
3½-inch HD	1987	1440	1.44 MB
3½-inch ED	1987	2880	2.88 MB
3½-inch Floptical (LS)	1991	21000	21 MB
3½-inch LS-120	1996	120.375 MB	120 MB
3½-inch LS-240	1997	240.75 MB	240 MB
3½-inch HiFD	1998/99	150/200 MB	150/200 MB

Abbreviations: DD = Double Density; QD = Quad Density; HD = High Density; ED = Extended Density; LS = Laser Servo; HiFD = High capacity Floppy Disk; SS = Single Sided; DS = Double Sided
¹ The formatted capacities of floppy disks frequently corresponded only vaguely to their capacities as marketed by drive and media companies, due to differences between formatted and unformatted capacities and also due to the non-standard use of binary prefixes in labeling and advertising floppy media. The erroneous “1.44 MB” value for the 3½-inch HD floppies is the most widely known example
Dates and capacities marked? are of unclear origin and need source information; other listed capacities refer to: Formatted Storage Capacity is total size of all sectors on the disk:
• For 8-inch see Table of 8-inch floppy formats IBM 8-inch formats. Note that spare, hidden and otherwise reserved sectors are included in this number. • For 5¼- and 3½-inch capacities quoted are from subsystem or system vendor statements.
Marketed Capacity is the capacity, typically unformatted, by the original media OEM vendor or in the case of IBM media, the first OEM thereafter. Other formats may get more or less capacity from the same drives and disks.

Table: 4.1

4.2.1 Trouble shooting of FDD

Issue:

Basic floppy disk drive troubleshooting.

Cause: A floppy drive may not work because of one or more of the below reasons:

1. Bad floppy diskette.
2. Not setup in CMOS.
3. Confliction with other hardware.
4. Not connected properly.
5. Bad drivers.
6. Bad hardware.

Solution:

4.2.1.1 Bad Floppy Diskette

Verify that the floppy diskette that you are attempting to read from is not writing protected or bad. Verify that the diskette is not writing protected by sliding the tab into the position not allowing light to shine through it. If you do not have a tab place tape over this hole.

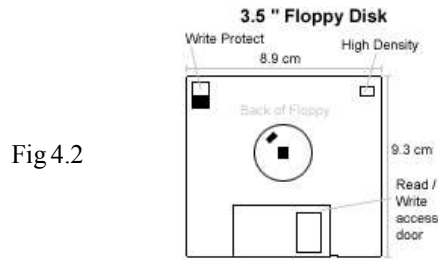


Fig 4.2

Because of the technology of floppy diskette drives, it is likely for floppy diskettes to easily become bad. Verify that other floppy diskettes are not exhibiting the same issue.

If other floppies work it is likely that you may have a bad floppy diskette.

4.2.1.2 Not Setup in CMOS

Verify that the floppy drive is properly setup in CMOS. If the floppy drive is not setup properly you may experience read / write errors or the floppy may not work at all. Most computers need to have the floppy setup as a 3.5, 1.44MB.

4.2.1.3 Conflicition with other hardware

If you have recently physically installed any new hardware such as a tape drive or other backup medium, temporarily disconnect that new hardware to ensure that it is not the cause of your floppy drive not working.

4.2.1.4 Not Connected Properly

- Power down, unplug, and open computer, being aware of ESD and its potential dangers.
- Verify that the floppy connection is connected to the motherboard FDD connector. If it appears to be connected, disconnect and reconnect cable to verify cable is seated properly.
- Verify that the floppy cable coming from the motherboard is connected to the back of the floppy drive. If connected, disconnect and connect the floppy drive cable to verify seated properly.
- Verify that a power connection is also connected to the back of the floppy drive.

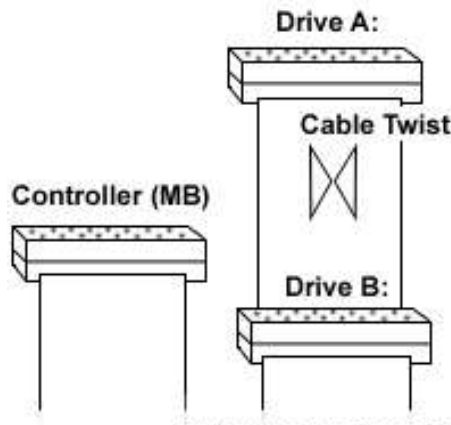


Fig 4.3

- If your floppy cable has more than one connection, verify that you have connected the floppy to the appropriate connection. The above figure illustrates what drive should be connected where.

4.2.1.5 Bad Drivers

If you are not able to read or write to a floppy diskette from Windows, verify that the computer is not exhibiting floppy drivers issues by testing the floppy drive from MS-DOS.

If you are running Windows 3.x click File and click Exit Windows to get to an MS-DOS prompt.

If you are running Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, or Windows 2000 click Start / Shutdown and restart the computer to a MS-DOS prompt.

Once at the prompt, place a diskette into the floppy disk drive and type **format a:** if you get:

Invalid Media or Track 0 Bad = Attempt to format another floppy disk.

Write Protect Error = Ensure that the disk is not write protected by removing the floppy disk and insuring that you cannot see through both holes; if you can, move the tab in the left hand side down (looking from the back of the floppy) and try again. If the disk is not write protected try another floppy disk.

Invalid Drive Specification = Ensure that you floppy drive is setup properly in CMOS.

If the floppy disk drive formats properly in MS-DOS but does not format in Windows, it is likely that Windows or a program within Windows is preventing the floppy drive from working. If you continue to experience the same issues we recommend that Windows be reinstalled.

4.2.1.6 Bad Hardware

If you continue to experience issues after following the above steps it is likely that hardware within the computer is bad. Attempt to replace the following hardware in the computer in the below order.

1. Replace the floppy data cable which connects the computer floppy drive to the motherboard \ I/O board.
2. Replace the floppy if the floppy data cable did not resolve your issues.
3. Replace or request that the motherboard \ I/O board be replaced.

4.3 Hard Disk Drive (HDD)

A **hard disk drive (HDD)**, commonly referred to as a **hard drive**, **hard disk**, or **fixed disk drive**, is a non-volatile storage device which stores digitally encoded data on rapidly rotating platters with magnetic surfaces. Strictly speaking, “drive” refers to a device distinct from its medium, such as a tape drive and its tape, or a floppy disk drive and its floppy disk. Early HDDs had removable media; however, an HDD today is typically a sealed unit (except for a filtered vent hole to equalise air pressure) with fixed media.

HDDs (introduced in 1956 as data storage for an IBM accounting computer) were originally developed for use with general purpose computers. In the 21st century, applications for HDDs have expanded to include digital video recorders, digital audio players, personal digital assistants, digital cameras and video game consoles. In 2005; the first mobile phones to include HDDs were introduced by Samsung and Nokia. The need for large-scale, reliable storage, independent of a particular device, led to the introduction of embedded systems such as RAID arrays, network attached storage (NAS) systems and storage area network (SAN) systems that provide efficient and reliable access to large volumes of data.

4.3.1 Form Factors

The earliest “form factor” hard disk drives inherited their dimensions from floppy-disk drives (FDDs), so that either could be mounted in chassis slots, and thus the HDD form factors became colloquially named after the corresponding FDD types. “Form factor” compatibility continued after the 3½ inch size even though floppy disk drives with new smaller dimensions ceased to be offered.

- **8 inch:** 9.5 in × 4.624 in × 14.25 in (237.5 mm × 116.6 mm × 1356.25 mm)

In 1979, Shugart Associates’ SA1000 was the first form factor compatible HDD, having the same dimensions and a compatible interface to the 83 FDD. Both “full height” and “half height” (2.313 in) versions were available.

- **5.25 inch:** 5.75 in × 1.63 in × 8 in (143.75 mm × 40.75 mm × 260 mm)

This smaller form factor, first used in an HDD by Seagate in 1980, was the same size as full height 5¼-inch diameter FDD, i.e., 3.25 inches high. This is twice as high as “half height” commonly used today; i.e., 1.63 in (40.75 mm). Most desktop models of drives for optical 120 mm disks (DVD, CD) use the half height 5¼3 dimension, but it fell out of fashion for HDDs. The Quantum Bigfoot HDD was the last to use it in the late 1990s, with “low-profile” (H”25 mm) and “ultra-low-profile” (H”20 mm) high versions.

- **3.5 inch:** 4 in × 1 in × 5.75 in (100 mm × 25 mm × 143.75 mm) = 357.5cm³

This smaller form factor, first used in an HDD by Rodime in 1984, was the same size as the “half height” 3½3 FDD, i.e., 1.63 inches high. Today has been largely superseded by 1-inch high “slimline” or “low-profile” versions of this form factor which is used by most desktop HDDs.

- **2.5 inch:** 2.75 in × 0.374–0.59 in × 3.945 in (68.75 mm × 9.35–14.75 mm × 98.625 mm) = 66.3575cm³–104.775cm³

This smaller form factor was introduced by PrairieTek in 1988; there is no corresponding FDD. It is widely used today for hard-disk drives in mobile devices (laptops, music players, etc.) and as of 2008 replacing 3.5 inch enterprise-class drives. Today, the dominant height of this form factor is 9.5 mm for laptop drives, but high capacity drives have a height of 12.5 mm. Enterprise-class drives can have a height up to 15 mm.

- **1.8 inch:** 54 mm × 8 mm × 71 mm = 30.672cm³

This form factor, originally introduced by Integral Peripherals in 1993, has evolved into the ATA-7 LIF with dimensions as stated. It is increasingly used in digital audio players and subnotebooks. An original variant exists for 2–5 GB sized HDDs that fit directly into a PC card expansion slot. These became popular for their use in iPods and other HDD based MP3 players.

- **1 inch:** 42.8 mm × 5 mm × 36.4 mm

This form factor was introduced in 1999 as IBM’s Microdrive to fit inside a CF Type II slot. Samsung calls the same form factor “**1.3 inch**” drive in its product literature.

- **0.85 inch:** 24 mm × 5 mm × 32 mm

Toshiba announced this form factor in January 2004 for use in mobile phones and similar applications, including SD/MMC slot compatible HDDs optimised for video storage on 4G handsets. Toshiba currently sells a 4 GB (MK4001MTD) and 8 GB (MK8003MTD) version and holds the Guinness World Record for the smallest harddisk drive.

Major manufacturers discontinued the development of new products for the 1-inch (1.3-inch) and 0.85-inch form factors in 2007, due to falling prices of flash memory, although Samsung introduced in 2008 with the SpinPoint A1 another 1.3-inch drive.

The inch-based nickname of all these form factors usually do not indicate any actual product dimension (which are specified in millimeters for more recent form factors), but just roughly indicate a size relative to disk diameters, in the interest of historic continuity.

4.3.2 Troubleshooting of Hard Drive

When a hard disk fails, the computer doesn't boot, as in the case of a boot drive failure, and the frenzy to save important company data ensues. When faced with such a problem, don't panic. Just remember these simple hard drive troubleshooting tips.

Seven Steps to Troubleshooting Hard Drives: Here's a quick and proven hard disk troubleshooting process. With each point, ask yourself the question(s) that follow.

- 1. Physical Connectivity** - Is the drive receiving power? Is it plugged into the PC by a correctly connected ribbon cable? For IDE drives, are its jumpers set correctly? Or with SCSI drives, are its SCSI termination and ID set correctly?
- 2. BIOS Setup** — Does the BIOS see the drive?
- 3. Viruses** — Does the drive contain any boot sector viruses that need to be removed before continuing?
- 4. Partitioning** — Does FDISK find a valid partition on the drive? Is it active?
- 5. Formatting** — Is the drive formatted using a file system that the OS can recognise?
- 6. Drive Errors** — Is a physical or logical drive error causing read/write problems on the drive?
- 7. Operating System** — Does your OS have a feature that checks the status of each drive on your system? If so, what is that status?

4.3.2.1 Checking Physical connectivity

To work properly, a hard drive needs power and a connection via a ribbon cable to the PC. If a drive doesn't work after moving it to a new PC, after physically moving the PC, or after the cover has been taken off, start your troubleshooting by checking the physical connectivity. It's possible for plugs to jiggle loose when moving a PC, and it's easy to uproot a ribbon cable connection when pulling circuit boards or performing other maintenance tasks inside the case.

A hard disk works with any Molex connector from the PC's power supply. Make sure the plug is fully inserted. Molex connectors require a lot of pressure to fully insert, and even more pressure to remove, so don't be afraid to push hard or pull, as the case may be. Just make sure you handle the plastic connector, and do not try to push or pull the wires.

As the PC starts up, place the palm of your hand on the flat part of the hard disk. If you can detect any vibration, the drive probably has power. If there's no movement at all, either the drive's physical mechanism is shot or the Molex connector you have selected is faulty. Try using a different connector before assuming the drive has a problem.

Systems like the AT/LPX have a small connector that runs from the front of the case to the hard disk. On ATX systems, it runs from the motherboard to the hard disk. This enables the LED on the case

to illuminate when the hard disk is in use. Don't rely on that LED as a positive indicator as to whether the hard disk is receiving power. The light could be burned out, the wire disconnected, or the drive might be receiving power but not be connected correctly to the PC.

The other physical requirement for a drive is the PC itself. If it's an IDE model, the drive should be connected via a ribbon cable to the IDE bus on the motherboard. Connections can also be made with a SCSI or proprietary expansion card. Secure both ends of the ribbon cable connector and make sure the connector is covering all pins. On systems where the pins are bare instead of surrounded by a plastic ridge, it's easy to offset the connector by a row or two on the pins. If the drive is getting power but the BIOS can't find it, try a different ribbon cable; the one in use might have a broken wire or other flaw.

Note that there are different types of hard disk ribbon cables. Ultra DMA 66 and above drives require 80-wire cables. If you use the 40-wire type, the drive will be limited to Ultra DMA 33 performance.

The red stripe on the ribbon cable must match up with Pin 1 on both the drive and the motherboard or expansion card. Sometimes, though, it's not easy to locate Pin 1. Look for tiny numbers at one end of the connector. If you see a 1 or 2, that's the end with which the red stripe should be matched. Some connectors are notched on one side while the ribbon cables have a tab that fits into that notched area. However, this isn't always the case. Unlike with floppy drives, where the drive light stays on even if you have the ribbon cable backward, there is no simple way to tell whether you have the cable backwards. Without the notched connectors, your only choice is to use the trial-and-error method.

4.3.2.2 Checking Jumper Settings

On an IDE hard disk, one or more jumpers on the drive must be set to determine its Master/Slave status. This setting isn't usually an issue in an existing hard disk installation that suddenly doesn't work anymore, but it can cause problems when you move a drive from one PC to another.

Depending on the drive, the following jumper settings may be available:

Single: Use this setting when the drive is the only one on that IDE subsystem; that is, the only one on that ribbon cable. Not all drives have a Single setting; if there is none, use the Master setting instead.

Master (MS): When there are two drives on the IDE subsystem and the other drive's jumpers are set to Slave, or if this is the only drive on the subsystem and it doesn't have a separate Single setting, use this setting.

Slave (SL): Use this setting when there are two drives on the IDE subsystem and the other drive's jumpers are set to Master.

Cable Select (CS): If you are using a cable that relies on the device positioning to determine its Slave/Master status, use this setting. This setting is uncommon.

4.3.2.3 Checking SCSI Termination

If the machine uses a SCSI drive, there are two factors with which to be concerned: termination and ID. These settings are not an issue when troubleshooting a drive that has suddenly gone bad in an existing system, but if you are moving a drive from one system to another and it doesn't work in the new system, improper SCSI settings may be the culprit.

If this is the last SCSI device in the chain, it must be terminated. Termination methods vary. On some devices, you set termination with an extra jumper; on others, you use a cap or plug over a connector. On most hard disks, you terminate using a jumper setting.

SCSI-based drives usually have jumpers just like ATAPI ones, but instead of setting the Master/Slave status, they assign a SCSI ID number to the device. Some SCSI devices have a wheel or button instead of jumpers with a little window indicating the setting, but this is uncommon on a hard disk.

There can be up to seven SCSI devices on a single narrow SCSI bus, and up to 15 devices on a wide SCSI bus. There are either eight or 16 addresses in total, depending on your system. The host adapter takes one of those addresses, leaving seven or 15 for the remaining drives. Usually, the host adapter claims the highest number for itself.

The SCSI ID comes from a binary representation of the jumpers. For example, on a device with three SCSI jumpers and all of them are without jumper settings, the ID would be 000b (b stands for binary here), or 0. An ID of 001b would be 1; 010b would be 2; and so on.

The problem lies in the fact that some manufacturers set the jumpers to read from left-to-right, while others use right-to-left. So on one drive, the leftmost jumper set would be 1, while on some other drive, the rightmost jumper set would be 1. Check the drive's label for information about which way the drive works. If all else fails, try the manufacturer's Website.

4.3.2.4 Checking BIOS Setup (IDE only)

In most modern systems, the **BIOS** can automatically detect your hard disk, so no special BIOS setup is required. However, if you are working with an older or quirky BIOS, you might need to enter the BIOS setup programme and change the drive's IDE channel (such as Primary Master or Primary Slave, for example) from None to Auto so the BIOS will attempt to find and identify the drive.

On an old BIOS, you occasionally may need to select user as the drive type and manually enter the drive's settings. Automatic detection of IDE devices was part of the ATA-3 standard, released more than 10 years ago, though, doing so would be rare.

Some BIOSs also have a separate detect IDE Devices utility built in. If the BIOS contains such a utility, you can use it to prompt the BIOS to detect the new hard disk. This comes in handy when you aren't sure whether or not the drive is working, because you can get an answer immediately rather than rebooting and waiting to see whether the BIOS finds the drive on startup.

4.3.2.5 Virus Checking

If you've come this far in the troubleshooting process and the drive still isn't working, check for viruses. A drive containing a boot-sector virus will not only malfunction, it can spread the virus to the disk you boot from, such as your emergency startup disk.

On a system that you know is good and that has an anti-virus program installed, update the virus definitions, and then make a virus-checking boot disk. Write protect it, and then use it to start the system containing the nonworking hard disk and check it for errors. If the drive is not partitioned and formatted, the boot disk might not be able to check the data area of the drive. That's okay for now; just let it get as far as it can before moving on to the next step, checking the partition.

4.3.2.6 Checking for a Valid Partition

If the BIOS can see the drive but the drive isn't working, make sure the drive is partitioned. Use FDISK, a command-line utility you'll find on a Windows 9x/Me startup disk, to check. Boot from the write-protected startup disk and type FDISK. When asked whether or not you want large disk support, type Y.

If the active partition's type is FAT, FAT32, or NTFS, it should be recognised by the operating system. One exception would be if you put an NTFS drive into a Windows 9x/Me system. The OS wouldn't recognise the NTFS because it doesn't support NTFS, not because it was partitioned incorrectly.

If it is a partition problem, you have two choices: Try to recover the data using a disk recovery programme, or give up on the data, delete the partition, and re-create it in FDISK. If you want to try recovery first, see the section below on Advanced Data Recovery Options.

If you want to delete the partition and recreate it, return to the FDISK main screen by pressing [Esc] and deleting the partition (option 3 on the screen), and then return to the main screen again and create a partition (option 1 on the screen). After using FDISK to create or delete partitions, you must reboot the machine before doing anything else.

4.3.2.7 Checking Drive Formatting

If FDISK recognizes the drive and it has a valid partition type, you should be able to view the drive's content from a command prompt via your startup disk, or from the Recovery Console in Windows 2k or XP. Change to that drive by typing its drive letter followed by a colon and pressing [Enter]. Then, display a list of files on the drive with the DIR command.

If you see a message about an invalid media type, the drive is probably not formatted using a file system that your OS recognises. You can either try a data recovery program, or you can give up on the drive's data and reformat it with the FORMAT command.

4.3.2.8 Fixing Physical and Logical Drive Errors

Let's assume at this point that your OS finds the drive and can read some files on it, but not all of them. Maybe you're receiving read or write errors, or certain programmes aren't working right. The problem is likely a physical or logical disk error.

A physical disk error is a bad spot on the drive. It can result from physical trauma to the computer, like knocking it off of a table while it's running.

A logical disk error is a discrepancy between the two copies of the file allocation table (FAT) on the disk, or a discrepancy between the FAT's version of what clusters are stored on the drive and the reality of actual storage. Such errors are typically caused by improperly shutting down the PC or abnormal program termination.

A message about a data error while reading or writing the drive is probably a physical error. Logical errors are manifested in many different ways, not always directly attributable to the disk itself. For example, certain programmes might fail to run or might lock up after starting. Such a problem could mean a memory parity error or even a bad cooling fan; you never know until you check the system and eliminate the possibilities.

It's best to try the simplest solution first, so run a disk-checking programme. Windows 9x/Me/2k comes with ScanDisk, which will check for both physical and logical errors. Windows XP comes with a similar utility called *Check Disk*. In Windows XP, access Check Disk from the Tools tab of the drive's Properties sheet. In early versions of DOS, a command-line utility called CHKDSK does the same thing. Use it with the /F switch to fix any errors it finds.

4.3.2.9 Checking and Reactivating Disks in the Windows 2k/XP Oss

Windows 2k and Windows XP both have a Disk Management feature that checks the status of each drive on your system. This utility allows you to convert to dynamic disks, change space allocation, and much more.

With Disk Management, the most important thing to check is the status of each drive. The Windows Disk Management application will display the drive's status. If a drive reports that it is offline or a status other than healthy, right-click it and choose Reactivate Disk.

4.4 CD ROM/ DVD

CD-ROM drives are necessary today for most programs. A single CD can store up to 650 MB of data (newer CD-Rs allow for 700 MB of data, perhaps more with "overburn"). Fast CD-ROM drives have been a big topic in the past, but all of today's CD-ROM drives are sufficiently fast. Of course, it's nice to have the little bits of extra speed. However, when you consider CD-ROM drives are generally used just to install a programme or copy CDs, both of which are usually done rarely on most users' computers, the extra speed isn't usually very important. The speed can play a big role if you do a lot of CD burning at high speeds or some audio extraction from audio CDs (i.e. converting CDs to MP3s).

CD-R/RW (which stands for Recordable / Re-Writable) drives (aka burners, writers) allow a user to create their own CDs of audio and/or data. These drives are great for backup purposes (backup your computer's hard drive or backup your purchased CDs) and for creating your own audio CD compilations (not to mention other things like home movies, multimedia presentations, etc.).

DVD-ROM drives can store up to 4 GB of data or about 6 times the size of a regular CD (not sure on the exact size, but suffice to say it's a very large storage medium). DVDs look about the same and are the same size as a CD-ROM. DVD drives can also read CD-ROM drives, so you don't usually need a separate CD-ROM drive. DVD drives have become low enough in price that there isn't much point in purchasing a CD-ROM drive instead of a DVD-ROM drive. Some companies even make CD burner drives that will also read DVDs (all in one). DVD's most practical use is movies. The DVD format allows for much higher resolution digital recording that looks much clearer than VCR recordings.

DVD recordable drives are available in a couple of different formats — DVD-R or DVD+R with a RW version of each. These are slightly different discs and drives (although some drives support writing to both formats). One is not much better than the other, so it really boils down to price of the media (and also availability of the media).

The most basic and potentially most disastrous problem that can occur with a CD or DVD drive is a stuck tray. Will the tray eject when you press the eject button? Press it once, like a doorbell, and then move your finger away, or you may be sending it repeated open and close commands. The drive won't pop right open if it is actively playing a disc, and the operating system may be able to override the stop and open command. If you're trying to eject a music CD using Media Player software (clicking on a software eject button on the screen) and it doesn't work, try the manual button on the drive. If this is a newly installed drive, make sure you used the short screws shipped with the drive and not longer screws which can jam the mechanism. If there's a disc in the drive that can no longer be read, make sure the power supply lead is still seated in the socket on the back of the drive.

Shut down, restart, and try again. If the tray still doesn't eject, reboot again and note whether the BIOS registers the drive. Some brand name PCs don't report installed hardware on a boot screen, so you'll have to access CMOS Setup to check. If the BIOS doesn't register the drive, it may have dropped dead. I've seen CD recorders as cheap as \$19.95 and CD players for less, so you know they aren't built to last forever. Proceed to IDE Drive Failure if the BIOS no longer registers the drive.

Assuming the drive is still registered by the BIOS and operating system, you really do have a stuck disc. The next step is to look for a pinhole on the front of the CD or DVD drive. Power down the system and unplug the power cord, then straighten out a couple inches worth of paper clip, the heaviest gauge that will fit in the hole. Gently push the paper clip straight into the hole, until you feel it depress the release mechanism. This will sometime cause the tray to pop out a fraction of an inch, other times you will have to pry it a little to get it started. Once you have enough tray sticking out to grab it with your fingers, you should be able to pull it out, though it can offer quite a bit of resistance, and you may damage whatever disc is inside. If the faceplate seems to be bulging as you pull, the disc is hung up on it, and the best thing to do is remove the drive from the PC and then remove the faceplate.

The faceplate is normally held on by simple plastic clips working from the inside out. Gently depress them into the side of the drive while removing the faceplate so you don't break them off. If you have removed the drive from the system, tried the manual pinhole release, removed the faceplate and still can't get the disc out, you have a problem. I've taken whole drives apart with no luck. If there's a mechanical failure, it probably isn't repairable without access to parts. At this point, I usually just pry and pray. If I had a DVDR worth several hundred dollars, I'd consider sending it out.

Does the drive read discs? When you mount a disc, be it software or music, does the drive acknowledge that a disc is present and let you view the contents? It doesn't matter (at this point) whether or not you can get through installing the software on the disc or read all of the information. The question is simply, can the drive see anything at all on the disc?

Do you have CD and DVD drives installed? It's easy enough to mix up drives on a PC, and a CD drive isn't going to have much luck reading a DVD. A CD recorder along with a DVD player is a common two drive combination, but the DVD may not be able to read CDs recorded just two inches away. See CD or DVD recording problem if you're having trouble reading a recorded disc. Some older systems have both a CD ROM (reader) and a CDR (recorder).

Are you reading the right drive? If you have two physical drives, make sure the operating system is actually looking at the drive the CD or DVD has been placed in. Trust me, I've been fooled myself into opening up a machine by blind belief in the wrong drive letter. Most drives have an activity LED that tells you when the drive is active. Make sure the activity LED is lighting up on the drive you put the disc in when you try to read it.

Does the drive read other discs? Try another disc, a factory CD in CD ROMs or CDRs or a factory DVD in DVD ROMs or DVDRs. If it works, the problem is with the media and not the drive. Make sure the disc you can't read is the right type for the drive your are trying it in, ie, CD, DVD, CDR, DVDR, noting that many of the recordable discs won't be readable in other players. Clean the disc with a soft bit of flannel. The discs are plastics, so don't use solvents. Scratches can render a disc unreadable, including scratches on the surface (label), which cause distortions in the layer that is actually being read from the bottom. Try the disc in another reader before chucking it out, it could just have trouble with the device you were trying it in.

Does the drive show up in the operating system, on your desktop or in Device Manager in Windows operating systems? If not, the first step is to reinstall the driver. Get the latest driver from the manufacturer's website and install it. If you can boot an OS CD in the drive, but the drive has disappeared from Device Manager, try reinstalling the OS. If that doesn't make Device Manager happy, see if there's a firmware update for the drive itself, though flashing a drive, just like flashing a motherboard BIOS, should be a last resort. Even though the BIOS registers the drive's presence, you can still try swapping the ribbon cable. Try changing the transfer mode the CD is operating in CMOS Setup to a lower speed, if that's possible. Try swapping the drive to another lead from the power supply, even though it's already "awake" enough for the BIOS to have registered its presence. The laser lens in the drive could be incredibly dirty, so if you can find an inexpensive cleaning kit, it's worth a try.

You could have a simple cabling problem or Master/Slave conflict. If the drive is the Slave on primary IDE controller with the hard drive, move it to the secondary IDE controller as the Master (requires another IDE ribbon cable). If you already have another device installed as the secondary Master, you can try the drive as the secondary Slave or temporarily replace the secondary Master for the sake of seeing if it will work. If the BIOS is new enough (say, post 1997) to identify individual IDE devices on the power up screen and it doesn't see your IDE CD or DVD, you aren't going to get it to work.

Can you listen to music CDs through your speakers? The following assumes that you can get operating system sounds to play from your speakers. If not, proceed to Sound Failure. First, make sure that the volume controls in software aren't turned down. Next, if the drive is equipped with an audio jack on the front, stick in a cheap headphone (if you have one) and see if the CD is playing. In any case, if the CD is spinning and the time is advancing in whatever version of Media Player you have installed, the drive is actually playing the CD. The audio patch cord from the drive to the sound card or the sound port on the motherboard may not be connected, or the device volume could be turned down in a software mixer panel. The easy check for incorrect audio patch cable (3 or 4 wires) connection without opening the PC is to try a multimedia CD, such as a game. If the sound works in the game, the problem is a missing or improperly connected cable. Note also that in two drive systems, the builder may only have patched the audio output of one of the drives through to the sound card.

Does the drive cause the whole PC to tremble when it spins up? Is it noisy? Make sure that the drive, if internal, is mounted with four screws, and level. Super high speed drives, say anything over 40X, will vibrate like crazy if a disc is off balance, either because it was chucked up wrong on the spindle, or because the disc itself has some weighting problem. Aside from obvious physical flaws (like the dog or the kid took a bite out of the edge of the disc) a miss-applied label can create an unbalanced disc. Try ejecting and reinserting the disc. I wouldn't keep running a drive that vibrates badly. It could end up damaging the discs (discs have been known to shatter at high speeds) and it doesn't do the other components

in your system any good to be vibrated, which can lead to connections working apart or worse. If the problem only occurs with some discs, you can blame the discs. Otherwise, I'd look into a new drive.

Does your problem involve recording CDs or DVDs? If so, proceed to CD/DVD Recording Problems. For a problem booting a factory CD in a recorder, stay here. It's become increasingly difficult to tell factory pressed CDs from recorded CDs, due to the highly polished labels that can be easily printed for recorded CDs and DVDs. Factory produced discs are usually silver on the read surface, while recorded discs are often gold or green.

Does your system refuse to boot known good boot CDs, like operating systems from Windows 98 on up? Try setting the boot sequence in CMOS Setup to boot to the CD or DVD first. This shouldn't really be necessary if the hard drive is uninitiated, but I've seen it fix the problem. I've also seen some high speed drives which take too long to spin up and report to the BIOS that there's a bootable disc present. Sometimes you can get around this by opening and closing the tray, which should cause the drive to spin up, and hitting reset right after you've done so. With any luck, you'll get the timing right so that the BIOS checks for a bootable CD while the drive is still active

4.5 Printers

A device that prints text or illustrations on paper. There are many different types of printers. In terms of the technology utilised, printers fall into the following categories:

1. **Daisy-Wheel:** Similar to a ball-head typewriter, this type of printer has a plastic or metal wheel on which the shape of each character stands out in relief. A hammer presses the wheel against a ribbon, which in turn makes an ink stain in the shape of the character on the paper. Daisy-wheel printers produce letter-quality print but cannot print graphics.
2. **Dot-Matrix:** Creates characters by striking pins against an ink ribbon. Each pin makes a dot, and combinations of dots form characters and illustrations.
3. **Ink-Jet:** Sprays ink at a sheet of paper. Ink-jet printers produce high-quality text and graphics.
4. **Laser:** Uses the same technology as copy machines. Laser printers produce very high quality text and graphics.
5. **LCD & LED:** Similar to a laser printer, but uses liquid crystals or light-emitting diodes rather than a laser to produce an image on the drum.
6. **Line Printer:** Contains a chain of characters or pins that print an entire line at one time. Line printers are very fast, but produce low-quality print.
7. **Thermal printer:** An inexpensive printer that works by pushing heated pins against heat-sensitive paper. Thermal printers are widely used in calculators and fax machines.

Printers are also classified by the following characteristics:

1. **Quality of Type:** The output produced by printers is said to be either *letter quality* (as good as a typewriter), *near letter quality*, or *draft quality*. Only daisy-wheel, ink-jet, and laser printers produce letter-quality type. Some dot-matrix printers claim letter-quality print, but if you look closely, you can see the difference.
2. **Speed:** Measured in characters per second (cps) or pages per minute (ppm), the speed of printers varies widely. Daisy-wheel printers tend to be the slowest, printing about 30 cps. Line printers are fastest (up to 3,000 lines per minute). Dot-matrix printers can print up to 500 cps, and laser printers range from about 4 to 20 text pages per minute.

3. **Impact or Non-impact:** Impact printers include all printers that work by striking an ink ribbon. Daisy-wheel, dot-matrix, and line printers are impact printers. Non-impact printers include laser printers and ink-jet printers. The important difference between impact and non-impact printers is that impact printers are much noisier.
4. **Graphics:** Some printers (daisy-wheel and line printers) can print only text. Other printers can print both text and graphics.
5. **Fonts:** Some printers, notably dot-matrix printers, are limited to one or a few fonts. In contrast, laser and ink-jet printers are capable of printing an almost unlimited variety of fonts. Daisy-wheel printers can also print different fonts, but you need to change the daisy wheel, making it difficult to mix fonts in the same document.

4.5.1 Troubleshooting of Printers

Here are a few simple techniques that will solve many printer problems.

1. Reboot your computer. This generally solves most printing problems.
2. If it's not printing, or you're getting a message about the Fax printer, change your default printer: Start — Settings — Printers/Faxes. Right-click the printer you want, and then select (left-click) Set as Default.
3. Check and make sure all connections going to and coming from the printer are firmly in place.
4. Check that the printer is on-line:
 - * Start — Settings — Printers, right-click the printer.
 - * If there isn't a checkmark by "Set as Default", left-click that option to select it.
5. Print a test page. If that prints and the application you are using doesn't, you probably will need to contact the application's vendor for support.
6. Turn off your printer for 10 seconds and turn it back on. Make a note of any error messages or flashing lights when the printer is turned back on.
7. If your printer is connected directly to another computer, try rebooting that computer. If your printer is connected to a Jet Direct box, try unplugging the JetDirect box for 10 seconds.
8. You may wish to uninstall and then re-install your printer.

4.6 Modems

Modem (from **mod**ulator-**dem**odulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analogue signals, from driven diodes to radio. The most familiar example is a voiceband modem that turns the digital 1s and 0s of a personal computer into sounds that can be transmitted over the telephone lines of Plain Old Telephone Systems (POTS), and once received on the other side, converts those 1s and 0s back into a form used by a **USB**, Ethernet, serial, or network connection. Modems are generally classified by the amount of data they can send in a given time, normally measured in bits per second, or "bps". They can also be classified by Baud, the number of times the modem changes its signal state per second.

Troubleshooting of Modems :—

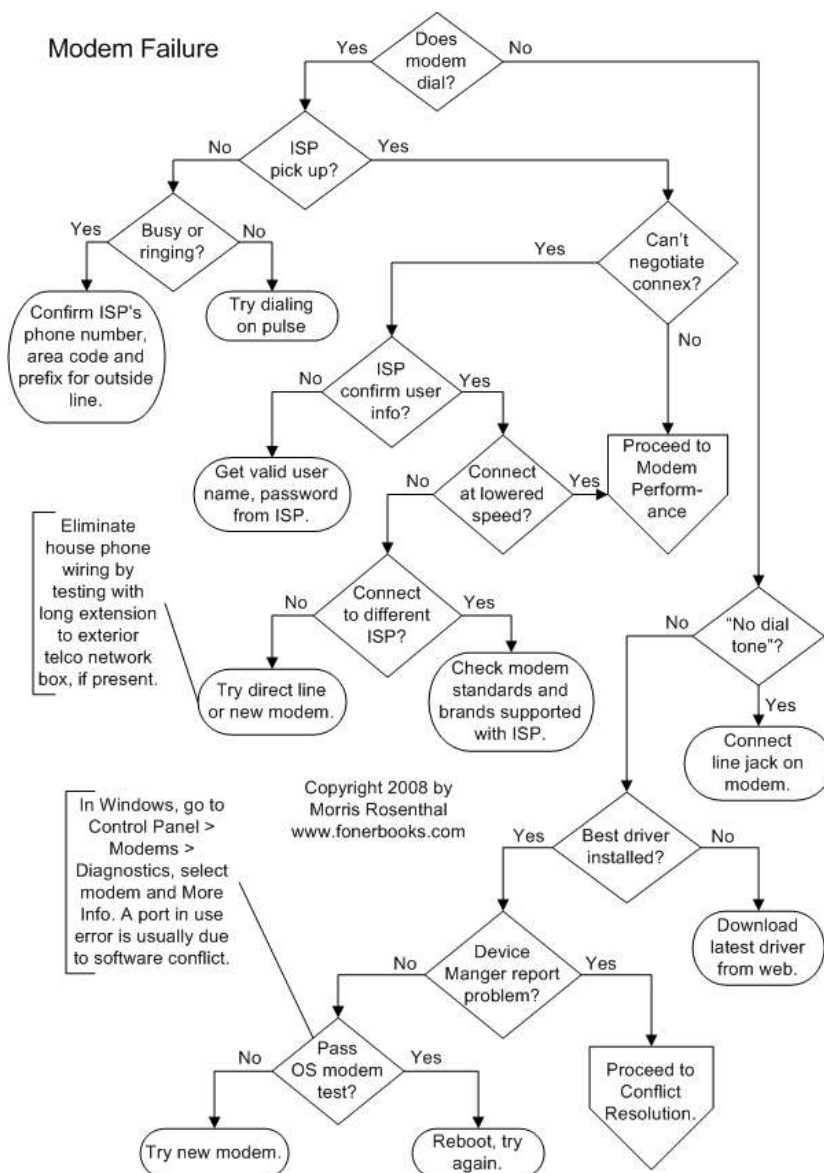


Fig 4.5 Steps of Troubleshooting the Modems

Baud is not the modem's speed in bit/s, but in symbols/s. The baud rate varies, depending on the modulation technique used. Original Bell 103 modems used a modulation technique that saw a change in state 300 times per second. They transmitted 1 bit for every baud, and so a 300 bit/s modem was also a 300-baud modem. However, casual computerists confused the two. A 300 bit/s modem is the only modem whose bit rate matches the baud rate. A 2400 bit/s modem changes state 600 times per second, but due

to the fact that it transmits 4 bits for each baud, 2400 bits are transmitted by 600 baud, or changes in states. Faster modems are used by Internet users every day, notably cable modems and ADSL modems. In telecommunications, “radio modems” transmit repeating frames of data at very high data rates over microwave radio links. Some microwave modems transmit more than a hundred million bits per second. Optical modems transmit data over optical fibres. Most intercontinental data links now use optical modems transmitting over undersea optical fibres. Optical modems routinely have data rates in excess of a billion (1×10^9) bits per second. One kilobit per second (kbit/s or kb/s or kbps) as used in this article means 1000 bits per second and not 1024 bits per second. For example, a 56k modem can transfer data at up to 56,000 bits (7kB) per second over the phone line.

The first troubleshooting question for a dial-up modem is, does your modem actually dial the phone? If you have a desktop PC, there should be a little piezoelectric speaker on the modem itself. Many people (and computer vendors) turn down the volume for this in software, which you can find on the “Properties” tab of the modems in Windows Control Panel. Notebook computers will normally run the sound through the notebook speakers, which means the volume controls in Windows and the volume dial built into the notebook body must both be turned up.

Does the ISP answer? You should be able to hear the ISP’s modem pick up and whistle and hiss back at your modem through the speaker. If not, make sure you are dialing the right phone number and that the ISP isn’t temporarily down. Just dial the number from a regular phone handset and the ISP modem should pick up and whistle at you.

Make sure you have the area code and any prefix for an outside line correct, especially if you are dialing from a business. Dial-up lines in a business must have a clean path through a business phone system (PBX — Private Branch eXchange), just like fax lines. If the phone is always busy, call the ISP’s tech support for help or try one of the other phone numbers they provide. It could simply be that they don’t have enough modems available for the traffic in your area at certain times of day.

If you hear the modem dial but the dial tone remains until an operator picks up and tells you that your phone is off hook, you’re trying to use “tone” dialing on a “pulse” system. This problem is easily corrected in the “Dialing Properties” of the basic modem page in Control Panel.

Do you get an error stating that the ISP can’t negotiate a connection, protocol, anything along those lines? Unfortunately, this error is too generic to help much with how to troubleshoot the problem. Even messages telling you to check your password can be caused by just about anything. Try redialing several times without changing anything to make sure you aren’t just encountering an overloaded modem pool. While standards such as V.90 and V.92 are backwards compatible, it pays to match your standard to the ISP’s for both 56Kb/s performance and reliability.

Call your ISP help line to confirm your login information if it’s the first time you’re dialing in. Re-enter your password, remembering that caps usually count. Assuming you have your username and password right, the odds are any errors reported aren’t due to any protocol settings on your part, especially if you haven’t changed the defaults. If the error crops up at random, it’s usually due to the weather and the time of day, as both play a major role in the circuit conditions of the telco infrastructure. Stormy or damp weather can badly degrade the lines of older telephone networks. Trying at different times of the day is also important for troubleshooting modem problems, with the beginning of the business day, and a period in the mid-afternoon usually being the worst times. I’ve actually run non-Internet modem applications on dedicated lines that showed a huge increase of line noise during these periods, whatever your telco tells you.

Will your modem connect at a lower speed? You can change the maximum speed the modem will try to connect at in Control Panel, but I've noted that the settings don't always take effect, even after rebooting. You can search on the Internet for the modem control string to force your modem to V.34 compatibility, then insert it in the Advanced Settings for the modem which can be accessed through the Modem Properties in Control Panel or Device Manager. If you succeed in connecting at a lower speed, try going through the Modem Performance troubleshooting.

Can you connect to a different ISP? The best test for eliminating modem failure is to see if it will connect to a different service. If you can connect to a friend's ISP, it's a definite proof that the modem isn't bad. It doesn't mean that the ISP you can't connect to is at fault, it could be a question of matching modem standards. By the same token, if you can't connect to another ISP, it doesn't prove your modem is faulty, it could still be a problem with line conditions. The current 56Kb/s standards in use are V.90 and V.92 although some services still support K56Flex and X2.

If the software reports, "No Dial Tone", make sure you have the patch cord from the modem to the wall jack plugged into the "line" jack of the modem. The "phone" jack on the modem is for plugging in a regular telephone to use when you aren't online. If the wall jack is live, try changing the telephone patch cord running from the "line" jack on the modem to the jack on the wall. Check the phone jack at the wall with a telephone handset. If it doesn't work you need to troubleshoot the in-wall wiring or try a different jack.

Have you installed the most recent driver you can find on the modem manufacturer's website? If your modem is integrated on the motherboard, it would be an update to your motherboard driver. Even if your modem is brand-new, hardware often ships with obsolete drivers, either because it's been sitting on the shelf somewhere for a year, or because a recent operating system release has overtaken it and a better driver is available.

Does the operating system report the modem as present and operating? This information appears in Device Manager in Windows. If not, reinstall the driver for the modem. If an IRQ conflict is reported in Device Manager, resolve it by either changing IRQ in software (with a plug-n-play modem) or changing the IRQ jumper on the modem for an old card. If you absolutely can't get around it, you may have an extremely unfriendly sound card or other adapter on the bus which is hogging the IRQ the modem is capable of dealing with. Note that a modem can share an IRQ with a serial port in some cases, though it can't be used when a device is actually attached to that port. If you can't resolve the Device Manager problem, either you have a hardware conflict, or the modem is bad. See the illustrated guide for how to install a 56K modem. Proceed to the Conflict Resolution chart.

Does the operating system or dialing software report the port is "in use" when you try to dial? In Windows Control Panel > Modems, go to "Diagnostics," select your modem, and click on "More Info". Try shutting down and rebooting. The "port in use" error is due to another active software application claiming the port the modem is set on. You could get this error if you're already using the modem but don't realise it for some reason, but it's more likely that you've recently installed software for synchronizing a palm device or for a camera that's colliding with the modem driver.

4.7 Monitors

A **monitor** is an approach to synchronise two or more computer tasks that use a shared resource, usually a hardware device or a set of variables. With monitor-based concurrency, the compiler or interpreter transparently inserts locking and unlocking code to appropriately designated procedures, instead of the

programmer having to access concurrency primitives explicitly. Invented by Per Brinch Hansen, first implemented in the Concurrent Pascal language and used to structure inter-process communication in the Solo Operating System.

4.7.1 Troubleshooting of Monitors

This section discusses problems related to the system monitor. The monitor of course displays the video signals sent by the **video card** in the PC. The monitor is in some ways easier to troubleshoot than other parts of the PC simply because it is not inside the PC box. It interacts only with the video card (or cards in a multiple-video-card **system**) and therefore there are fewer places for problems or conflicts to occur. If you don't find the answer to your problem in this section on monitors, then you should check the problem listings for video cards as well, since the two are so closely related.

4.7.1.1 Monitor is Blank after Restarting System

1. Check to be sure that the monitor has power and that the light is on.
2. Disconnect all devices except for the mouse, keyboard and monitor. Reboot your computer to see if the issue is resolved. If it is, then it is one of the devices that you have disconnected that is causing the problem. Try connecting them one at a time and rebooting each time until the original problem occurs. Once identified, try reinstalling the device and updating the driver to resolve the issue.
3. Try connecting the monitor to a different PC using the problem monitor's power cable. If it still doesn't work, try the known good monitors power cable.
4. Try unplugging the monitors power cable, then wait about 20 or 30 seconds and plug it back in.
5. If none of the above troubleshooting steps does not solve the issue, then it is likely that the monitor is bad.

4.7.1.2 After Connecting a Monitor, the Picture Looks Bad

1. Start the system in Safe Mode by rebooting the system and pressing the F8 key once per second while it is rebooting. Once you see the Windows Startup menu, select Safe Mode from the listed options, press Enter.
2. Go to Start>> Right click My Computer>> Properties>> Hardware tab>> Device Manager button.
3. Click the plus (+) symbol next to the Monitors entry to expand it.
4. Once expanded, right click on the installed monitor(s) and select Uninstall.
5. Exit the Device Manager and restart your system.

Windows will reinstall your hardware automatically.

4.7.1.3 The Monitor has Started Making a Strange Noise

It is usually a glass display type monitor that will create some unusual noise. Such noise could be:

1. A high pitched tone or high pitched squealing sound:

Usually, these sounds will be of such a high frequency that they are out of the human ears range. But it is possible for these frequencies to radiate off of internal components making the sound audible. Most of the time, moving or adjusting the height of the monitor cures this problem. Also, try simply turning the monitor off and then back on. If the sound continues or worsens, then either have a qualified technician take a look at your monitor or replace the monitor.

2. Monitor is making a clicking sound:

This type of noise is usually caused by the monitors relays opening and closing. You could hear this type of sound when the computer starts up or when you are playing a game and a display setting is changed. This sound is considered normal.

4.7.1.4 Monitors Display Settings are not Correct

This problem usually occurs when a new monitor is installed. It can happen if the automatic detection installs the wrong driver for your hardware resulting in incorrect display settings for your application.

You can try reinstalling the monitor by using the above troubleshooting step; “After connecting a monitor, the picture looks bad”. It is possible that Windows will find the correct drivers this time.

4.7.1.5 Display is Rotated

This is usually caused from a game that has changed the Rotation setting within the Graphics Controller. To change this back:

1. Go to Start>> Control Panel>> Intel Extreme Graphics Applet>> Rotation tab.
2. Uncheck the Enable Rotation check box.
3. Click on Apply, then OK.
4. Exit from Control Panel.

***Note:** The above steps may vary depending on the graphics card you have installed. You are looking for the Graphics Controller properties window to change the Rotation setting.*

An alternate method of finding your Rotation setting is:

1. Right click an empty area of your desktop.
2. Select Properties.
3. Click the Settings tab.
4. Select the Advanced button.
5. Click the Graphics card tab.
6. Select the Graphics Properties button.
7. Click the Rotation tab.
8. Uncheck the Enable Rotation checkbox.

Select Apply and exit all windows.

4.8 Switched – mode power supply (SMPs)

A **switched-mode power supply** (also **switching-mode power supply** and **SMPS**) is an electronic **power supply unit (PSU)** that incorporates a switching regulator. While a linear regulator maintains the desired output voltage by dissipating excess power in a pass power transistor, the SMPS rapidly switches a power transistor between saturation (full on) and cutoff (completely off) with a variable duty cycle whose average is the desired output voltage. The resulting rectangular waveform is low-pass filtered with an inductor and capacitor. The main advantage of this method is greater efficiency because the switching transistor dissipates little power in the saturated state and the off state compared to the semiconducting state (active region). Other advantages include smaller size and lighter weight (from the

elimination of low frequency transformers which have a high weight) and lower heat generation due to higher efficiency. Disadvantages include greater complexity, the generation of high amplitude, high frequency energy that the low-pass filter must block to avoid electromagnetic interference (EMI), and a ripple voltage at the switching frequency and the harmonic frequencies thereof.

SMPS can be classified into four types according to the input and output waveforms:

- AC in, DC out: rectifier, off-line converter input stage.
- DC in, DC out: voltage converter, or current converter, or DC to DC converter.
- AC in, AC out: frequency changer, cycloconverter.
- DC in, AC out: inverter.

4.8.1 SMPS and Linear Power Supply Comparison

There are two main types of regulated power supplies available: SMPS and linear. The reasons for choosing one type or the other can be summarised as:

Size and weight Small	Linear power supply If a transformer is used, large due to low operating frequency transformerless.	Switching power supply (mains power frequency is at 50 or 60 Hz), if Smaller due to higher operating frequency (typically 50 kHz - 1 MHz)
Output voltage	With transformer used, any voltages available; if transformerless, not exceeding input. If unregulated, voltage varies significantly with load.	Any voltages available. Voltage varies little with load.
Efficiency, heat, and power dissipation	If regulated, output voltage is regulated by dissipating excess power as heat, which is inefficient; if unregulated, transformer iron and copper losses significant.	Output is regulated using duty cycle control, which draws only the power required by the load. In all SMPS topologies, the transistors are always switched fully on or fully off.
Complexity	Unregulated may be diode and capacitor; regulated has a voltage regulating IC or discrete circuit and a noise filtering capacitor.	Consists of a controller IC, one or several power transistors and diodes as well as a power transformer, inductors, and filter capacitors.
Radio frequency interference	No high-frequency interference. Some mains hum induction into unshielded cables, problematical for low-signal audio.	EMI/RFI produced due to the current being switched on and off sharply. Therefore, EMI filters and RF shielding are needed to reduce the disruptive interference.
Electronic noise at the output terminals	Unregulated PSUs may have a little AC ripple superimposed upon the DC component at twice mains	Noisier due to the switching frequency of the SMPS. An unfiltered output may cause glitches in digital circuits or noise in audio circuits.

	frequency (100-120 Hz). Can cause audible mains in audio equipment or brightness ripples or banded distortions in analog security cameras.	
Electronic noise at the input distortion terminals	Causes harmonic distortion to the input AC, but no high frequency noise.	Very low cost SMPS may couple electrical switching noise back onto the mains power line, causing interference with A/V equipment connected to the same phase. Non power-factor-corrected SMPSs also cause harmonic
Acoustic noise	Faint, usually inaudible mains hum, usually due to vibration of windings in the transformer and/or magnetostriction.	Inaudible to humans, unless they have a fan or are unloaded/malfunctioning.
Power factor	Low for a regulated supply because current is drawn from the mains at the peaks of the voltage sinusoid.	Ranging from low to medium since a simple SMPS without PFC draws current spikes at the peaks of the AC sinusoid.
Risk of electric shock	Supplies with transformers allow metalwork to be grounded, safely. Dangerous if primary/secondary insulation breaks down, unlikely with reasonable design. Transformerless mains-operated supply dangerous. In both linear and SM the mains, and possibly the output voltages, are hazardous and	Common rail of equipment (including casing) is energised to half mains voltage, but at high impedance, unless equipment is earthed/grounded or doesn't contain EMI/RFI filtering at the input terminals.
Risk of equipment damage	must be well-isolated. Very low, unless a short occurs between the primary and secondary windings or the regulator fails by shorting internally.	Can fail so as to make output voltage very high. Can in some cases destroy input stages in amplifiers if floating voltage exceeds transistor base-emitter breakdown voltage, causing the transistor's gain to drop and noise levels to increase. Mitigated by good failsafe design. Failure of a component in the SMPS itself can cause further damage to other PSU components; can be difficult to troubleshoot.

Table 4.2

4.8.2 Theory of Operation

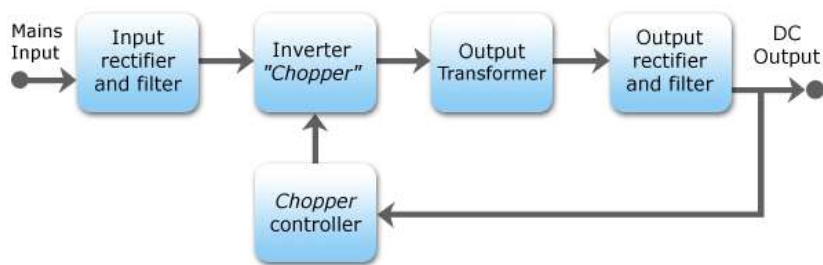


Fig: 4.6 Block diagram of a mains operated AC-DC SMPS with output voltage regulation

4.8.2.1 Input Rectifier Stage

AC, half-wave and full wave rectified signals. If the SMPS has an AC input, then the first stage is to convert the input to DC. This is called *rectification*. The rectifier circuit can be configured as a voltage doubler by the addition of a switch operated either manually or automatically. This is a feature of larger supplies to permit operation from nominally 120 volt or 240 volt supplies. The rectifier produces an unregulated DC voltage which is then sent to a large filter capacitor. The current drawn from the mains supply by this rectifier circuit occurs in short pulses around the AC voltage peaks. These pulses have significant high frequency energy which reduces the power factor. Special control techniques can be employed by the following SMPS to force the average input current to follow the sinusoidal shape of the AC input voltage thus the designer should try correcting the power factor. A SMPS with a DC input does not require this stage. An SMPS designed for AC input can often be run from a DC supply (for 230V AC this would be 330V DC), as the DC passes through the rectifier stage unchanged. It's; however; advisable to consult the manual before trying this, though most supplies are quite capable of such operation even though nothing is mentioned in the documentation. However, this type of use may be harmful to the rectifier stage as it will only utilise half of diodes in the rectifier for the full load. This may result in overheating of these components, and make them fail as short circuits.

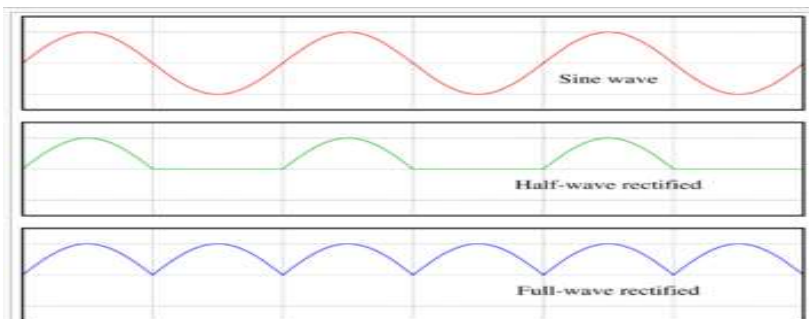


Fig: 4.7 AC, half-wave and full wave rectified signals.

If an input range switch is used, the rectifier stage is usually configured to operate as a voltage doubler when operating on the low voltage (~120 VAC) range and as a straight rectifier when operating on the high voltage (~240 VAC) range. If an input range switch is not used, then a full-wave rectifier is usually used and the downstream inverter stage is simply designed to be flexible enough to accept the

wide range of DC voltages that will be produced by the rectifier stage. In higher-power SMPSs, some form of automatic range switching may be used.

4.8.2.2 Inverter Stage

The inverter stage converts DC, whether directly from the input or from the rectifier stage described above, to AC by running it through a power oscillator, whose output transformer is very small with few windings at a frequency of tens or hundreds of kilohertz (kHz). The frequency is usually chosen to be above 20 kHz, to make it inaudible to humans. The output voltage is optically coupled to the input and thus very tightly controlled. The switching is implemented as a multistage (to achieve high gain) MOSFET amplifier. MOSFETs are a type of transistor with a low on-resistance and a high current-handling capacity. Since only the last stage has a large duty cycle, previous stages can be implemented by bipolar transistors leading to roughly the same efficiency. The second last stage needs to be of a complementary design, where one transistor charges the last MOSFET and another one discharges the MOSFET. A design using a resistor would run idle most of the time and reduce efficiency. All earlier stages do not weight into efficiency because power decreases by a factor of 10 for every stage (going backwards) and thus the earlier stages are responsible for at most 1% of the efficiency. This section refers to the block marked *Chopper* in the block diagram.

4.8.2.3 Voltage Converter and Output Rectifier

If the output is required to be isolated from the input, as is usually the case in mains power supplies, the inverted AC is used to drive the primary winding of a high-frequency transformer. This converts the voltage up or down to the required output level on its secondary winding. The output transformer in the block diagram serves this purpose.

If a DC output is required, the AC output from the transformer is rectified. For output voltages above ten volts or so, ordinary silicon diodes are commonly used. For lower voltages, Schottky diodes are commonly used as the rectifier elements; they have the advantages of faster recovery times than silicon diodes (allowing low-loss operation at higher frequencies) and a lower voltage drop when conducting. For even lower output voltages, MOSFETs may be used as synchronous rectifiers; compared to Schottky diodes, these have even lower conducting state voltage drops. The rectified output is then smoothed by a filter consisting of inductors and capacitors. For higher switching frequencies, components with lower capacitance and inductance are needed.

Simpler, non-isolated power supplies contain an inductor instead of a transformer. This type includes boost converters, buck converters, and the so called *buck-boost converters*. These belong to the simplest class of single input, single output converters which utilize one inductor and one active switch (**MOSFET**). The buck converter reduces the input voltage in direct proportion to the ratio of conductive time to the total switching period, called the *duty cycle*. For example an ideal buck converter with a 10 V input operating at a 50% duty cycle will produce an average output voltage of 5 V. A feedback control loop is employed to regulate the output voltage by varying the duty cycle to compensate for variations in input voltage. The output voltage of a boost converter is always greater than the input voltage and the buck-boost output voltage is inverted but can be greater than, equal to, or less than the magnitude of its input voltage. There are many variations and extensions to this class of converters but these three forms the basis of almost all isolated and non-isolated DC to DC converters. By adding a second inductor the Cuk and SEPIC converters can be implemented, or, by adding additional active switches, various bridge converters can be realised. Other types of SMPSs use a capacitor-diode voltage multiplier instead of

inductors and transformers. These are mostly used for generating high voltages at low currents. The low voltage variant is called *charge pump*.

4.8.2.4 Regulation

A feedback circuit monitors the output voltage and compares it with a reference voltage, which is set manually or electronically to the desired output. If there is an error in the output voltage, the feedback circuit compensates by adjusting the timing with which the MOSFETs are switched on and off. This part of the power supply is called the *switching regulator*. The Chopper controller shown in the block diagram serves this purpose. Depending on design/safety requirements, the controller may or may not contain an isolation mechanism (such as opto-couplers) to isolate it from the DC output. Switching supplies in computers, TVs and VCRs have these opto-couplers to tightly control the output voltage.

Open-loop regulators do not have a feedback circuit. Instead, they rely on feeding a constant voltage to the input of the transformer or inductor, and assume that the output will be correct. Regulated designs work against the parasitic capacity of the transformer or coil, monopolar designs also against the magnetic hysteresis of the core. The feedback circuit needs power to run before it can generate power, so an additional non-switching power-supply for stand-by is added.

4.8.2.5 Transformer Design

SMPS transformers run at high frequency. Most of the cost savings (and space savings) in off-line power supplies come from the fact that a high frequency transformer is a lot smaller than the 50/60 Hz transformers used before SMPS.

There are several differences in the design of transformers for 50 Hz v/s 500 kHz. Firstly; a low frequency transformer usually transfers energy through its core (soft iron), while the (usually ferrite) core of a high frequency transformer limits leakage. Since the waveforms in a SMPS are generally high speed (PWM square waves), the wiring must be capable of supporting high harmonics of the base frequency due to the skin effect, which is a major source of power loss.

4.8.2.6 Power Factor

Simple off-line switched mode power supplies incorporate a simple full wave rectifier connected to a large energy storing capacitor. Such SMPSs draw current from the AC line in short pulses when the mains instantaneous voltage exceeds the voltage across this capacitor. During the remaining portion of the AC cycle; the capacitor provides energy to the power supply.

As a result, the input current of such basic switched mode power supplies has high harmonic content and relatively low power factor. This creates extra load on utility lines, increases heating of the utility transformers and standard AC electric motors, and may cause stability problems in some applications such as in emergency generator systems or aircraft generators. Harmonics can be removed through the use of filter banks but the filtering is expensive, and the power utility may require a business with a very low power factor to purchase and install the filtering onsite.

In 2001; the European Union put into effect the standard IEC/EN61000-3-2 to set limits on the harmonics of the AC input current up to the fortieth harmonic for equipment above 75 W. The standard defines four classes of equipment depending on its type and current waveform. The most rigorous limits (class D) are established for personal computers, computer monitors, and TV receivers. In order to comply with these requirements; modern switched-mode power supplies normally include an additional power factor correction (PFC) stage.

Putting a current regulated boost chopper stage after the off-line rectifier (to charge the storage capacitor) can help correct the power factor, but increases the complexity (and cost).

4.8.3 Troubleshooting of SMPs

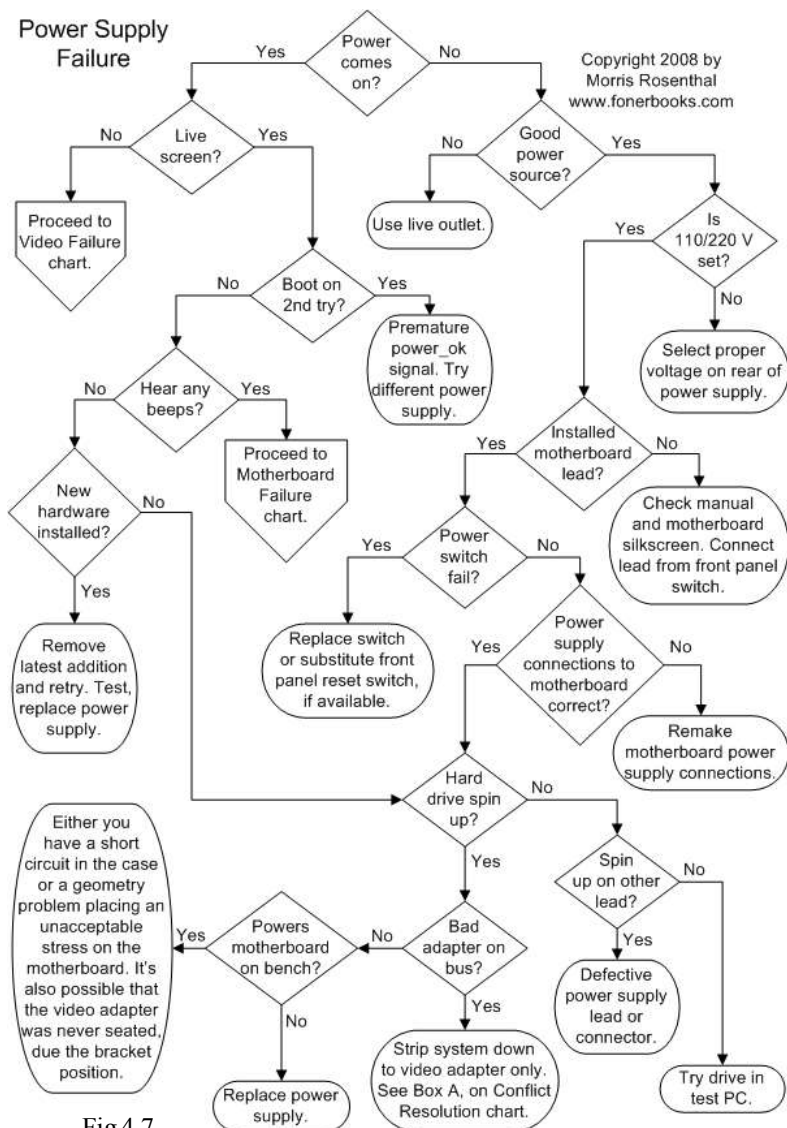


Fig4.7

The first step in power supply diagnostics is determining whether or not the power comes on. How can you tell if the power is on? Can you hear fans turning and drives motors spinning up, see little lights on the front of the CPU case or hear any beeps? If the system case is hot (if you get a shock) pulling the plug immediately — you have a ground failure and a short. If your hearing isn't good, you can always

check to see if the power supply fan is creating a breeze. Monitors are powered independently, so unless you're looking at a notebook PC, a live screen doesn't indicate a working power supply.

If the power doesn't come on, the first thing to check is that you have a live power source. You don't need a DVM (Digital Volt Meter) to check if your power outlet is live. Just unplug the power supply cord and plug in a lamp or a radio. If you are using a power strip, don't assume the socket you are using is good because the other outlets are working and the power strip status light is on. Many power strips I've encountered in the field have at least one bad outlet, and working outlets have been known to fail for no particularly good reason. Power supply cords very rarely fail, but it's possible for the female connector on the power supply end to back out of the socket. Make sure that both ends of the power supply cord are fully seated in the outlet and the power supply, respectively.

Check to make sure the correct voltage (110V/ 220V) is selected on the power supply. While this should never come up with a PC that's just been sitting on the desk, if you've replaced the power supply or moved the PC, it's always a possibility. This small red slide switch is located on power supply, usually between the power cord and the on/off override switch on the back of the case. Unplug the supply and select the proper voltage for your country. If you tried to power up with the switch set to 220V in a country using 110V, the system should be OK when you correct the voltage. If you tried running on 110V in a 220V country, you've at probably blown a fuse in the supply (at the least), or damaged the supply and possibly other components.

If pressing your power switch doesn't immediately shut down the PC, that's normal for ATX systems. The action of the power switch is programmable and is controlled through CMOS Setup. The default operation for most power switches requires you to hold the switch in for three to five seconds before the system will power down. This allows use of the power switch to wake the PC from some power saving "sleep" or "stand-by" modes, depending on CMOS Setup power management settings. If the problem is that the operating system can't turn off the PC when you shut down, it's likely a bad setting in power management or a corrupted file in the operating system.

One very good reason for the power supply to fail is an unconnected power switch. The power switch lead on ATX PCs, often labelled PW or PW-ON, runs from the front panel of the case to a connector block on the motherboard. This issue should only come up if you've been working in the case (the leads can pull off the connection block very easily), or if you've replaced the motherboard. The switch isn't polarized so it doesn't matter which way it goes on the motherboard posts, but it must be on the correct two posts. The proper location is usually printed right on the motherboard next to the connector block, and you can also consult the motherboard documentation. In cases where the documentation provided with the system and the information printed on the motherboard don't agree, I go with the motherboard.

Check the switch operation with a Digital Volt Meter on the continuity or resistance setting. On all ATX systems, the power switch is really just a logic switch that tells the motherboard, to which a trickle of live power is always supplied, to instruct the power supply to come fully alive. If your power supply features a heavy cord running forward to a large switch on the case front, with four connections, you have an old AT style supply and potentially deadly live line voltage is present at the switch. These procedures do not apply to the obsolete AT power supplies. When I'm working on an ATX system and don't have a tester handy, I short the two pins on the motherboard with a screwdriver, where the logic switch from front panel should be attached, and see if the system starts. This is a "live power" test. Don't do it if you may get startled and bash the screwdriver into something should the system power up,

because there's no way to repair short-circuit or gouging damage once it's done. If the switch is bad and you don't have a replacement switch, check for a reset button on the front panel. You can usually get away with using the reset button for the PW-ON logic switch, and live without the hard reset.

The power supply will fail to operate if the power to motherboard isn't connected. Check that the 20 pin ATX power connector and any additional motherboard power connections, such as the 12V supply for P4 systems, are properly connected and seated. The latching mechanism for the standard ATX connector is counter-intuitive. You have to push in on the latch at the top to release it at the bottom, at which point the connector should pull off with almost no force required. You should hear or feel the latch click in when the connector is seated.

Remove the power leads to the drives to ensure that you aren't trying to power up into a short. The motherboard power must remain connected to activate the ATX power supply. If you have a DVM (Digital Volt Meter) and experience working around live circuitry, you can try checking the DC voltages at the connectors to see if they are live, or within 5% of the rated voltage. I'm not advising you do this live testing, as it's much easier and safer to try swapping in a new power supply. Unless you have a special testing fixture, you must leave the connectors attached while checking, which requires an exposed connector surface or a cheater lead. This is necessary because switching power supplies won't operate properly without a load, either failing to come on or even self-destructing (in extreme, low quality, instances). I just poke the DVM probes into the top of the 20 wire connector at the motherboard, since there's usually room next to the wire to get down to the conductor.

ATX Version 1.2 - 20 wire motherboard connector:

Pin 1	Pin 2	Pin 3	Pin 4	Pin 5	Pin 6	Pin 7	Pin 8	Pin 9	Pin 10
3.3V	3.3V	Gnd	5V	Gnd	5V	Gnd	P_OK	5VSB	12V
Oran	Oran	Blk	Red	Blk	Red	Blk	Gray	Purp	Yell
Oran	Blue	Blk	Green	Blk	Blk	Blk	White	Red	Red
3.3V	-12V	Gnd	P_ON	Gnd	Gnd	Gnd	-5V	5V	5V
Pin 11	Pin 12	Pin 13	Pin 14	Pin 15	Pin 16	Pin 17	Pin 18	Pin 19	Pin 20

The colour scheme used for the voltages in the 20 pin connector holds for the other ATX standard power supply connectors. However, brand name manufacturers often build proprietary power supplies or make up their own colour coding, so I wouldn't throw out a power supply that supplies 5V where you think it should supply 3.3V. It's more likely a proprietary design than a failure.

The 5V on Pin 9 is always present when the power supply is plugged in. This connection supplies power to the various PC circuits that operate even when the PC is turned off, such as "Wake on Modem" or "Wake on LAN". It's also the reason you should never work in the PC with the power supply plugged in, unless you can remember to turn off the override switch every time. This live power is supplied to the adapter slots, so replacing adapters with the power cord plugged in may damage the motherboard or adapters. Even though the drive leads aren't powered with the system turned off, you might drop a screw while working on a drive. If that screw lands in just the wrong place, like an open bus slot, it could create a short and damage the motherboard.

Assuming your PC is connected to a monitor, the next question is, do you have a live screen? Does text or a splash screen appear? A message saying "Please connect monitor" or "No video signal detected" counts as a "No" answer in this case. If the screen is live, but you see multiple images or endless

scrolling, the video adapter is providing signals that cannot be interpreted by the monitor. This usually occurs when you attach an old monitor to a new PC and the monitor doesn't support the refresh rate at the screen resolution selected in the Windows settings.

If the power supply comes on but you don't get a live screen, switch off and try again. You may have to hold the power switch in for five or more seconds before the system powers back down. If it fails to power down, you can turn off the switch on the back of the power supply, turn off your power strip, or unplug the cord. A PC that boots on the second or third try is most likely suffering from a quick power_ok (or power_good) signal, coming on before the power supply has stabilised. The presence of the power_ok signal tells the motherboard that the power supply is stable, while its absence tells the motherboard to stay off to protect itself. It's possible the power supply isn't quite up to the current ATX standard or the motherboard is a little too demanding about timing. Booting twice every time you want to turn on the PC isn't an ideal situation, so unless you leave it on all the time, look into buying a higher quality power supply, ideally one recommended by the motherboard manufacturer.

Beep codes are part of the PC's Power On Self Test (POST) routine. One beep means the system has passed the test and the BIOS believe that the CPU and memory and video are functioning properly. All other beep codes vary by BIOS supplier and system brand, but endlessly repeating slow beeps often indicate RAM failure, so shut down and try reseating the memory module(s). A repeated string of beeps, either 3 or 9 beeps long, is frequently video failure, so unplug the power and try reseating the video adapter. If you are getting beeps with a live screen, the problem is unlikely to be power supply related. Proceed to the Motherboard, CPU and RAM Failure diagnostics.

If you don't get any beeps, make sure the case speaker is connected and check for beeps again. If the motherboard lacks a connection point for a case speaker near the power switch and LED block, it probably employs an onboard piezoelectric speaker. If you have recently added any new components to the system, they may be overtaxing the power supply or causing a short circuit. This includes both adapters and drives. The first step in any failure situation is to try undoing the last change you made. I recently encountered a system which powered up but failed to initialise the video adapter when the secondary IDE ribbon cable was connected backwards to a CD drive! Although the component you just added may have worked in another system, it doesn't mean you hooked it up properly, that it's compatible with the current PC, or that it didn't fail in the interim.

Common power supply problems unrelated to the boot process are noisy operation and unstable voltages, both of which are a reason to replace the supply. There are two common noise problems associated with power supplies, noisy fans and whistling capacitors. Noisy fans can be replaced, but only if you're a reasonably competent technician because you can really get a nasty zap from the stored energy in the capacitors even when the power supply is unplugged. Make sure your noisy fan problem isn't due to something silly like a piece of paper poking in through the fan grille before you rush out and buy a replacement. If your dog won't stay in the room when the computer is turned on or if your kids hear a high pitched whistling that you don't, it's probably a capacitor. To determine whether the capacitor is in the power supply or elsewhere in the system will require a process of elimination or some parts swapping.

Unstable voltage problems are real ghosts in the machine, and can mimic all sorts of other problems. If you get into a flaky failure situation that you can't diagnose and you've already started troubleshooting (i.e.; swapping parts), you may as well try a new power supply as well. I've seen power supplies produce some really bizarre failures, like a PC that reboots when you set your coffee cup down too hard on the table. The most pervasive of the unstable power supply problems are random lockups or spontaneous

reboots. Modern motherboards have some ability to regulate the power they receive, but it's got to be within a reasonable range. When it starts overshooting the limits, the system may freeze or shutdown the motherboard to protect itself.

As soon as the PC powers up, you should be able to hear the hard drive motor spin the drive (like a very, very, quiet jet taking off) and the read/write head seeking (a gentle clunking sound). If you're absolutely baffled as to whether or not the drive is spinning up, due to background noise or hearing problems, you can resort to feeling the drive cover. If that still doesn't do it, I power down, remove the drive cage or the drive itself, and hold it firmly by the edges (not touching any exposed wires or the circuit board on the bottom) while powering up. The drive resists twisting movements like a gyroscope if it's spun up. Don't play with it. If you move too fast or touch the circuit board to something that can cause a short, you'll damage the drive. Just power down, reinstall, and continue with the diagnostics.

If system power is coming on but the drive still isn't spinning up, make sure that your power lead is seated in the drive power socket. It doesn't need to go all the way to the ridge stop on the connector, but it should go in a good half inch or so. It does take a good deal of force to seat the cheaper leads in some drives. Try another lead, even if you have to disconnect another drive to get it. Try another drive. At this point it's still quite possible that the power supply is defective, but if you have a drive that you know spins up, it's a good way to eliminate one possibility. As long as you don't smell smoke coming out of the drive you can test the drive in another system. If you are using SCSI rather than IDE hard drives, check the documentation for a jumper that suppresses spin up on boot. SCSI drives offer this option because you can install as many as 15 in a single system, and if they all tried to spin up at once it would swamp any power supply. Normally, the SCSI host adapter will spin them up in order of their SCSI ID.

If system power isn't coming on, disconnect all drives, one at a time, and try powering up after each change. If the system powers up, you've found a faulty drive or a faulty lead from the power supply. If the system won't power up with all drives disconnected, start removing adapters, one at a time, leaving the video for last. Unplug power cord before removing each adapter, then reconnect to power up. If the system powers up, replace all adapters except the last one removed before power came on. If power still comes on, try the last adapter you removed in different slot before giving up on it.

If you find an adapter that actually prevents the system from powering up, it must be replaced. If this is your video adapter and it is an AGP type, for which the motherboard only has one slot, it could be that the AGP slot is faulty. Another possibility is that the adapter is keyed as universal but is installed on a new motherboard that expects low voltage AGP adapters (AGP 4X or 8X).

Once you've eliminated the drives and the adapters, one of the few remaining possibilities is a motherboard short. Remove the motherboard and check for a standoff or screw located in the wrong place or rolling around loose. I often build out systems on the bench without a case, supporting the motherboard on a static proof bag over a cardboard box or some similar arrangement to give the adapters room to seat. This method eliminates any case mounting issues from the diagnostics process, but it introduces all sorts of risks, not the least of which is absence of the case ground.

Normally, a short circuit will result in a burnt smell and a ruined motherboard, sometimes damaging any of the attached components (memory, CPU, adapters) as well. In many instances, you'll be able to figure out which component is ruined by the presence of burn marks or a strong odor of smoke coming from the component, though if it happens in a closed case, the smoky smell can stick to everything. If you can't locate a failed component by visual inspection, you need to have access to a test-bed system (an

inexpensive but completely functioning PC for testing questionable parts). Don't test parts that may be fried in a good system, because some types of failures will cause damage to the next machine.

If you've reached this point without getting the system to power up, you probably have a defective power supply or motherboard. Try replacing the power supply first since they're cheaper than motherboards. Repairing power supplies requires a good knowledge of electronics as there are usually "no user serviceable parts." Even when power supplies are unplugged, they can give nasty zap from stored power in the electrolytic capacitors. If the power supply or motherboard is new, they may be incompatible with one another due to poor adherence to ATX standards or support for different generations of the ATX standard.

EXERCISE

1. Define Mother Board? Explain the process of troubleshooting the Motherboard with the help of a diagram.
2. Define the steps of trouble shoot to :
 - (i) FDD
 - (ii) HDD
3. Define CD ROM/DVD? Explain the process of troubleshooting the CD ROM/DVD with the help of a diagram.
4. Define printers and explain its types also. Explain the process of troubleshooting the printers?
5. Define Modems. Explain the process of troubleshooting the Modems with the help of a diagram.
6. Explain the process of troubleshooting the Monitors with the help of a diagram.
7. Define SMPs? Explain the process of trouble shooting the SMPs with the help of a Diagram?
8. Explain the "Theory of Operation" with help of diagram of SMPs.

Computer Repair and Maintenance

Chapter

5

Instructional Objectives

- 5.1 Specification, Maintenance and Repair of CVT
- 5.2 Specification, Maintenance and Repair of UPS
- 5.3 Technologies

5.1 Specification, Maintenance and Repair of CVT (Constant Voltage Transformer)

Constant Voltage Transformers have been used for many years, primarily as a noise-isolation device. Recently they have found value when applied as a voltage-sag protection device for industrial and commercial facilities. The purpose of this section in the book is to give power-system engineers and facility engineers who are unfamiliar with the CVT technology (also known as *Ferro resonant transformers*) the insights and information necessary to determine the types of electric-power-supply events that CVTs can mitigate.

Continuous stable supply of A.C. Power is the life line of any sophisticated electronic system. Performance of any electrical equipment/instrument is optimum at its rated voltage; Under-voltage Over-voltage produce harmful effect. Under-voltage generally reduces efficiency, whereas Over-Voltage shortens the life. Power SPIKES, accidental OR from the Electricity Boards, can waste very valuable time and corrupt the valuable data fed in. Also a very low voltage can force the system to shut down. PACE CONSTANT VOLTAGE TRANSFORMER [CVT] is the only remedy to overcome hazardous consequences of BROWN-OUTS, SAGS, SURGES, SPIKES and in general all EMI / RFI NOISES. PACE CVT IS A STATIC VOLTAGE STABILIZER with no moving parts, gives very accurate output voltage of $\pm 2\%$ of rated output voltage over a wide input voltage range of 175V to 265V, 50Hz. Super fast correction within 1/50th of second.

A Voltage Stabilizer is a type of household mains regulator which uses a continuously variable autotransformer to maintain an AC output that is as close to the standard or normal mains voltage as possible, under conditions of fluctuation. It uses a servomechanism (or negative feedback) to control the position of the tap (or wiper) of the autotransformer, usually with a motor. An increase in the mains voltage causes the output to increase, which in turn causes the tap (or wiper) to move in the direction that reduces the output towards the nominal voltage.

An alternative method is the use of a type of saturating transformer called a **Ferro resonant transformer** or **constant-voltage transformer**. These transformers use a tank circuit composed of a high-voltage resonant winding and a capacitor to produce a nearly constant average output with a varying

input. The Ferro resonant approach is attractive due to its lack of active components, relying on the square loop saturation characteristics of the tank circuit to absorb variations in average input voltage. Older designs of Ferro resonant transformers had an output with high harmonic content, leading to a distorted output waveform. Modern devices are used to construct a perfect sine wave. The Ferro resonant action is a flux limiter rather than a voltage regulator, but with a fixed supply frequency it can maintain an almost constant average output voltage even as the input voltage varies widely.

The Ferro resonant transformers, which are also known as *Constant Voltage Transformers* (CVTs) or ferrous are also a good surge suppressors, and it provides high isolation and an inherent short-circuit protections.

It can operate with an input voltage range as wide as $\pm 40\%$ or more of the nominal voltage.

Output power factor remains in the range of 0.96 or higher from half to full load.

Because it regenerates an output voltage waveform, output distortion, which is typically less than 4%, is independent of any input voltage distortion, including notching.

Efficiency at full load is typically in the range of 89% to 93%. However, at low loads, efficiency can drop below 60% and no load losses can be as high as 20%. The current-limiting capability also becomes a handicap when a CVT is used in an application with moderate to high inrush current like motors, transformers or magnets. In this case, the CVT has to be sized to accommodate the peak current, thus forcing it to run at low loads and poor efficiency.

Minimum maintenance is required beyond annual replacement of failed capacitors. Redundant capacitors built into the units allow several capacitors to fail between inspections without any noticeable effect to the device's performance.

Output voltage varies about 1.2% for every 1% change in supply frequency. For example, a 2-Hz change in generator frequency, which is very large, results in an output voltage change of only 4%, which has little effect for most, loads.

It accepts 100% single-phase switch-mode power supply loading without any requirement for derating, including all neutral components.

Input current distortion remains less than 8% THD even when supplying nonlinear loads with more than 100% current THD.



Fig. 5.1: Typical Constant Voltage Transformers

Draw backs of CVTs (constant voltage transformers) is larger size, a high audible humming sound, and high heat generation.

5.1.1 History of CVT

The industrial use of CVT also called Ferro resonant transformers goes back to the early-1940s. Living in the US during the 1930s, Joseph G. Sola, a German-born engineer, discovered the CVT technology based on the single transformer rather than an arrangements of transformers, separate filters and capacitors. This innovation provides several important advantages: its inherent robustness (CVT consists of just three or four windings and a high-reliability capacitor), its imperviousness to continuous short circuits (whether it is turned on into a short circuit or from full load), and its capability to maintain output-voltage stabilisation on a cycle-to-cycle basis for significantly large overvoltage's and under voltages.

Sola were both a farsighted inventor and successful businessman. Internationally recognised as the pioneer of the transformer magnetic technology, his inventions and subsequent refinements of other electronic equipment were considered revolutionary by the electrical industry. Sola's first transformer for furnace-ignition systems and neon lighting, based on the unique application of Ferro resonant principals led in 1938 to his invention of the CVT. This timely discovery was eagerly accepted by prime military contractors during World War II and established Sola as a world leader in voltage regulation. Sola was awarded a total of 55U.S. patents during his lifetime, including five patents each for CVTs, Solatrons, and electronic power supplies, and 19 patents for high-intensity-discharge lighting ballasts.

Throughout the last six decades, a series of applications has been found for products based on Sola's CVT technology. It is one of the most cost-effective ac power conditioners available.

5.1.2 Uses of CVT

Office & Business Equipment: Computers, Electronic Typewriters, Ledger Posting Machines, Electronic Cash Registers, Telephone Exchanges, Facsimile [FAX] etc.

CNC systems, Photo Typesetters, Tele-printer, Security Systems, etc.

Process Controls Medical Equipment: Life saving emergency equipments in ICUs, X-ray Machine, Medical Monitors, Field & Lab Instruments, Communication Equipments, etc.

5.1.3 Operation of CVT

The CVT (Ferro) uses the unique principle of Ferro resonance: operation of a transformer in the region of magnetic saturation. When the iron core of a transformer is in saturation, relatively large changes in winding current results in very small changes in magnetic flux. Winding current and magnetic flux are proportional to the input and output voltage, respectively. This means that relatively large changes in input voltage result in small changes in output voltage: this being the fundamental purpose of an automatic voltage regulator.

The graphic below shows a simplified version of a magnetization curve to demonstrate this concept. In the saturation region of the curve (red), a large change in input voltage results in a small change in output voltage. Operation in the saturation region has the disadvantage of very poor electrical efficiency. Standard power transformers are designed to operate in the normal range (blue) where electrical efficiency is much higher. While standard power transformers have some minimal capacity for voltage regulation, their primary purpose is to transform voltage from one level to another (e.g.; convert 480V to 208V) with high electrical efficiency.

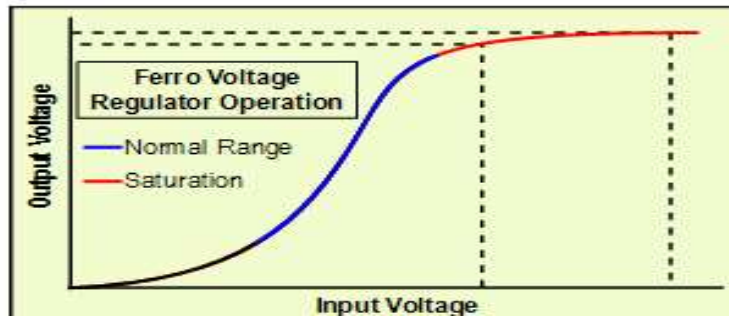


Fig. 5.2

Operation in the saturation region also produces another undesirable effect: sine wave distortion. As shown in the graphic, most Ferro resonant transformers incorporate an LC (inductor-capacitor) circuit (tank circuit) tuned to the AC frequency to effectively filter out many of the distortions.

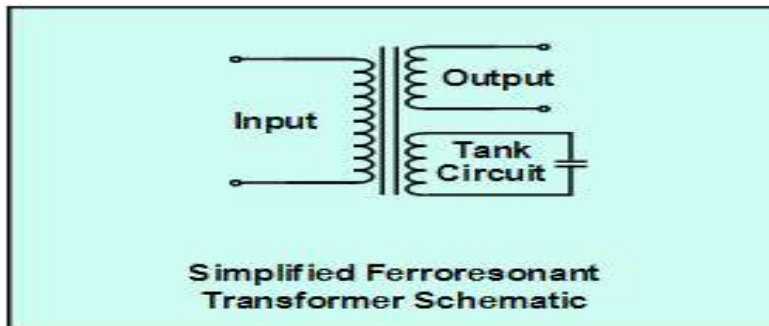


Fig 5.3

5.1.4 Advantages and disadvantages

Advantages

The CVT, by its unique design, provides good isolation of load equipment from line noise and surges. The output voltage regulation is also smooth so long as the manufacturer has taken steps to minimise the distortion that is caused by operation in the saturation region. Ferro voltage regulators can be very durable with some manufacturers offering warranties in excess of 10 years.

One unusual operating characteristic of the CVT is that its design can limit the amount of current to the load. When the load current exceeds about 150% of rated current of a CVT, the unit is "pulled" out of the saturation region, the output voltage collapses to a very small value and the current is thereby limited. In some applications, this characteristic is intentionally used to protect loads from high currents, however in other applications this characteristic becomes a substantial disadvantage.

Disadvantages

The principle of magnetism that affords the CVT its voltage regulation capability is also its Achilles heel. Voltage regulators of this type can have electrical efficiencies up to 92% at full load and ideal conditions but at lighter loads the efficiency drops off substantially. The graphic at the right shows a typical range of

CVT efficiency versus percent load. It can be seen that at 50% load, the CVT voltage regulator efficiency ranges from 75 to 85%. As a comparison, a typical power transformer would have an efficiency of 90% or more at 50% load.

In applications with high overload or inrush currents, it is common that the constant voltage transformer be oversized by 2 to 3 times the rated load current. This is to permit the CVT to pass enough current before the output voltage collapses as described above. However, over sizing the constant voltage regulator greatly reduces its efficiency. The scales inserted in the lower right of the graphic demonstrate what happens to efficiency when a constant voltage regulator is oversized by a factor of 2 or 3 times the load: at 3X the efficiency even at 75% load only reaches 60 to 75%.



Fig 5.4

5.1.5 Instructions for Use (Installation)

- Place the CVT away from your equipment in well ventilated surroundings, away from magnetic storage devices like diskettes, tapes, cartridges, monitors, etc.
- Always connect 3 pin input/output with good earthing.
- Ensure good contacts and no loose connections.
- Not recommended for use with D.G. sets not having regulated frequency
- Not recommended for high inductive loads like motors, compressors, welding, spark erosion, etc.
- Switch off the CVT when not in use to reduce iron and heat losses

5.1.6 Features

There are times when one feels that a stabiliser is not enough. After all, a stabiliser can correct voltage with a certain finite speed. We would think that our instruments are connected to a stabilizer and are unaware of the fact that it is still passing on the spikes, voltage surges, glitches, noise etc. Which are so short, that it cannot be corrected by a stabiliser.

What then? The answer is a C.V.T. from 'ASEEM-OORJA' this works on magnetic saturation principle, resonating with a tank circuit of high Q factor. When incoming mains voltage is low the capacitor provides the necessary additional gain in power, keeping the output voltage steady. On the other hand, when the mains voltage is high the leakage reactance drops the difference of voltage. This correction of voltage is instantaneous even for sudden dips and spikes.

There are some features listed below:

1. Resonance occurs when the inductance is in saturation.
2. As the value of inductance in saturation is not known precisely, a wide range of capacitances can potentially lead to Ferro resonance at a given frequency.
3. More than one stable, steady-state response is possible for a given configuration and parameters values.
4. Proven technology.
5. High reliability.
6. Fast response.
7. Output short circuit protected.
8. Rugged industrial design.
9. High efficiency.
10. CMRR & DMRR noise rejection up to 100 dB.
11. Can handle inductive loads.
12. VERY HIGH VOLTAGE CORRECTION SPEED - Almost Instantaneous.
13. VERY HIGH ISOLATION between Input & Output to filter EMI/RFI.
14. COMPUTER GRADE Clean, Filtered continuous Power supply.
15. Built-in inherent protection against UNDER-VOLTAGE, OVER-VOLTAGE & OVER-LOAD.
16. Silent, Sleek, Compact, light weight, aesthetic design for desk top use.
17. NO-LOSS OF OUTPUT SUPPLY for line loss up to 30 milliseconds.
18. BUILT-IN VOLTMETER provided to continuously monitor the output voltage.
19. Output provided through 3 SOCKETS [for computer application - CPU, Monitor, and Printer].
20. Higher Reliability as NO MOVING parts - MAINTENANCE FREE.
21. High reliability because no semiconductors or moving parts are used.
22. No feedback control used.
23. Intrinsic current limiting and short circuit protection.
24. Output voltage correction within $\frac{1}{2}$ cycles (10 milliseconds) from no load to full load for specified load and line variation.
25. Short-term overload capacity.
26. Energy storage for line loss up to three milliseconds at typical load.
27. Higher input voltage control range, for loads less than rated load.
28. Very high line transient/spike rejection capability and excellent isolation characteristic.

5.1.7 Output Voltage vs. Input Voltage

The y-axis in fig. 5.5 is the CVT output voltage at the secondary terminals, while the x-axis in the CVT's is input primary voltage. There are three possible modes of behaviour, depending on the level of the input

voltage. At input voltage V_1 , the CVT operates in non saturation mode. The secondary responds linearly to the primary supply. Note that this mode is used in a conventional transformer but is undesirable in CVT.

Input voltages V_2 , there are three outputs denoted by V_{o1} , V_{o2} , and V_{o3} . Output V_{o1} and V_{o3} are both in stable state. Output V_{o1} corresponds to the normal state, whereas V_{o3} corresponds to the Ferro resonant state. Output V_{o2} is an unstable state that cannot be obtained in practice. Whether CVT output is V_{o1} or V_{o3} depends on the initial value of residual flux and voltage at the capacitor terminals. The phenomenon where the output voltage either suddenly changes to the regulating mode of operation at some value of the ascending input voltage, or suddenly drops out of the regulating mode of operation with descending input voltage is called **jump resonance**. The jump resonance is a factor during dynamic supply-voltage conditions. At the input voltage V_3 , the CVT operates in Ferro resonant mode. The CVT must operate in this mode for proper operation.

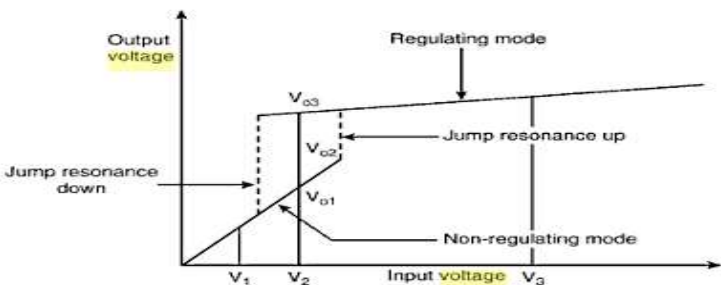


Figure 5.5: Output Voltage vs Input Voltage for constant voltage transformer with jump resonance

5.1.8 Typical Service, Storage, and Shipment Conditions

Table 5.1 list typical service conditions for ambient temperature, relative humidity, altitude and type of cooling. If forced-air cooling is available or required, the direction of airflow, velocity, temperature, and volume flow per minute at the constant-voltage transformer are included in the specification. For liquid-cool units, the type of coolant, rate of flow and the inlet coolant temperature range are specified.

Table 5.2 lists storage temperature, relative humidity, and altitude ranges for a typical CVT.

Table 5.3 lists shipment condition as it's relates to temperature, relative humidity, and altitude ranges for a typical CVT.

Service Condition	
Service Conditions	Range
Ambient Temperature	0–50°
Relative humidity	20–90%
Altitude	0–1500 m
Type of cooling	Convection cooling is assumed

Table: 5.1

Storage Conditions	
Storage Conditions	Range
Ambient Temperature	– 40 to 60°C
Relative humidity	5-90%
Altitude	02,000 m

Table 5.2

Shipment Condition	
Temperature	Range
Temperature	– 55°C to 60°C
Relative humidity	5-90%
Altitude	012,000 m

Table 5.3

5.1.9 Application Considerations-Output Performance under Dynamic Supply Conditions

The objective of this application was to characterise the CVT performances during power system disturbances such as momentary interruptions sag, phase shifts, capacitor switching, and lighting strikes. The CVT was connected to a full, purely resistive load.

5.1.9.1 Performance: Voltage Interruption

The CVT was subjected to a voltage interruptions lasting from 0.5 to 5 cycles and adjusted in 0.5-cycles increments. Switching from the normal supply voltage source to an open circuit created each interruption. The input and the output voltage are shown in below figure:

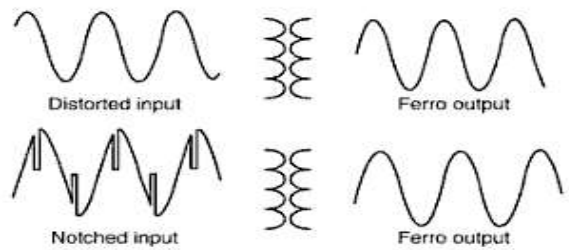


Figure 5.6: Output Voltage resulting from distorted and notched input voltages at full load

During the three-cycle interruption, the CVT drooped out the regulating mode and the output voltage decreased as the resonant capacitor in the CVT discharged.

When the input voltage returned to normal, an overshoot occurred on the output voltage as the resonant capacitor recharged. Note that the CVT does not act as an uninterruptible power supply, which is designed to eliminate the effect of an interruption on the electric service supply, but it does slightly decrease the effect of an interruption by reducing it to deep voltage sag. In conclusion a CVT can moderately mitigate, but not eliminate, the effects of momentary voltage interruptions.

5.1.9.2 Performance: Voltage Sag

To simulate the fault in the load's electric-service supply, the input voltage to the CVT was decreased to 90%, 70%, and 58% of nominal voltage for one, two, three, four, and five cycles. The variations in the output voltage were measured and recorded for each of the applied voltage sags. Figure 5.7 shows the CVT's input and output voltage waveforms down to 58% nominal voltage lasting three cycles. In general, the input voltage sags produce output voltage sag having approximately the same duration but smaller sag depth.

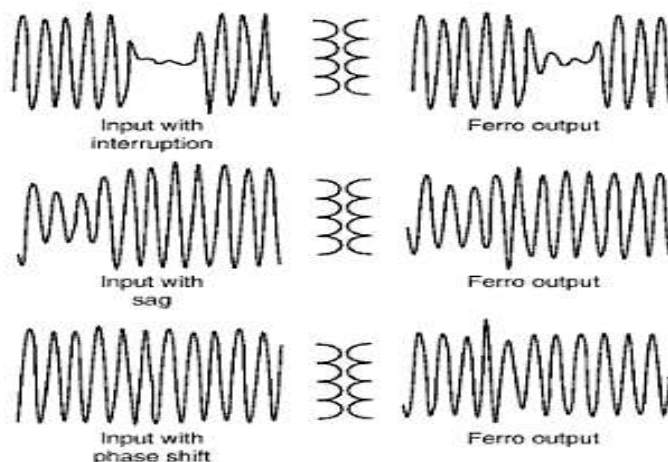


Figure 5.7: Output voltages resulting from voltage interruption

5.1.9.3 Performance: Voltage Phase Shift

To simulate the effects of a large load being switched off near the end of a long electric-service supply feeder, the input voltage of the CVT was shifted forward 10μ while the input and output voltages were monitored and recorded. The phase shift occurred at the positive peak of the input voltage (see Figure 5.7). The resulting phase shift in the input voltage caused the output voltage to briefly swell. The CVT is sensitive to voltage phase shift in the electric-service supply.

5.1.9.4 Performance: Oscillating Transient

A transient caused by capacitor switching was simulated with a 500-Hz ring wave with a peak magnitude of 1 per unit and duration of 10ms. The ring wave was applied to the positive peak of the input voltage.

5.1.9.5 Performance: Oscillating Transient

To simulate a lightning strike, a 2-kV, 1.2/50- μ s combination wave (as described in ANSI C62.41-1991) was applied to the positive peak of the input voltage. As shown in Figure: 5.8, the CVT significantly damped and filtered the surge.

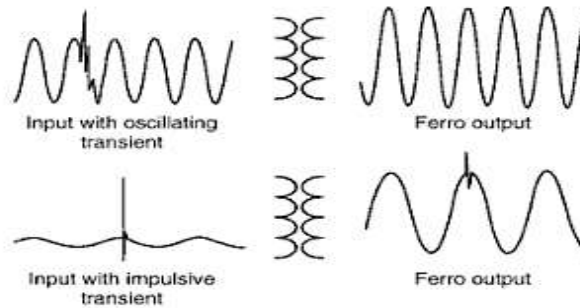


Figure 5.8: Output voltages resulting from oscillating and impulsive transient in the input voltages

5.1.10 Application Considerations—CVT Electrical Characteristics during Linear and Nonlinear Loading

The objective of this application was to characterise the CVT as load while the CVT supplied a simple linear load and while it supplied a complex nonlinear load. In the following tests, the CVT was connected first to a simple linear load and then to a complex nonlinear load. An electric-service supply source with an average total harmonic distortion in the voltage of 3% supplied power to the CVT during all tests.

5.1.10.1 Performance: Line Current Distortion

A resistive linear load consisting of incandescent lamp was connected to the output of the CVT. The load was increased in ten equal increments from 0 to 8.3 A (Open current rating of the CVT). Next a bridge rectifier (such as the type that might be used in electric-vehicle battery chargers) was connected to the CVT. The rectifier and its resistive load (incandescent lamps) were the complex nonlinear load of the CVT. By adding lamps, this complex load was increased in ten equal increments from approximately 0.4 A (rectifier with no lamps connected) to 8.3 A. Figure 5.9 and Figure 5.10 show the line-current distortion during these tests compared with the line-current distortion for the same loads connected directly to the electric-service supply. At no load, the power consumption of the CVT was approximately 120 W (core losses only). With the full linear load, total losses increased to approximately 134 W (core losses plus load losses); with the full nonlinear load, total losses dropped to approximately 110 W.

Notice in Figure 5.9 and Figure 5.10 that while the y-axis current-distortion magnitudes are significantly different, the absolute current-distortion value of the CVT's input current with either linear or nonlinear load is nearly identical. Current distortion at the CVT's input terminals was practically independent of the type of load connected to the output (approximately 40% at no loading to approximately 5% at full loading). When a linear, low-distortion load was connected to the CVT output, the CVT contributed to the current distortion at its input terminals from the electric-service power source, particularly during low loading. When a nonlinear, high-distortion load was connected, the CVT substantially reduced load-current distortion. When fully loaded, the CVT had relatively small power consumption and an efficiency of 85% to 90%. As opposed to most voltage regulators, the losses of the CVT decreased as the nonlinear load increased. The CVT also significantly affected the power factor of the load.

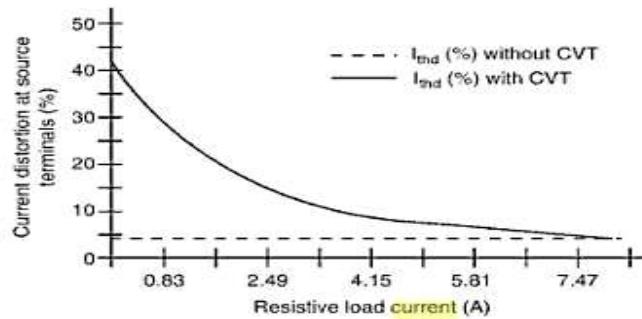


Figure 5.9: Line-current distortions for a linear load.

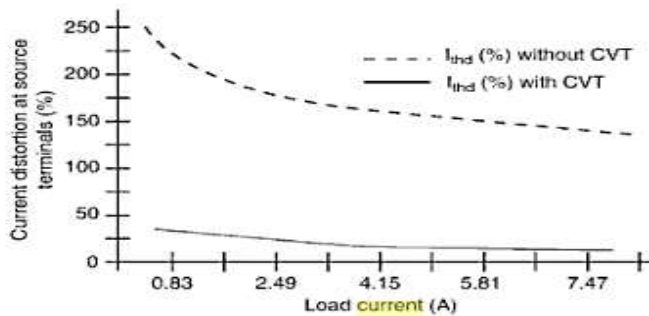


Figure 5.10: Line-current distortions for a nonlinear load.

5.1.10.2 Performance: Power Factor

For both linear and nonlinear loads, the size of the load affected the input power factor of the CVT. While the CVT was loaded at less than 40% of its output power rating (approximately 3.3 A), the power factor ranged from 0.65 to 0.95. While the CVT was loaded at greater than 40%, the power factor was greater than 0.95 for the linear load and greater than 0.90 for the nonlinear load. For the linear load, the power factor crossed from lagging to leading at approximately 60% load (approximately 5 A). Figure 5.11 and Figure 5.12 shows the power factors for the linear and nonlinear load (without and with the CVT), respectively. The CVT significantly affected the power factor of the load. At low loading the nonlinear load without the CVT had a power factor as low as 0.44. With the CVT, the total power factor of the nonlinear load ranged from 0.61 to near unity. However, when loaded at less than 50%, the CVT significantly reduced the power factor for the linear, resistive load which normally has a unity power factor. Note that in most CVT applications, the aggregate facility loading is significantly small, so it would not be prudent to attempt any power-factor at individual CVT operating loads. Power factor correction initiatives should be accomplished at the electric service meter of the facility.

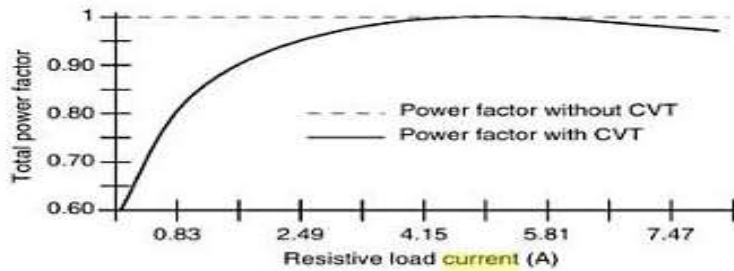


Figure 5.11: Power factor for a linear load

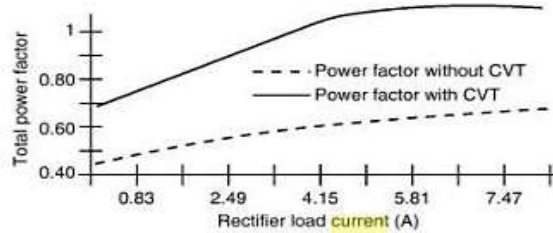


Figure 5.12: Power factor for a nonlinear load

5.1.11 Specifications: Below there is a chart of general specifications:

1. Input Voltage Range	170 - 270 Volts A. C. 1 ph.
2. Frequency	50 Hz $\pm$ 2.5 Hz
3. O/P Voltage	230 V AC (Adjustable to 220 V or 240 V)
4. Line Regulation	$\pm$ 2% at rated load
5. Load Regulation	1 %
6. Waveform	Sinusoidal
7. Response Time	20 ms.
8. CMRR Noise Rejection	100 db.
9. DMRR Noise Rejection	120 db.
10. Efficiency	Better Than 85 %
11. Total Galvanic Isolation	5 KV
12. Energy Storage	3ms.
13. Protection	a) Short CKT; b) Over Load; c) Fuse in the input CKT

Table: 5.4

5.1.12 Maintenance and Repair of CVT

Constant Voltage Transformers are ideal maintenance free solutions for loads that can suffer erratic operation or be damaged by electrical noise (common and series mode) local transient's mains power sags surges and brownouts.

Constant Voltage Transformers are the best and most reliable Power Conditioners for applications ranging from process control and automation to remote sites and third world applications.

5.2 Specification, Maintenance and Repair of UPS (Uninterruptible Power Supply)

An **uninterrupted power supply (UPS)**, also known as a **battery back-up** provides emergency power and, depending on the topology, provide line regulation as well to connected equipment by supplying power from a separate source when utility power is not available. It differs from an auxiliary or emergency power system or standby generator, which does not provide instant protection from a momentary power interruption. A UPS, however, can be used to provide uninterrupted power to equipment, typically for 5-15 minutes until an auxiliary power supply can be turned on or utility power is restored.

While not limited to safeguarding any particular type of equipment, a UPS is typically used to protect computers, data centers, telecommunication equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption or data loss. UPS units come in sizes ranging from units which will back up a single computer without monitor (around 200 VA) to units which will power entire data centers or buildings (several megawatts).

5.2.1 Common Power Problems

There are various common power problems that UPS units are used to correct. They are as follows (with a typical example of damage that might be caused):

1. Power failure — Total loss of utility power, with possibility of severe transient conditions upon failure and/or restoration: Causes electrical equipment to stop working (transients may cause permanent damage).
2. Voltage Sag — Transient (short term) under-voltage: Causes flickering of lights.
3. Voltage Spike — Transient (short term) over-voltage i.e. spike or peak: Causes wear or acute damage to electronic equipment.
4. Under-voltage (Brownout) — Low line voltage for an extended period of time: Causes overheating in motors.
5. Over-voltage — Increased voltage for an extended period of time: Causes light bulbs to burnout.
6. Line Noise — Distortions superimposed on the power waveform: Causes electromagnetic interference.
7. Frequency Variation — Deviation from the nominal frequency (50 or 60 Hz): Causes motors to increase or decrease speed and line-driven clocks and timing devices to gain or lose time.
8. Switching Transient — Instantaneous undervoltage (notch) in the range of milliseconds to seconds: May cause erratic behaviour in some equipment, memory loss, data error, data loss and component stress.
9. Harmonic Distortion — Multiples of power frequency superimposed on the power waveform: Causes excess heating in wiring and fuses.

UPS units are divided into categories based on which of the above problems they address. Manufacturers categorize their products in accordance with the number of power related problems they address.

5.2.2 Applications

5.2.2.1 N+1

In large business environments where reliability is of great importance, a single huge UPS can also be a single point of failure that can disrupt many other systems. To provide greater reliability, multiple smaller UPS modules and batteries can be integrated together to provide redundant power protection equivalent to one very large UPS.

5.2.2.2 Multiple Redundancy

Many computer servers offer the option of redundant power supplies, so that in the event of one power supply failing, one or more other power supplies are able to power the load.

While it is common to plug each of these individual power supplies into one single UPS, redundant protection can be extended further yet by connecting each power supply to its own UPS. This provides double protection from both a power supply failure and a UPS failure, so that continued operation is assured.

5.2.2.3 Outdoor Use

When a UPS system is placed outdoors, it should have some specific features that guarantee that it can tolerate weather with a 'minimal to none' effect on performance. Factors such as temperature, humidity, rain, and snow among others should have been considered by the manufacturer when designing an outdoor UPS system. Operating temperature ranges for outdoor UPS systems could be around -40°C to +55° C.

Outdoor UPS systems can be pole, ground (pedestal), or host mounted. Outdoor environment could mean extreme cold, in which case the outdoor UPS system should include a battery heater mat, or extreme heat, in which case the outdoor UPS system should include a fan system or an air conditioning system.

5.2.2.3 Internal Systems

UPS systems can be designed to be placed inside a computer chassis. There are two types of Internal UPS. The first type is a miniaturised regular UPS that is made small enough to fit into a 5.25" CD-ROM slot bay of a regular computer chassis. The other type are re-engineered switching power supplies that utilise dual power sources of AC and/or DC as power inputs and have an AC/DC built-in switching management control units.

5.3 Technologies

The general categories of modern UPS systems are *on-line*, *line-interactive*, and *standby*. An on-line UPS uses a "double conversion" method of accepting AC input, rectifying to DC for passing through the battery (or battery strings), then inverting back to AC for powering the protected equipment. A line-interactive UPS maintains the inverter in line and redirects the battery's DC current path from the normal charging mode to supplying current when power is lost. In a standby (off-line) system the load is powered directly by the input power and the backup power circuitry is only invoked when the utility power fails. Most UPS below 1 kVA are of the line-interactive or standby variety which is usually less expensive.

For large power units, Dynamic Uninterruptible Power Supply are sometimes used. A synchronous motor/alternator is connected on the mains via a choke. Energy is stored in a flywheel. When the mains power fails, an Eddy-current regulation maintains the power on the load. DUPS are sometimes combined or integrated with a diesel-genset, forming a diesel rotary uninterruptible power supply, or DRUPS.

Fuel cell UPS have been developed in recent years using hydrogen and a fuel cell as a power source, potentially providing long run times in a small space. A fuel cell replaces the batteries used in other UPS designs.

5.3.1 Offline/Standby

The **Offline / Standby UPS** offers only the most basic features, providing surge protection and battery backup. Usually the Standby UPS offers no battery capacity monitoring or self-test capability, making it the least reliable type of UPS since it could fail at any moment without warning. These are also the least expensive, selling for as little as US\$ 40. The Standby UPS may be worse than using nothing at all, because it gives the user a false sense of security of being assured protection that may not work when needed the most.

With this type of UPS, a user's equipment is normally connected directly to incoming utility power with the same voltage transient clamping devices used in a common surge protected plug strip connected across the power line. When the incoming utility voltage falls below a predetermined level the UPS turns on its internal DC-AC inverter circuitry, which is powered from an internal storage battery. The SBS then mechanically switches the connected equipment on to its DC-AC inverter output. The switch over time is stated by most manufacturers as being less than 4 milliseconds, but typically can be as long as 25 milliseconds depending on the amount of time it takes the Standby UPS to detect the lost utility voltage.

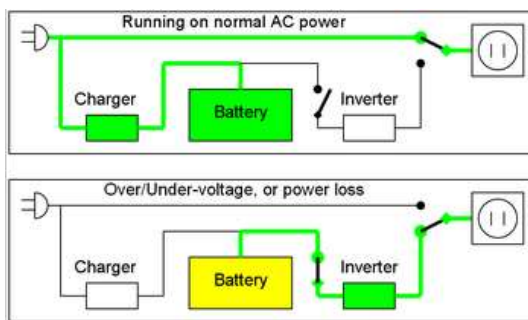


Figure 5.3: Offline/Standby UPS. Typical protection time: 0 - 20 minutes

5.3.2 Line-interactive

The **Line-Interactive UPS** is similar in operation to a Standby UPS, but with the addition of a multitap variable-voltage autotransformer. This is a special type of electrical transformer that can add or subtract powered coils of wire, thereby increasing or decreasing the magnetic field and the output voltage of the transformer.

This type of UPS is able to tolerate continuous undervoltage brownouts and overvoltage surges without consuming the limited reserve battery power. It instead compensates by auto-selecting different power taps on the autotransformer. Changing the autotransformer tap can cause a very brief output power disruption, so the UPS may *chirp* for a moment, as it briefly switches to battery before changing the selected power tap.

Autotransformers can be engineered to cover a wide range of varying input voltages, but this also increases the number of taps and the size, weight, complexity, and expense of the UPS. It is common for the autotransformer to only cover a range from about 90v to 140V for 120V power, and then switch to battery if the voltage goes much higher or lower than that range.

In low-voltage conditions the UPS will use more current than normal so it may need a higher current circuit than a normal device. For example to power a 1000 watt device at 120 volts, the UPS will draw 8.32 amps. If a brownout occurs and the voltage drops to 100 volts, the UPS will draw 10 amps to compensate. This also works in reverse, so that in an overvoltage condition, the UPS will need fewer amps of current.

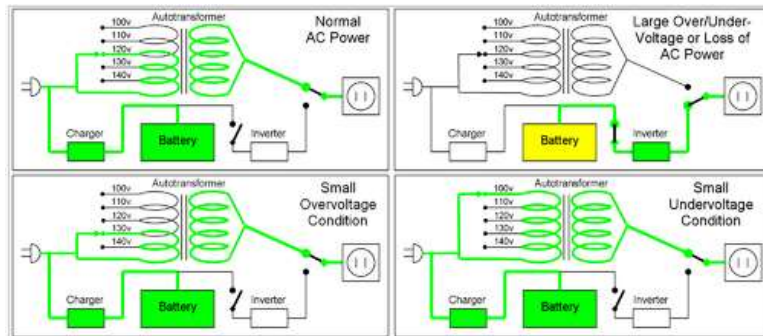


Figure 14: Line-Interactive UPS. Typical protection time: 5 – 30 minutes

5.3.3 Double-conversion/online

The **Online UPS** is ideal for environments where electrical isolation is necessary or for equipment that is very sensitive to power fluctuations. Although once previously reserved for very large installations of 10kW or more, advances in technology have permitted it to now be available as a common consumer device, supplying 500 watts or less. The Online UPS is generally more expensive but may be necessary when the power environment is “noisy” such as in industrial settings, for larger equipment loads like data centers, or when operation from an extended-run backup generator is necessary.

The basic technology of the online UPS is the same as in a Standby or Line-Interactive UPS. However; it typically costs much more, due to it having a much greater current AC-to-DC battery-charger/rectifier, and with the rectifier and inverter designed to run continuously with improved cooling systems. It is called a UPS due to the rectifier directly driving the inverter, even when powered from normal AC current.

In an Online UPS, the batteries are always connected to the inverter, so that no power transfer switches are necessary. When power loss occurs, the rectifier simply drops out of the circuit and the batteries keep the power steady and unchanged. When power is restored, the rectifier resumes carrying most of the load and begins charging the batteries, though the charging current may be limited to prevent the high-power rectifier from overheating the batteries and boiling off the electrolyte.

The main advantage to the online UPS is its ability to provide an electrical firewall between the incoming utility power and sensitive electronic equipment. While the Standby and Line-Interactive UPS merely filters the input utility power, the Double-Conversion UPS provides a layer of insulation from power quality problems. It allows control of output voltage and frequency regardless of input voltage and frequency.

5.3.4 Ferro-resonant

Ferro-resonant units operate in the same way as a standby UPS unit with the exception that a Ferro-resonant transformer is used to filter the output. This transformer is designed to hold energy long enough to cover the time between switching from line power to battery power and effectively eliminates the transfer time. Many Ferro-resonant UPSs are 90-93% efficient and offer excellent isolation.

This used to be the dominant type of UPS and is limited to around the 15KVA range. These units are still mainly used in some industrial settings due to the robust nature of the UPS. Many Ferro-resonant UPSs utilising controlled ferro technology may not interact with power-factor-correcting equipment.

5.3.5 DC Power

A UPS designed for powering DC equipment is very similar to an online UPS, except that it does not need an output inverter, and often the powered device does not need a power supply. Rather than converting AC to DC to charge batteries, then DC to AC to power the external device, and then back to DC inside the powered device, some equipment accepts DC power directly and allows one or more conversion steps to be eliminated. This equipment is more commonly known as a *rectifier*.

Many systems used in telecommunications use 48 volt DC power, because it is not considered a *high-voltage* by most electrical codes and is exempt from many safety regulations, such as being installed in conduit and junction boxes. DC has typically been the dominant power source for telecommunications, and AC has typically been the dominant source for computers and servers.

There has been much experimentation with 48v DC power for computer servers, in the hope of reducing the likelihood of failure and the cost of equipment. However, to supply the same amount of power, the current must be greater than an equivalent 120V or 240V circuit, and greater current requires larger conductors and/or more energy to be lost as heat.

High voltage DC (380 volts) is finding use in some data center applications, and allows for small power conductors, but is subject to the more complex electrical code rules for safe containment of high voltages.

5.3.6 Rotary

A Rotary UPS uses the inertia of a high-mass spinning flywheel to provide short-term ride-through in the event of power loss. The flywheel also acts as a buffer against power spikes and sags, since such short-term power events are not able to appreciably affect the rotational speed of the high-mass flywheel. It is also one of the oldest designs, predating vacuum tubes and integrated circuits.

It can be considered to be online since it spins continuously under normal conditions. However, unlike an electronic double-conversion UPS, it is only capable of providing reserve power for a few seconds before the flywheel has slowed and the protection fails. It is traditionally used in conjunction with standby diesel generators, providing backup power only for the brief period of time the engine needs to start running and stabilise its output.

The Rotary UPS is generally reserved for applications needing more than 10,000 watts of protection, to justify the expense of an extremely large and heavy power system that can only be transported by forelift or crane. A larger flywheel or multiple flywheels operating in parallel will increase the reserve running time, but at greatly increasing cost due to the size and weight of the precision-balanced flywheels.

Because the flywheels are a mechanical power source, it is not necessary to use an electric motor or generator as an intermediary between it and a diesel engine designed to provide emergency power. By using a transmission gearbox, the rotational inertia of the flywheel can be used to directly start up a diesel engine, and once running, the diesel engine can be used to directly spin the flywheel. Multiple flywheels can likewise be connected in parallel through mechanical countershafts, without the need for separate motors and generators for each flywheel.

They are normally designed to provide very high current output compared to a purely electronic UPS, and are better able to provide inrush current for inductive loads such as motor startup or compressor loads, as well as medical MRI and cath lab equipment. It is also able to tolerate short-circuit conditions up to 17 times larger than an electronic UPS, permitting one device to blow a fuse and fail while other devices still continue to be powered from the Rotary UPS.

Its life cycle is usually far greater than a purely electronic UPS, up to 30 years or more. But they do require periodic downtime for mechanical maintenance (ball bearing replacement), while solid-state designs, using batteries, do not require downtime if the batteries can be hot-swapped, which is usually the case for larger units.

Typically, the high-mass flywheel is used in conjunction with a motor-generator system. These units can be configured as:

1. A motor driving a mechanically connected generator,
2. A combined synchronous motor and generator wound in alternating slots of a single rotor and stator,
3. A Hybrid Rotary UPS, designed similar to an Online UPS, except that it uses the flywheel in place of batteries. The rectifier drives a motor to spin the flywheel, while a generator uses the flywheel to power the inverter.

In case No.3 the motor generator can be synchronous/synchronous or induction/synchronous. The motor side of the unit in case No.2 and No.3 can be driven directly by an AC power source (typically when in inverter bypass), a 6-step double-conversion motor drive, or a 6 pulse inverter. Case No.1 uses an integrated flywheel as a short-term energy source instead of batteries to allow time for external, electrically coupled gensets to start and be brought online. Case No.2 and No.3 can use batteries or a free-standing electrically coupled flywheel as the short-term energy source.

EXERCISE

1. Explain the terms CVT and UPS.
2. Why is it required to keep proper maintenance of UPS and CVT?
3. What is the difference between CVT and UPS?
4. What is the rotary UPS? Which applications it is used for?
5. Explain the general categories of modern UPS in detail.

Environmental Requirement of Computer System and Peripherals

Chapter

6

Instructional Objectives

6.1 Environmental Requirements of Computer Systems and Peripherals

6.1 Environmental Requirements of Computer Systems and its Peripherals

“Environment Management” is the management of the physical environment within which IT infrastructure is housed. It is about ensuring the physical location and conditions within which PCs, servers and other IT equipment are stored or operated is appropriate for the effective operation of that equipment.

Why do we need to be concerned with Environment Management? An organisation may have critical operations dependent on the effective operation of its IT infrastructure. An event that leads to loss of expensive equipment, data or services can therefore have a major detrimental effect on an organisation. Consequently, the environment must be managed and controlled appropriately, with proper responsibility and accountability. Physical IT equipment impacts on all parts of an organisation. Not least it can be a fire hazard so the organisation must ensure appropriate management. IT equipment also has its own space requirements. Space may be a scarce resource and so the organisation as a whole should allow for these requirements.

Definition of IT Equipment

IT equipment requiring a managed environment will vary depending on the scale and complexity of the IT infrastructure in use within the organisation. It may include some or all of the following:

- PC Desktops and Peripherals (printers, scanners).
- Computer Servers.
- Networking Equipment, Telephone Equipment and Cabling.
- Laptops and Mobile Devices.
- Consumables (manuals, software disks, spares).
- Data Backups (tapes, CDs).

Components of Environment Management

The components of environment management will vary according to the size of the organisation, but some consideration should be made to each of the following components by those accountable and responsible for IT.

Key Components:

- Computer / Server Room
- Data and Cabling Requirements
- Power conditioning
- Temperature and Humidification
- Fire Detection and protection
- Access and Security
- Location
- Health and Safety Requirements

Each component is listed below with example considerations for each. Further detail in each area is available from the references listed.

Computer/Server Room

It is recognised that not all organisations will need a dedicated “room”. However, where use of IT is expected to increase dedicated space should be planned for. The decision to dedicate space in a separate room will be dependent on factors such as:

- Quantity of equipment in use.
- Security requirements.
- Space availability.

If a dedicated room is to be used it should be located on a first floor where possible. Flooring (including false floors) must be able to support the weight of the equipment. In choosing the “room” location, water, gas and fire hazards should be avoided and access must be available for equipment to be delivered and maintained. Additionally when planning the use of a dedicated computer room tries to anticipate expected future requirements as the amount of equipment will impact all components described in this document.

It must be remembered that IT equipment generates noise and heat and this will impact the general office environment so it is important to anticipate the need for a dedicated room if one is not currently in use.

Electrical and Data Cabling

Cabling must be safe within the office environment. Preferably cables should be stored in multi-compartment trunking and must support the current and predicted loads. False floors may be needed in larger equipment rooms.

Power Conditioning

The building supply must provide suitable power for the load required. A power distribution unit (PDU) may be required depending on this load.

Consider the impact to the organisation if power is lost.

An Uninterrupted Power Supply (UPS) normally gives sufficient of power to allow a controlled shut down of equipment. Where guaranteed power supplies are required backup generators may be required but this can be a substantial investment.

Temperature and Humidification

Ensure the equipment and the room it is in is not going to overheat.

In a normal office computer equipment can add significantly to the ambient temperature causing discomfort for employees. Computer equipment located separately in a computer room must be appropriately cooled.

During the planning phase consideration must be given to the following questions amongst others. Is the air conditioning of the right specification depending on heat output (BTU)? Does this allow for current and anticipated equipment levels and during the summer months? Is air conditioning currently placed such that if a fault develops condensation water could leak onto the IT equipment? Is air conditioning maintenance contracts are in place?

Service critical computer rooms require 22 degrees C +/- 5 degrees C. and will require dedicated air conditioning separated from the building's services. Humidity should be at 50% (+/- 10%).

Fire Detection and Protection

Necessary preventative steps must be in place. Office alarms may not be sufficient.

Ensure basic housekeeping activities taking place – e.g., air cooling clear, dust minimised, other potentially combustible materials such as software manuals are stored away from equipment.

Are sufficient fire extinguishers available? Is staff trained in their use? Fire suppression may be required for larger rooms, together with VESDA – Very Early Smoke Detection Apparatus.

If there is a catastrophic fire are data backups being made on a regular basis and being stored in a secure fire proof safe?

Access and Security

Appropriate levels of security should be in place for the IT equipment. For examples; access alarms on doors and windows. If possible there should be no signage or external windows to identify that the room is a computer room. An audit trail should be kept of access made by both internal staff and external suppliers.

Are the organisation's laptops and mobile devices stored securely in the office or when out on tour? Have appropriate locks been provided?

Location

Because of the investment required in maintaining a physical environment for critical systems the option of outsourcing may be appropriate to some organisations. Services which are available include renting rack space at a dedicated location where all required services are provided and managed as part of a service agreement. Additional capacity can be rented on an as needed basis without a major incremental investment. Appropriate networking and connectivity to the location is, however, required.

Any organisation with multiple locations may be able to cheaply minimise risks with the use of different sites to store backup materials or locate components of their IT infrastructure.

Computer system reliability is dependent upon a stable environment. The design of the environmental control system for your data center must ensure that each system can operate reliably while remaining within the range of its operating specifications.

Accurate and comprehensive monitoring of environmental support equipment and in-room conditions is extremely important in a sensitive data center environment. The monitoring system should have historical trend capabilities. Analyzing historical trend information is instrumental when determining seasonal changes or other contributing influences. Also, the environmental control system should have critical alarm capabilities. The system must be able to notify the appropriate personnel when conditions move outside of the systems' established operating specifications.

6.1.1 Operating Specifications

The servers can operate in diverse locations and within a wide range of environmental conditions, stringent control over temperature, humidity, and airflow is necessary for *optimal* system performance and reliability.

6.1.2 Temperature

An ambient temperature range of 21 to 23°C (70 to 74°F) is optimal for system reliability and operator comfort. While most computer equipment can operate within a rather broad range, a temperature level near 22°C (72°F) is desirable because it is easier to maintain a safe associated relative humidity level at this temperature. Further, this recommended temperature provides an operational buffer in case the environmental support systems are down.

Air Intake Temperatures

Note that the operating temperature range for the servers is either 5 to 40 °C (41 to 104 °F) or 5 to 35 °C (41 to 95°F). These temperatures apply to the air taken in by each server at the point where the air enters the server, and not necessarily the temperature of the air in the aisles. Ensure that the air intake temperature is within the operating range of the system.

Aisle Temperatures

Aisle temperatures can give you a first-level alert to conditions in the data centre. In a hot-aisle/cold-aisle cabinet layout, verify that the temperatures within the cold aisles are also within the servers' operating temperature ranges. These measurements are necessary because temperatures in the data centre are different depending on where in the room the measurements are taken. The heat load in the data centre can vary as a result of the density of heat-producing equipment located within the room. Avoid placing temperature sensors in areas that are exposed to drafts or other uncontrolled airflow.

Rate of Change

Also measure the rate of temperature changes within a 60-minute period. Conditions should not be allowed to change by more than 5.5 °C (10 °F) or 10% relative humidity during a 60-minute period. If you detect fluctuations, measure conditions over a 24-hour period and compare results against historical data to analyse trends.

Also avoid cooling *short cycles*, which can occur if perforated tiles or gridded tiles are placed between the air conditioners and the nearest heat-producing equipment. If tiles are laid out in that way, cold air returns to the air conditioner without circulating through the equipment. The air conditioner might register that temperatures in the room are cooler than is actually the case. The air conditioner might cycle out of its cooling mode while temperatures in the room still call for cooler air.

6.1.3 Humidity

Relative humidity (RH) is the amount of moisture in a given sample of air at a given temperature in relation to the maximum amount of moisture that a sample could contain at the same temperature. A volume of air at a given temperature can hold a certain amount of moisture. Because air is a gas, it expands as it is heated. As air gets warmer, its volume increases and the amount of moisture it can hold increases, thus causing its relative humidity to decrease.

Ambient relative humidity levels between 45% and 50% are most suitable for safe server operations. This optimal range also provides the greatest operating time buffer in the event of an environmental control system failure.

Data centre equipment is particularly sensitive to high humidity levels. When relative humidity levels are too high, water condensation can occur, which can lead to hardware corrosion problems.

Further, maintaining a relative humidity level between 45% and 50% helps avoid system damage or temporary malfunctions caused by intermittent interference from electrostatic discharge (ESD), which occurs when relative humidity is too low. Electrostatic discharge is easily generated and less easily dissipated in areas where the relative humidity is below 35%, and becomes critical when relative humidity drops below 30%.

Though the 20 to 80% RH operating specifications for the servers are wide, conditions should be maintained near the optimal relative humidity levels. Extremes within the 20 to 80% RH range can lead to unacceptable conditions. For instance, if very high temperatures are maintained with very high humidity levels, condensation can occur, which can cause corrosive equipment damage. If very low temperatures are maintained with very low humidity levels, even a slight rise in temperature can lead to unacceptably low relative humidity levels.

It is also imperative that sensors on humidifiers are calibrated correctly. If one unit is calibrated to add humidity, and an adjacent unit is calibrated to remove humidity, energy is wasted and an unacceptable environment can occur.

6.1.4 Troubleshooting Environmental Conditions

The temperature and humidity in the data center have a direct relationship to the proper functioning of the installed systems. Data center managers need to be proactive by continually monitoring data centre conditions. Regularly scheduled temperature and humidity measurements are one way that data centre managers can troubleshoot environmental conditions.

Three types of data centre temperature and humidity tests are suggested:

- Facility Environmental Tests.
- Equipment Installation Environmental Tests.
- Equipment Failure Environmental Tests.

These tests are described in the following sections.

Facility Environmental Tests

Facility environmental tests are designed to measure ambient temperature and humidity throughout the data centre in order to avoid environmental-related equipment problems. These measurements provide an overall assessment of the facility and ensure that the temperature and humidity of air in the cold aisles are within the systems' recommended operating ranges.

Knowing the temperature and humidity of the facility also gives you a general assessment of how the systems are functioning and how much cooling capacity is available to expand the facility.

To measure the ambient temperature and humidity of the data centre, follow these guidelines:

- Place sensors in cold aisles, where cold air outlets provide conditioned air to the systems. Hot-aisle measurements will be typically out the systems' recommended operating ranges and; therefore; are not a valid indication of the required temperature and humidity levels.
- Place sensors 10 to 30 feet (3 to 9 m) apart, or in front of every fourth rack in the aisle.
- Place sensors in the middle of the aisle, between the rows of racks.
- Place sensors 4.9 feet (1.5 m) above the tiled floor.

These measurements will provide you with a detailed and representative profile of the temperature and humidity of air in the cold aisles. By continually monitoring temperature and humidity within the aisles, you can guard against changes that could affect the systems' optimal environmental ranges. If any measurements are outside of the systems' optimal operating ranges, data centre managers must identify the source of, and correct, the problem.

It is also important to measure the temperature and humidity of the return air in front of the HVAC systems. If the return air is below the ambient temperature of the cold aisles, it might mean that cold-aisle air is short cycling, that is, returning to the system units before filtering through the systems.

Equipment Installation Environmental Tests

Equipment installation environmental tests are used to ensure that systems are properly installed and laid out within the facility. These tests measure the temperature and humidity of the air immediately in front of the systems or cabinets. Unacceptable environmental conditions can occur if racks of systems have mixed airflow patterns, if cabinets are not properly vented, or if high-density systems are laid out too closely, causing hot spots.

To measure the temperature and humidity in front of the installed systems, follow these guidelines:

- Take measurements in front of the top, middle, and bottom system in the rack.
- Take measurements at the mid-point vertically and horizontally at the front of each of the three systems.
- Take measurements at 2 inches (5 cm) from the front of the three systems.
- If there are three or fewer systems in the rack, take measurements at 2 inches (5 cm) from the front mid-point of each system.

For example, if there are ten servers in the rack, measure the temperature and humidity at the mid-point of the servers at 2 inches (5 cm) from the front of the first, fifth, and tenth server, bottom to top, in the rack.

All temperature and humidity measurements should be within the systems' recommended operating ranges. If the environmental levels are outside of these ranges, data centre managers should reevaluate airflow patterns and equipment layout, and determine whether the required cold air is available to the systems.

Equipment Failure Environmental Tests

Equipment failure environmental tests can help you determine whether the system failure was due to environmental conditions. These tests are similar to the equipment installation environmental tests, except that temperature and humidity measurements are isolated to the failed system. These tests can help you determine whether the air intake to the system is within the system's recommended temperature and humidity ranges.

To measure the temperature and humidity of air in front of a failed system, follow these guidelines:

- For a 1RU to 3RU system, take measurements at three points midway vertically and horizontally at 2 inches (5 cm) from the front of the system. This provides one horizontal row of three measurement points.
- For a 4RU to 6RU system, take measurements at six points at 2 inches (5 cm) from the front of the system. Divide the six points into two rows of three points each. Center each row of points vertically and horizontally in front of the system.
- For a 7RU or larger system, take measurements at nine points at 2 inches (5 cm) from the front of the system. Divide the nine points into three rows of three points each. Center each row of points vertically and horizontally in front of the system.
- For systems with a localized air inlet area, take measurements in a circular grid pattern, with the number of points dependent on the size of the inlet area.
- For a system installed in a cabinet, take measurements in front of the system with the cabinet doors in their normal operating position, that is, either with the cabinet doors opened or closed.

All temperature and humidity measurements should be within the recommended operating range of the system. If all measurements are within this range, environmental conditions are probably not the cause of the system failure.

6.1.5 Cooling and Aisle Airflow

Data centers have different cooling and airflow capacities, often depending on when the data center was built and the requirements it was designed to meet. When designing a data center, you should consider the facility's heating, ventilation, and air conditioning capacity so that equipment in fully populated cabinets and racks can be adequately cooled. The air conditioners need to be set accurately with a sensitivity of $\pm 1^{\circ}\text{C}$ ($\pm 2^{\circ}\text{F}$).

Calculating Cooling Requirements

Typically, a cabinet footprint requires 12 square feet (1.115 sq m). However, cooling measurements are calculated using the gross square footage required by the cabinets or racks, which is not just the area where cabinets or racks are located. The measurement includes aisles and areas where power distribution, ventilation, and other facility equipment is located. Gross square footage is estimated to be 20 square feet (1.858 sq m) per cabinet or rack.

For example, a data centre may provide 100 watts per square foot of cooling capacity using air conditioners. Based on 100 watts per square foot and 20 square feet (1.858 sq m) per cabinet, each cabinet is allowed a cooling capacity of 2000 watts (100 watts x 20 sq ft) or 2 kW. Remember, 2 kW per cabinet gross square footage in a data center is only an example. Some cabinets might require 3 kW or more of cooling capacity. Some dense computing equipment, such as blade servers in a rack, can require 10 kW or higher of cooling per rack.

Measuring Aisle Airflow Speed

It is also important to consider the intake and discharge airflow required to cool the systems. All of the servers described in this guide draw in ambient air for cooling from the front and discharge heated exhaust air to the rear. Ensure that the air conditioning equipment can adequately move air down the aisles so that heated air does not flow over the cabinets and racks to the front of the systems.

Measure airflow speed in different zones of the floor to determine whether the existing airflow pressure is sufficient to provide the necessary conditioned air to the systems. Take measurements every 13 to 16 feet (4 to 5 m). Measurements taken at lesser distances might not detect a significant pressure difference. A typical airflow speed ranges between 10 to 13 feet (3 to 4 m) per second.

Adequate airflow speed will facilitate the required delivery of conditioned air down the cold aisles and to the systems. If airflow pressure is inadequate, the conditioned air will heat up before it reaches the areas in need of cooling. While an office environment might require only two air changes per hour, the high-density heat load in a data centre can require as many as 30 air changes per hour.

6.1.6 Acclimatization

When determining how long you must allow a system to acclimatise after delivery to the data centre, and before power can be applied to the system without causing damage, you should compare the temperature and humidity of the environment in which the system had been stored to the conditions in the data centre. Equipment damage can occur if the *rate* of temperature or humidity change is too great.

The maximum positive or negative temperature gradient that is recommended for multilayered boards is approximately 2°C (4°F) per hour. The same consideration applies to humidity; it is best to have a slow rate of change.

If it is necessary to compensate for significant temperature or humidity differences between the systems and the data centre, place the systems, in their shipping containers, in a location that has a similar temperature and humidity environment as the data centre. Wait at least 24 hours before removing the systems from their shipping containers to prevent thermal shock and condensation.

6.1.7 Vibration and Shock

Make sure that your installation adequately protects equipment from excessive vibration and shock. When installing systems of different types in the same cabinet or rack, be sure that the overall vibration and shock characteristics do not exceed those of the system with the lowest vibration and shock specifications.

For example, if you are installing two different types of systems in the same cabinet, and one system can tolerate 4 g peak shock, and the other system can tolerate 10 g peak shock, make sure that vibration of your cabinet does not exceed 4 g peak shock.

6.1.8 Contaminants

The impact of contaminants on sensitive electronic equipment is well known, but the most harmful contaminants are often overlooked because they are so small. Most particles smaller than 10 microns, are not visible to the naked eye. Yet it is these particles that are most likely to migrate to areas where they can do damage.

Some sources of contaminants include the following:

Personnel Activity: Human movement within the computer room is probably the single greatest source of contamination in an otherwise clean room. The opening and closing of drawers or hardware panels or any metal-on-metal activity can produce metal filings. Simply walking across the floor can agitate settled contaminants making them airborne and potentially harmful.

Hardware Movement: Hardware installation or reconfiguration involves a great deal of on-floor and sub-floor activity, and settled contaminants can be disturbed, forcing them to become airborne.

Stored Items: Storage and handling of unused equipment or supplies are also a source of contamination. Cardboard boxes or wooded skids shed fibres when moved or handled.

Cleaning Activity: Many chemicals used in office cleaning solutions can damage electronic equipment. Gases from these products or direct contact with the hardware can cause component failure. Solutions that can damage hardware include chlorine-based products, phosphate-based products, bleach-enriched products, petro-chemical-based products, and floor strippers or reconditioners.

6.1.9 Fire Containment

A fire in the data center can cause catastrophic damage to the equipment and the building structure. Take the following precautions to minimize the risk of a fire:

Separate the data centre from other building offices using fire-resistant walls: Ensure that the walls are fire-rated and constructed of noncombustible or limited-combustible materials.

Isolate rooms within the data centre with firewalls: Extend the firewalls from the sub-floor to the structural ceiling.

Install an automatic fire detection system: Use a fire detection system that is sensitive to smoke and other products of combustion rather than solely temperature in the room. Also install manual fire alert stations and provide fire extinguishers throughout the data centre.

Avoid unnecessary storage: Do not store combustible materials in the data center. Remove packing materials and other unnecessary materials as soon as possible.

Check the electrical system insulation periodically: Breakdowns in insulation and the resultant short circuiting can lead to intense heat that can melt materials or cause a fire.

Check heat recoils on the air conditioners periodically: If left unused for a long time, these recoils can collect layers of dust that can ignite when the unit is turned on.

Inspect the data centre perimeter: Look for any openings that could expose the data centre to hazardous areas.

Create detailed disaster response plans: Train personnel how to respond in the event of a fire.

Additional components requiring management for critical operations:

- Electromagnetic Interference (EMI).
- Radio frequency Interference (RFI).
- Vibration.
- Air Quality.

EXERCISE

- 1) What are the environmental requirements of computer system and its peripherals?
- 2) Define IT equipment.
- 3) What is environment management? What are the key components of environment management?
- 4) Explain the diverse locations in which a server can operate within a wide range of environmental conditions.
- 5) What are the three different types of data center temperature and humidity tests?

Instructional Objectives

7.1 Site Preparations and Design of Computer Rooms

7.2 Testing Specifications and Installation of Computer System and Peripherals

7.1 Site Preparations and Design of Computer Rooms

Background

For the implementation of a project, a key component is to setup IT infrastructure. These guidelines help you prepare your site for the delivery and installation of your server. They provide a generic framework for various aspects of site preparation, specifically for setting up server rooms in a local area network enabled environment. These aspects include:

- Site Selection
- Fitting Out Requirements
- Equipment layout planning
- Electrical Requirements
- Air-conditioning System
- Fire Prevention, Detection, and Suppression
- Prevention of Water Leakage
- Physical security

These guidelines can be applied to server rooms of varying capacity. The aim is to provide a generic framework, which can be suitably tailored by the respective complexes based on the specific hardware and network components that are installed. Kindly note that it is imperative to follow the hardware and network installation manuals, which are provided along with the equipment.

7.1.1 Site Selection

When site preparation requirements for a computer/server room are prepared, it is important to understand the infrastructure to be installed and the physical environment in which it will operate. The following information must be sought:

- Weight and dimensions of the computer equipment.
- Electrical requirements of the computer equipment.
- Total heat dissipation and cooling requirements of the computer equipment.
- Types of signal cables.
- Equipment footprint with clearance for maintenance and operation.

The followings are to be considered for site selection:

1. The computer room should be located away from the exterior walls of the building to avoid the heat gain from windows and exterior wall surfaces.
2. In case, exterior windows are unavoidable, windows that are double or triple-glazed and shaded should be used to prevent direct sunlight from entering the computer room.
3. The computer room should be maintained at a positive pressure relative to surrounding spaces.
4. There should be sufficient floor loading capability for computer equipment.
5. A vapor barrier should be installed around the entire computer room envelope to restrain moisture migration. All pipes and cables that penetrate the envelope should be caulked and vapour sealed.
6. Uniform room air distribution system should be maintained in the computer room
7. To avoid contamination, the site should be located away from heavy industries and areas with corrupted air.
8. The computer room should not be on top floor or ground floor or the basement of the building to avoid solar heat absorption or flooding.
9. The computer room should be away from dangerous goods storage, mechanical shock, excessive vibrations and high fire and water risks areas.
10. To eliminate the effect of electromagnetic interference, the computer room should be located away from generator room, lift plant room, or in some cases, the radar or telecommunication control rooms.
11. There should be minimum access by general public and irrelevant personnel to the computer room.

7.1.2 Fitting Out Requirements

All materials to be used in the computer room should be non-combustible, self-extinguishing or fire retardant and have the properties of smooth surface finishing and non-dust shedding. Any pipes and ducts not serving the computer room should be removed.

Walls/Partitions: In the computer room, rigid floor-to-ceiling perimeter walls/partitions having 2-hour fireproof rating should be erected.

Internal Partitions: Partitions inside computer room may be built to the headroom height. Consideration for ample air circulation has to be made. Half-glazed partitions are recommended for partitions inside the computer room. Double-glassed partitions for noise reduction may be considered for printer area.

Wall Finishing: Internal walls are to be finished smoothly with emulsion paint or vinyl wall papers. Finishing of light color can enhance the illumination of the computer room.

Kerb: Concrete kerb of floor void height is required to be built along perimeter walls of the computer room and around the piping of air-conditioning equipment to prevent water penetration to and from the computer room.

Thermal Insulator: Thermal insulator is used on the structural floor and ceiling to prevent heat gain to computer room, especially when bottom discharged type air-conditioners are used. It also helps to save energy and to minimise the running cost of the air-conditioning system. Permanent thermal insulator may be embedded inside the structural floor (sandwich type) during building construction stage or laid on the structural floor (add-on type) for accommodation revised to be computer room. For the latter one, all junctions between the insulator and fixtures are watertight and airtight. Inclinations are required at areas around the floor drains. An alternative is to install the thermal insulator on the structural ceiling of the floor below the computer room.

For thermal insulator not embedded inside the structural floor, the following selection criteria are recommended:

- Thermally insulated.
- Fire and water resistant.
- Dust-free and lightweights.
- Strong enough to be trod.
- Easy to maintain.

Raised Floor: Raised floor is recommended to be used in computer room. It provides the following advantages:

- Acts as an air podium for conditioned air distribution.
- Provides spaces for cable running.
- Enables simple equipment installation and provides flexibility for subsequent layout changes or equipment expansion.
- Protects the interconnecting cables, plugs and power connectors.
- eliminates hazardous cabling underfoot.
- Maintains a cleaner environment.

It is built of individual and interchangeable floor panels sturdily and rigidly above the structural floor. It must be evenly leveled and strong enough to withstand all necessary loads that exert on it. Additional support may be required if the panels are weakened by cutouts. Reference to the loading requirement of the computer equipment should always be made. The floor panel should be made of non-combustible and dust-free material. Its covering material is necessary to be well-bonded, anti-static, thermally insulated and free from scuffing and staining.

Floor Panel Fitting: Cable cutouts and adjustable air grilles are required on designated floor panels for cable connection of computer equipment and air delivery, respectively. The cutouts are protected by black extruded vinyl trimmings at the edges and covered by rubber grommet. The air grilles must have smooth edges and corners and be flush-mounted on the surface of the floor panels.

Ramp: To facilitate equipment transportation, a strong ramp with landing areas at both ends is recommended at the server/computer room. The ramp surface should be built with anti-static, non-combustible and non-slippery materials.

False Ceiling: The requirement of finished headroom is different from one vendor to another. In general, the headroom should not be less than 2.4 m. False ceiling provides tidiness and aesthetic effect to the computer room. It also serves as a plenum for lighting fixtures. The ceiling plate is preferred to be of easy remove and install type for the access of utilities in the ceiling void. Non-combustible and dust-free plates are required. If false ceiling is infeasible, the structural ceiling should be dustproof, waterproof and heat insulated.

Windows and Doors: All windows of the computer room are walled up to avoid direct sunlight and to provide better security and weather protection.

Main Entrance Door: 5-foot wide double-leaf steel door having a 2-hour fireproof rating and secure bolted hinge is recommended. An air lock composed of 2 sets of outward opening and self-closing doors prevents the loss of conditioned air and reduces the influx of dust.

Emergency Exit: The emergency exit requires an outward opening and self-closing steel door. It is also equipped with the same fireproof rating and secure bolted hinge as the main entrance.

Other Doors in the Computer Room: Double-leaf doors are preferred for ancillary machine room and printer room to ease printout movements.

Normal Lighting: Evenly distributed lighting is recommended for the computer room. It is necessary to align the distribution of lights with floor and equipment layouts to avoid shadowy areas caused by tall equipment, cabinets or racks. The lighting, sectional controlled by switches, should be able to switch off when they are not required.

Emergency Lighting: The lighting inside computer room should be connected to essential power supply and 50% of them should be supported by battery. The battery supported lights may be located at the console area, mains control panel areas and passages leading to the main entrance and emergency exit.

Conduit and Trunk: Grounded metal trunks are required to house signal cables from computer room to terminal locations between floors of the same building. Vertical conduit for signal cable of individual terminal equipment is usually connected to the horizontal trunk and ended at skirting level on wall at which termination box is required for cable termination. The termination boxes can be at desk-top level in a terminal room environment. To avoid electromagnetic interference being induced to the signal cables, it is recommended to house the power and signal cables in separate conduits and trunks. If they have to cross each other, they should be crossed in right angle.

Central Control and Monitoring System: The Central Control and Monitoring System is a PC-based integrated system controls and monitors facilities for computer room. With necessary devices to connect various facilities such as air conditioning system, power supply system, fire services system, access control system and CCTV system, etc., to the system, real time information on the performance from these facilities can be collected. This system enables central monitoring of computer centre environmental facility systems remotely.

7.1.3 Equipment Layout Planning

A properly designed equipment layout has the following benefits:

- Easy equipment installation and maintenance;
- Efficient computer operation;
- Efficient air circulation;

- Tidy environment; and
- Feasibility and flexibility of future expansion.

Floor Layout Inside Computer Room: A separate room should be provided for comfortable and silent working environment for computer and data entry operators.

Printer Room: Printers together with a small stationery store area should be in a separate room inside the computer room to reduce dust contamination and noise disturbances to other areas.

Air-conditioning Equipment: There are sufficient spaces for maintenance service for the AHUs. They are, as far as possible, to be located at corners or closed to wall partitions to enable more spaces for computer equipment.

Emergency Exit: The emergency exit is always located at the opposite end of the main entrance.

Technical Manpower Room: A room is required for IT personnel to perform on-site repairing work and to store spare parts of the equipment. It equips with work bench and storage cabinets and power points on the bench or any convenient point. If space is available, the engineer room may be located inside computer room.

Store Room: Store room, preferably on the same floor, provides storage area for computer stationery, consumable, reports and other accessories.

Locker and Changing Room: Computer operators are not allowed to bring their personal belongings into the computer room. In addition, eating and drinking are prohibited in the computer room. It is, therefore, necessary to provide an accommodation outside the room.

Equipment Layout:

1. Cable limitation, equipment operating requirement and operating convenience should be considered when placements of computer equipment is to be designed.
2. An expansion allowance of about 30% of the required area is suggested.
3. The equipment is preferably arranged in parallel rows to smooth the air-flow of the ventilation.
4. The computer equipment is to be aligned with the floor grid.

7.1.4 Electrical Requirements

Power Source: Computer equipment require a “CLEAN” and dedicated power source in conjunction with the use of electrical noise protection device or power conditioner to prevent electrical noise disturbance. For maximum reliability, the independent feeder for the computer equipment must not be shared with other electrical devices.

Basic Power Requirements: The power requirements of different computer equipment may vary. Specifications in the planning manual of the computer equipment should therefore be referred to before the requirements are finalised. The following aspects are to be specified:

Capacity: Sufficient capacity is required for computer loads and future expansions of computer equipment. The capacity of an equipment is expressed in terms of KVA or KW, where

$$\text{KVA} = \text{Voltage} \times \text{Current in Ampere} / 1000$$

$$\text{KW} = \text{KVA} \times \text{Power Factor of that equipment}$$

Always consult computer vendor(s) for the power factors of computer equipment.

Voltage Standard: The nominal voltage for a three-phase and single-phase power supply is 380V and 220V, respectively. However, some equipment may require different voltage. Detailed permissible tolerance of the voltage requirement can be referred to the hardware manuals or computer vendors.

Phase: In most computer installations, a three-phase, four wires and five conductor power supply is provided to the computer equipment power panel. Such a supply consists of three phase wires, one neutral wire and one insulated equipment ground conductor.

Grounding: For personnel safety and protection of equipment from damages and electromagnetic interference, a separated and insulated ground wire is necessary for the computer equipment. Computer vendors should be consulted for detailed specifications of the ground wire.

Power Protection Device: Poor quality of power can seriously affect the performance and reliability of the computer system and may cause damage. Before selecting the power protection device, the load characteristics of the equipment, computer service requirements and reliability must be known.

Uninterruptible Power Supply (UPS): It employs a means for charging a bank of batteries as a backup for the city mains during a short-term power interruption or to allow the computer system to be closed down. Its requirements depend on the computer power loads to be supported, the lead times to start up the backup emergency diesel generator or a tidy close down of the computer system. Using an UPS containing an isolation transformer and a harmonic reduction filter would be the best alternative possible because it may resolve all power line noise problems and provides a continuous power supply during power interruption.

Emergency Power Supply: A generator is to support the UPS in providing emergency power supply to the computer equipment in a prolonged power outage. The need of generator depends on the service requirements of the computer system. However, the generator should also be able to support other essential facilities and equipment such as the air-conditioning system, security and access control system and lighting.

Circuit Breaker: Besides the normal operating current, the circuit breaker of computer equipment handles the in-rush and surge current. Each computer equipment requires a separate circuit and a circuit breaker. Circuit breaker and its related power point/socket should be properly labelled to identify the branch circuit it is controlling.

Power Connector: Power connectors for the computer equipment should conform to the local standard. Their placements are to be planned so that they are always located within about 2m of the machine they supply.

Emergency Power Cutoff Switch: It is an emergency power cut off switch to disconnect the power of all computer equipment in the computer room. The switch is reset by key once it is activated and controlled from locations readily accessible to operators, such as console area and main entrance. The emergency switch is to be properly protected from accidental operation by mistake. Same switch is also required for the air-conditioning system.

Service Power Socket: Sufficient numbers of single-phase square prong service power points with ON/OFF switches are required at appropriate locations in computer room for use by maintenance and service personnel. These power points should be installed at skirting level and separated from the computer panel or feeder.

Automatic Transfer Switch (ATS) is a high availability redundant switch that has two input power cords, one for each AC line, providing redundant power supply to connected equipment. It is designed to

supply power to the connected load from a primary AC source. If the primary source becomes unavailable, it will automatically switch the power supply to the secondary source.

Cables: Cable trays and steel-wire-armored cables are recommended for all underfloor power cables. Power cables have to be laid separately from signal cables in order to avoid any interference. If crossing each other is unavoidable, crossing is suggested at right angle.

7.1.5 Air-conditioning System

Computer equipment is operated in an environment of controlled temperature and relative humidity. The air-conditioning system in the computer room must be able to control the temperature and relative humidity within the specific ranges automatically and independently.

Basic Requirements: An independent air-conditioning system with full backup are required. Spare capacity of 50% is recommended for anticipated expansion. Power source of the system should be separated from those for computer equipment and connected to emergency power supply. The system can be either water-cooled or air-cooled depending on the equipment specifications.

Cooling Capacity: Determination of the cooling capacity of a computer room mainly depends on the following factors:

1. Total heat dissipation of the equipment (always consult vendor for specifications).
2. Volume of the location.
3. Room and equipment layouts.
4. Anticipated expansion.
5. Heat gains and losses through walls, floor and ceiling.
6. Personnel working inside.

Temperature and Relative Humidity Ranges: The operating ranges of temperature and relative humidity for computer equipment are usually $20^{\circ}\text{C} \pm 3^{\circ}\text{C}$ and $50\% \pm 10\%$; respectively with the maximum rate of changes at 3°C and 6% per hour.

Air Distribution Method: Air distribution in computer room is usually classified into “Raised Floor” and “Non-raised Floor” distributions. **Raised Floor Distribution system** distributes the conditioned air through the floor void to the computer equipment via air grilles or perforated floor panels. The heat dissipate vents of most computer equipment are designed to suit such distribution as it is efficient in air circulation. In **Non-raised Floor Distribution**, air is distributed either from ceiling via diffusers or simply across the floor. Since air circulation of such distribution is not efficient, it is only recommended for small setups.

Air Cleanliness and Fresh Air Intake: The intake of adequate amount of filtered and pre-treated fresh air to the computer room is required. The location of the fresh air inlet should be carefully planned so that the intake of polluted air into the computer room can be avoided. Dust contamination inside the computer room can be minimised by using high efficiency filters. Detail requirement on dust level can be referred to vendor’s documentation.

Inter-switchability: In addition to its capability of simultaneous operation, manual and automatic switching between the normal and standby units of the entire air-conditioning system is preferred.

Water Supply: If the computer room is operated with water-cooled chiller plant, an automatic filled water tank which is not affected by water supply suspension or ration is required.

Power Supply: Power supply of air-conditioning units must not be connected to the computer loads.

Emergency Supply: It is essential to provide emergency power supply to the air-conditioning system as long as the emergency power supply is provided to computer equipment.

Emergency Power Cut off: Power supply of the entire system, including the fresh air intake unit is cut off automatically when fire extinguishing system is actuated. The installation of manual emergency power cut off switch is to shut down the system in case of emergency. It is preferred to be installed near the console area and duplicated at the main entrance.

System Monitoring: The audible and visual alarm panels of the air-conditioning system for the computer system and its ancillary machines (i.e. UPS Room) are to be installed in computer room at master console area to report the operating status and faults of all system components. The alarm/indicators include high/low temperature and relative humidity, filter status and chiller plant status.

Perforated Floor Panel: Perforated floor panel, equipped with air-flow control feature, is recommended for distribution of conditioned air in raised floor distribution system. It is more advantageous than air grille because it enables free placement for heavy computer equipment and has no frame protrusion.

Temperature/Humidity Recorder: Electrical temperature/humidity recorders are required in the computer room to provide 7-day continuous recording of the environmental conditions. They are wall-mounted at the locations near the computer equipment or other appropriate spots and must have visual and/or audible alarms.

Automatic Power Cut off Facility to Computer Equipment: An adjustable temperature sensing system with audible and visual alarms is required for computer room and power conditioner room. If the threshold limit is exceeded, a facility is required to cut the power supply to the computer equipment automatically. This facility is capable to be operated manually. Reset switch of the automatic power tripped equipment is required to stop the equipment from “uncontrolled” power ON/OFF due to changes of temperature.

Store Room: A normal office air-conditioning system is required for the store room of computer consumable such as magnetic media, printer ribbons and continuous stationery, etc. Acclimatisation to the computer store is necessary before they are put into use.

Power Conditioner Room: Power conditioner, such as UPS, is a heat generating device and is usually housed in a separate room away from the computer equipment. A reliable air-conditioning system with backup is required.

7.1.6 Fire Prevention, Detection and Suppression

In order to minimise fire damages to computer equipment, the equipment and furniture used inside the computer room should, as far as possible, be made of non-combustible material or at least having minimal fire propagation or smoke generating properties.

Storage of Stationery: The storage of bulky volume of continuous stationery must be fire protected and be kept away from computer room. Amount of continuous stationery stored in computer room must not exceed the consumption of a shift.

Ancillary Equipment: The accommodation for power conditioner, emergency diesel generator and its fuel storage must be away from computer room.

Ducts: The air ducts should be equipped with automatic fusible-link fire dampers.

Detecting Device and System:

Detector: A two-stage detection system, consisting of two sets of detectors and alarm signals in cross-zone operation, is required. Detectors should be located at the headroom, inside the ceiling void and floor void of the computer room. Detectors can be smoke detectors or together with heat detectors.

Detecting System: First fire alarm will cut power to air-conditioning system and be transmitted to the building management office and the nearest fire station. Second alarm cuts all power supply to the computer room and the fire suppression system will be triggered off after a pre-set time interval.

Fire Suppression System: Various options include:

- Gas Flooding System.
- Portable Gas Fire Extinguisher.

Design Criteria:

- The system should always be put to 'AUTO' mode under normal circumstances to fully protect the computer room against fire hazards and to cope with Fire Authority's practice. 'MANUAL' mode is only switched on when the system is under repair. **Manual mode** – In case of fire the system will have to be triggered off manually after all operation staff are evacuated. **Automatic mode** – In case of fire the system will be controlled by the detection system. System will be triggered off after a pre-set time interval when detectors of both zones sense a fire and activate detection system.
- No matter the system is in manual or automatic mode, an elapse time of at least 30 seconds is required for personnel evacuation before the gas is released. To facilitate evacuation, all emergency exits should be labelled with battery supported illumination. Furthermore, design of the door should be such that it can only be opened from the inside. The use of "push bar" or similar latch is preferred so that the door can be opened easily. However, to avoid the door from being used at times other than emergency, the door should be fitted with a burglar alarm.
- All duct work, doors, windows and any other air passages must be sealed off and exhaust air fans should then be installed. This is because if the protected area is not airtight, the pressurised extinguishing gas may dissipate, thus reducing the effectiveness of the system.
- The system is capable to be operated under all circumstances, including power failure. Regular maintenance and cleaning are necessary for the fire detection system and corresponding accessories.
- Portable gas fire extinguishers should be installed at various locations. The locations should be clearly marked to enable easy fetching of the extinguishers. All portable fire extinguishers should be periodically inspected and refilled by the supplier. The next inspection date should be clearly marked on the extinguishers.

Monitoring: The master alarm/indicator panel(s) of the system is/are to be installed inside the computer room. Audible and visual alarms are required to indicate the detection of fire. Fire alarms of the building must be provided inside computer room to alert operators of fire on other floors. Diagrams showing the locations of hose reels, fire exits, fire extinguishers and evacuation paths should be posted inside computer room. The fire extinguishing system is required to be accommodated in a separate room or compartment near the computer room.

7.1.7 Prevention of Water Leakage

- Concrete kerb is required along the perimeter of the computer room and power conditioner room.
- All unnecessary plumbing is to be removed away from computer room.
- Waterproof power connectors are to be used for underfloor power connections.
- All ducts, trunks and pipes for cables should be water-tight and be able to stop the water being led by them.
- All underfloor fixtures should be away from the floor drains.
- Waterproof treatment is required for internal wall surfaces, concrete ceiling and structural floor.
- Water detection system in the floor void with audible and visual alarm panel showing one or more locations of water threats is required in computer room. If the system is not a linear detection type, mimic diagram showing the locations of the water detectors is necessary.

7.1.8 Physical Security

Access Control System - Installation of Lock If the main entrance has 2 sets of door, the first set (outer) may be equipped with a cipher lock only. This lock is operated by entering a correct cipher code. The second (inner) set can be controlled by a cipher/cardkey lock. Both locks may be door-mounted or wall-mounted but the control circuit units are housed in locked metal cases inside computer room.

Cipher Code Operation: The cipher locks at both entrances must allow operations made by common code and individual codes. Changes of cipher codes are performed locally at the master control units of the locking system. The change of cipher code does not affect the information encoded in the magnetic cardkeys.

Power Supply to the Lock: A 24-hour battery power backup is required for the access control system including the electric door lock(s). The access control system should also be connected to the UPS if it is installed.

Door Lock: Heavy-duty electric lock is recommended for the main entrance doors. With time delay setting, the lock would effect after time is over. The lock must be fail-safe type. Panic bolt is recommended at emergency exits.

Surveillance System:

Closed Circuit Television System (CCTV): CCTV is used to monitor the security as well as operating environment of the computer room. The monitor unit is capable of programmable switching for selection of pictures for a multi-camera CCTV system. The requirement of the CCTV system depends on the system security level and mode of operation of the computer system.

Digital Video Recording System: It is a triplex (real time, playback and record) video recording system, which allows video monitoring, recording and playback simultaneously over the computer network or other telecommunications channels like phone line or mobile network.

Intercommunication System (INTERCOM): The master unit of the intercommunication system is placed at console area and the slave units are placed at the outer main entrance and other necessary places to provide a direct and clear communication between all functional areas.

Burglar Alarm System: To protect the computer room and other external restricted premises from unauthorised access or break-in, a burglar alarm system may be installed at the main entrances and

all exits. The alarm system may also provide “Door-Remains-Open” warnings to operators. 24 hours standby battery supply to the operation of the burglar alarm is necessary to cater for power outage. The system should allow each protected door to have both ACCESS and PROTECT modes. Mode setting should be done on the master panel inside computer room. An alarm and indicating mimic panel showing every protected door is required in computer room. Every break-in of these doors will give audible and visual signals to the master panel inside computer room and the building management office or even the police station via professional security company.

Security Review for Computer Room: Physical security of a computer room is the most vital aspect for the expensive computer hardware and invaluable computer data being stored.

Data communication trunks are trunks for data communication cables and telephone lines of the network. Special care is required to secure the access of the data communication cables and telephone lines in order to prevent malicious damage, interception and attachment of the cables and lines. Escort of computer vendors or telecommunication service provider is required in the course of the installation work.

7.2 Testing Specifications and Installation of Computer Systems and Peripherals

7.2.1 Validation Overview

Validation of computer systems is not a once off event. Annex 11 of the European GMP Directive is very clear about this: Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and modifying”.

For new systems validation starts when a user department has a need for a new computer system and thinks about how the system can solve an existing problem. For an existing system it starts when the system owner gets the task of bringing the system into a validated state. Validation ends when the system is retired and all-important quality data is successfully migrated to the new system. Important steps in between are validation planning, defining user requirements, functional specifications, design specifications, validation during development, vendor assessment for purchased systems, installation, initial and ongoing testing and change control. In other words, computer systems should be validated during the entire life of the system.

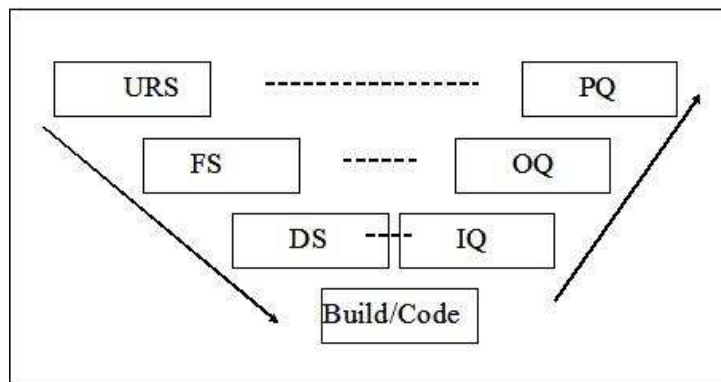


Figure 7.1: V-Lifecycle models

Because of the complexity and the long time span of computer validation the process is typically broken down into life cycle phases. Several life cycle models have been described in literature. One model that is frequently used is the V-model as shown in Figure 7.1.

This model comprises of User Requirement Specifications (URS), Functional Specifications (FS), Design Specifications (DS), development and testing of code, Installation Qualification (IQ), Operational Qualification (OQ) and Performance Qualification (PQ).

The V-Model as described above is quite good if the validation process also includes software development. However, it does not address some very important steps, for example, vendor assessment. It also looks quite complex for true commercial off the shelf system with no code development for customisation. Phases like design specification or code development and code testing are not necessary. For such systems the 4Q model is recommended with just four phases: design qualification (DQ), installation qualification (IQ), operational qualification (OQ), and performance qualification (PQ). The process is illustrated in Figure 7.2.

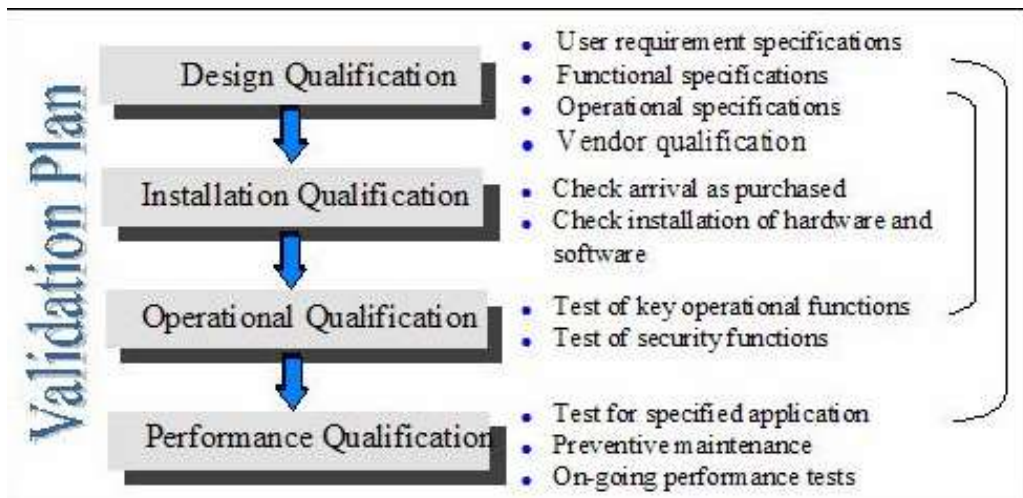


Figure 7.2: 4Q-Lifecycle model

Both the 4Q and the V-model do not address the retirement phase. The 4Q model is also not suitable when systems need to be configured for specific applications or when additional software is required that is not included in the standard product and is developed by the user's firm or by a 3rd party. In this case; a life cycle model that combines system development and system integration is preferred. An example is shown in Figure 7.3.

User representatives define User or System Requirement Specifications (URS, SRS). If there is no vendor that offers a commercial system the software needs to be developed and validated by following the steps on the left side of the diagram. Programmers develop functional specifications, design specifications and the code and perform testing in all development phases under supervision of the quality assurance.

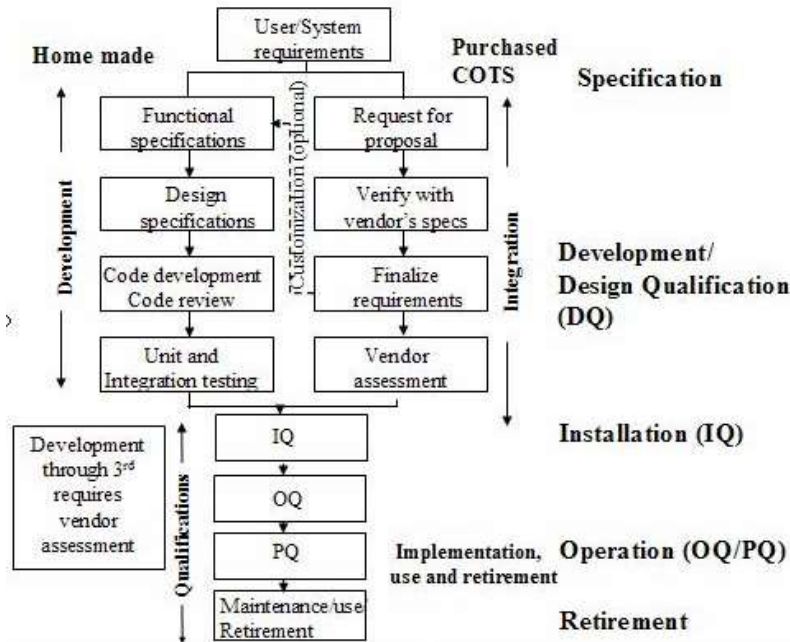


Figure 7.3: System Integration combined with System Development

When commercial systems are available either the SRS or a special Request for Proposal (RFP) is sent to one or more vendors (see right side of the diagram). Vendors either respond to each requirement or with a set of functional specifications of a system that is most suitable for the user's requirements. Users compare the vendor's responses with their own requirements. If none of the vendors meet all user requirements, the requirements may be adjusted to the best fit or additional software is written to fulfil the user requirements following the development cycle on the left side of the diagram. The vendor that best meets the user's technical and business requirements is selected and qualified.

The extent of validation depends on the complexity of the computer system. The extent of validation at the user's site also depends on the widespread use of the same software product and version. The more standard software is used and the less customisation made for such software the less testing is required by individual users. GAMP has developed software categories based on the level of customisation. In total there are five categories. Category one and two define operating systems and firmware of automated systems. In the context of these primer only categories three to five are of interest. They are described in Table 7.1. Each computer system should be associated to one of the three categories.

Category	Description
GAMP 3	Standard software package. No customisation. Examples: MS Word (without VBA scripts). Computer controlled spectrophotometers.

GAMP 4	Standard software package. Customisation of configuration. Examples: LIMS, Excel spreadsheet application where formulae and/or input data are linked to specific cells. Networked data systems.
GAMP 5	Custom software package. Either all software or a part or the complete package has been developed for a specific user and application. Examples: Add-ons to GAMP Categories 3 and 4, Excel® with VBA scripts.

Table 7.1

7.2.2 Validation Master Plan and Project Plan

All validation activities should be described in a validation master plan which should provide a framework for thorough and consistent validation. A validation master plan is officially required by Annex 15 to the European GMP Directive. FDA regulations and guidelines don't mandate a validation master plan; however, inspectors want to know what the company's approach towards validation is. The validation master plan is an ideal tool to communicate this approach both internally and to inspectors. It also ensures consistent implementation of validation practices and makes validation activities much more efficient. In case there are any questions as to why things have been done or not done, the validation master plan should give the answer.

Within an organisation a validation master plan can be developed for:

- Multiple sites.
- Single sites.
- Single locations.
- Single system categories.
- Department categories, e.g., for development departments.

Computer Validation master plans should include:

1. Introduction with a scope of the plan, e.g., sites, systems, processes.
2. Responsibilities by function.
3. Related documents, e.g., risk management plans.
4. Products/processes to be validated and/or qualified.
5. Validation approach, e.g., system life cycle approach.
6. Risk management approach with examples of risk categories and recommended validation tasks for different categories.
7. Vendor management.
8. Steps for Computer System Validation with examples on type and extent of testing, for example, for IQ, OQ and PQ.
9. Handling existing computer systems.
10. Validation of Macros and spreadsheet calculations.
11. Qualification of network infrastructure.

12. Configuration management and change control procedures and templates.
13. Back-up and recovery.
14. Error handling and corrective actions.
15. Re-qualification criteria.
16. Contingency planning and disaster recovery.
17. Maintenance and support.
18. System retirement.
19. Training plans (e.g., system operation, compliance).
20. Validation deliverables and other documentation.
21. Templates and references to SOPs2.
22. Glossary.

For larger projects a detailed individual validation project plan should be developed. An example would be implementing a Laboratory Information Management (LIMS) system or networked chromatographic data system. This plan is derived from the validation master plan using the principles and templates of the master plan. It formalises qualification and validation and outlines what is to be done in order to get a specific system into compliance. For inspectors it is a first indication on which control a department has over a specific computer system and it also gives a first impression of the validation quality.

A validation project plan should include sections on:

- Scope of the system, what it includes, what it doesn't include.
- System description.
- Validation approach.
- Assumptions, limitations and exclusions.
- Responsibilities.
- Risk assessment.
- Risk based test strategy and approach for validation steps, e.g., DQ, IQ, OQ, PQ.
- Ongoing performance control.
- Configuration management and change control.
- Handling system security * Data back-up and recovery.
- Contingency planning.
- Error handling.
- References to other documents.
- Timeline and deliverables for each phase.

7.2.3 Design Qualification and Specifications

“Design qualification (DQ) defines the functional and operational specifications of the instrument and details the conscious decisions in the selection of the supplier”. DQ should ensure that computer systems

have all the necessary functions and performance criteria that will enable them to be successfully implemented for the intended application and to meet business requirements. Errors in DQ can have a tremendous technical and business impact, and therefore a sufficient amount of time and resources should be invested in the DQ phase. For example, setting wrong functional specifications can substantially increase the workload for OQ testing, adding missing functions at a later stage will be much more expensive than including them in the initial specifications and selecting a vendor with insufficient support capability can decrease instrument up-time with a negative business impact.

Steps for design specification normally include:

- Description of the task the computer system is expected to perform.
- Description of the intended use of the system.
- Description of the intended environment.
- Includes network environment).
- Preliminary selection of the system requirement specifications, functional specifications and vendor.
- Vendor assessment.
- Final selection of the system requirement specifications and functional specification
- Final selection and supplier.
- Development and documentation of final system specifications.

System Requirement Specifications (SRS) or User Requirement Specifications (URS) are usually written by user representatives. The vendor's specification sheets can be used as guidelines. However, it is not recommended to simply writing up the vendor's specifications because typically commercial software has more functions than the user ever will need. On the other hand there should be documented evidence that the system performs all specified functions and compliance to the specifications must be verified later on in the process during operational qualification and performance qualification. Specifying too many functions will significantly increase the workload for OQ. The development of requirement specifications should follow a well documented procedure. Most important is to involve representatives of all user departments in this process.

User requirements should have a couple of key attributes. They should be:

- Necessary: Unnecessary functions will increase development, validation, support and maintenance costs.
- Complete: Adding missing functions at a later stage will be much more expensive than including them initially.
- Feasible: Specified functions that can not be implemented will delay the project.
- Accurate: Inaccurately specified functions will not solve the application's problem.
- Unambiguous to avoid guessing and wrong interpretation by the developer.
- Specific: to avoid wrong interpretation by the developer.
- Testable. Functions that are not testable can not be validated.
- Uniquely identified: This helps to link specifications to test cases.
- Functional specifications answer the question: what functions does the system need to comply with users requirements. They are normally written by the developer of the system and should be reviewed by the user.

Design specifications are also written by the developer. They answer the question: how does the system implement specified functions? They should be formally reviewed by a team of developers under the supervision of QA.

7.2.4 Vendor Assessment

Validation of software and computerised systems covers the complete lifecycle of the products which includes validation during design and development. When software and computer systems are purchased from vendors, the user is still responsible for the overall validation.

FDA's guide on Principles of Software Validation states this very clearly: "Where the software is developed by someone other than the device manufacturer (e.g., off-the-shelf software) the software developer may not be directly responsible for compliance with FDA regulations. In that case, the party with regulatory responsibility (i.e., the device manufacturer) needs to assess the adequacy of the off-the-shelf software developer's activities and determine what additional efforts are needed to establish that the software is validated for the device manufacturer's intended use".

The objective of vendor qualification is to get assurance that the vendor's products development and manufacturing practices meet the requirements of the user's firm for quality. For software development this usually means that the software is developed and validated following documented procedures.

Vendor assessment should answer the questions: "What type of assurance do you have that the software has been validated during development?" or "How can you be sure that the software vendor did follow a quality assurance programme?" Depending on the risk and impact on (drug) product quality answers can be derived from.

1. Documentation of experience with the vendor: Experience may come from the product under consideration or from other products.
2. External references: Useful if there is no experience within the vendor within your company.
3. Assessment checklists (mail audits): Use checklists available within your company, through public organisations, e.g., PDA and from private authors.
4. 3rd party audits: Gives an independent assessment of the quality system and/or product development.
5. Direct vendor audits: Gives a good picture on the vendors quality system and software development and validation practices.

Assessment cost increase from 1 to 5 and the final procedure should be based on justified and documented risk assessment. Such risk assessment includes two parts:

1. Product risk.
2. Vendor risk .

Factors for product risk include:

- System complexity.
- Number of systems to be purchased.
- Maturity of the system.
- Level of networking.
- Influence on other systems, e.g., through networks.

- Impact of the system on drug quality.
- Impact of the system on business continuity.
- Level of customisation.

Factors for vendor risk include:

- Size of company.
- Company history.
- Future outlook.
- Representation in target industry, e.g., Pharmaceutical.
- Experience with the vendor.

Risk factors are estimated for the computer system (product) and the vendor and entered in table like in Figure 7.4.

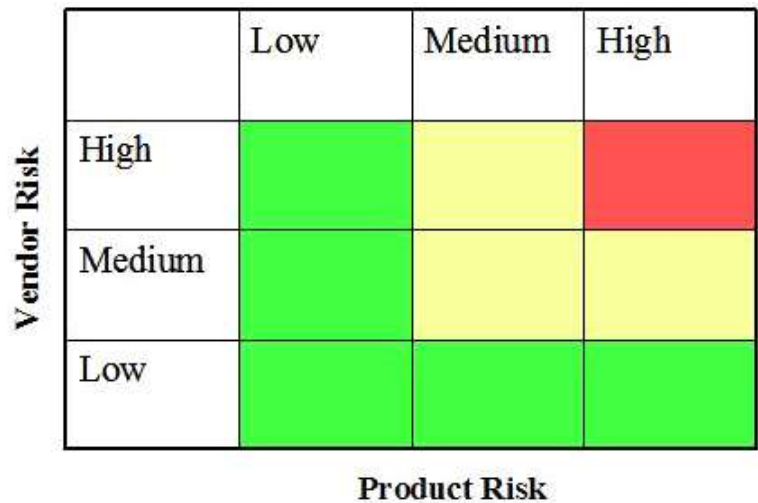


Figure 7.4: Vendor Risk vs Product Risk

Most critical is the red area with high product and high vendor risk. This scenario would require a vendor audit either through the user firm or through a trusted 3rd party. On the other hand green areas could be handled by a one to two page document describing who the vendor and why you did select the vendor.

Vendors in the yellow area could be assessed through mail audits supported by good internal or external references. Results of the vendor audits should be documented following a standardised ranking scheme. An example is shown in Table 7.2.

The results of the vendor assessment and any vendor audit should be well communicated within a company to avoid duplication of audits of the same vendor by different departments or sites. This can be achieved by developing a company wide repository with entries of all vendor assessment activities. The whole process of vendor assessment and audits should be controlled by documented procedures.

Rating	Meaning	Interpretation
3	Excellent	Vendor procedures and practices are above average
2	Adequate	Vendor procedures and practices are about average
1	Poor	Vendor procedures and practices are below average and need to be improved
0	Unsatisfactory	Vendor procedures and practices are unacceptable
N/A	Not Applicable	Question is not applicable to the type of function or service

Table: 7.2

7.2.5 Installation Qualification

Installation qualification establishes that the computer system is received as designed and specified, that it is properly installed in the selected environment, and that this environment is suitable for the operation and use of the instrument. The list below includes steps as recommended before and during installation.

Before Installation

- Obtain manufacturer's recommendations for installation site requirements.
- Check the site for the fulfilment of the manufacturer's recommendations (utilities such as electricity, water and gases and environmental conditions such as humidity, temperature, vibration level and dust).

During Installation

- Compare computer hardware and software, as received, with purchase order (including software, accessories, and spare parts).
- Check documentation for completeness (operating manuals, maintenance instructions, standard operating procedures for testing, safety and validation certificates).
- Check computer hardware and peripherals for any damage.
- Install hardware (computer, peripherals, network devices, cables).
- Install software on computer following the manufacturer's recommendation.
- Verify correct software installation, e.g., are all files accurately copied on the computer hard disk. Utilities to do this should be included in the software itself.
- Make back-up copy of software.
- Configure network devices and peripherals, e.g. printers and equipment modules.
- Identify and make a list with a description of all hardware, include drawings where appropriate, e.g., for networked data systems.
- Make a list with a description of all software installed on the computer.
- Store configuration settings either electronically or on paper.
- List equipment manuals.

- Prepare an installation report.

Installation and installation qualification (IQ) of larger commercial system is normally performed by a supplier's representative. Both the supplier's representative and a representative of the user's form should sign off the IQ documents.

7.2.6 Operational Qualification

“Operational qualification (OQ) is the process of demonstrating that a computer system will function according to its functional specifications in the selected environment.

Before OQ testing is done, one should always consider what the computer system will be used for. There must a clear link between testing as part of OQ and requirement specifications as developed in DQ phase. Testing may be quite extensive if the computer system is complex and if there is little or no information from the supplier on what tests have been performed at the supplier's site. Extent of testing should be based on a justified and documented risk assessment. Criteria are:

- Impact on product quality.
- Impact on business continuity.
- Complexity of system;
- Information from the vendor on type of tests and test environment.
- Level of customisation

Most extensive tests are necessary if the system has been developed for a specific user. In this case the user should test all functions. For commercial off-the-shelf systems that come with a validation certificate, only tests should be done of functions that are highly critical for the operation or that can be influenced by the environment. Examples are data acquisition over relatively long distance from analytical instruments at high acquisition rate. Specific user configurations should also be tested, for example correct settings of IP addresses of network devices should be verified through connectivity testing.

Based on the risk factors above a system risk factor should be estimated. Extent of testing should be defined for each risk level in a risk management master plan or in the 'risk' section of the validation master plan. An example is shown in the table below. The level of customization is expressed through the GAMP Categories 3, 4, or 5. Category three is standard software without customisation and configuration setting. Category 4 is a configurable system and Category 5 a fully customized system. Extent of testing increases from the left lower site (low risk, standard system) to the right upper site (high risk, full customisation).

System	GAMP3	GAMP4	GAMP5
High risk	Test critical functions. Link tests to requirements.	Test critical standard functions. Test all non standard functions	Test critical standard functions. Test all non standard functions Link tests to requirements.

Medium risk	Test critical functions.	Test all critical standard and non standard functions Link tests to requirements.	Test critical standard functions. Test all non standard functions. Link tests to requirements.
Low risk	No testing	Test critical non standard functions.	Test critical non standard functions.

Table: 7.3

Proper functioning of back-up and recovery and security functions like access control to the computer system and to data should also be tested.. Full OQ test should be performed before the system is used initially and at regular intervals, e.g., for chromatographic data systems about once a year and after major system updates. Partial OQ tests should be performed after minor system updates.

Tests should be quantitative. This means inspectors would not only expect a test protocol with test items and pass/fail information but also expected results, acceptance criteria and actual results. An example for a test protocol template is shown in figure 8.

Tests should be linked to requirement specifications through a test traceability matrix. A template for such a matrix is the table below should help to easily find a test protocol for a specific test requirement.

The matrix can be documented on paper format but for larger projects it is recommended to use electronic document management systems. This can range from simple Word tables to data bases and software specifically developed for managing traceability matrices.

Requirement Number	Requirement	Test ID
1.1	Example 1	4.1, 4.3
1.2	Example 2	1.2
1.3	Example 3	3.1
1.4	Example 4	3.1, 4.1

Table: 7.4

7.2.7 Performance Qualification

“Performance Qualification (PQ) is the process of demonstrating that a system consistently performs according to a specification appropriate for its routine use”. Important here is the word ‘consistently’. Important for consistent computer system performance are regular preventive maintenance, e.g., removal of temporary files and making changes to a system in a controlled manner and regular testing.

In practice, PQ can mean testing the system with the entire application. For a computerised analytical system this can mean, for example, running system suitability testing, where critical key system performance characteristics are measured and compared with documented, preset limits.

PQ activities normally can include:

- Complete system test to proof that the application works as intended. For example for a computerised analytical system this can mean running a well characterised sample through the system and compare the results with a result previously obtained.
- Regression testing: reprocessing of data files and compare the result with previous result.
- Regular removal of temporary files.
- Regular virus scan.
- Auditing computer systems.

Most efficient is to use software for automated regression testing. The software runs typical data sets through a series of applications and calculates and stores the final result using processing parameters as defined by the user. During regression testing the data are processed again and results are compared with previously recorded results. Normally such tests don't take more than five minutes but give assurance that they key functions of the system work as intended.

7.2.8 Configuration Management and Control

Any changes to specifications, programming codes or computer hardware should follow written procedures and be documented. Changes may be initiated because errors have been found in the programme or because additional or different software functions or hardware may be desirable. Requests for changes should be submitted by users and authorised by the user's supervisor or department manager. For initiation, authorisation and documentation of changes forms should be used. An example is shown in Figure 7.5.

Form ID	Change ID	Item ID
Initiator	Date	Location
Description of change	<i>Include reason for change</i>	
Priority	high medium low	
Impact assessment	<i>Business, technical, validation</i>	
Risk assessment	Risk, likelihood, severity, recovery	
Regulatory notification required? Yes No		
Test plan		
Roll back plan	<i>In case of severe problems</i>	
Change approval	Yes No Comments	
Approved by	Name Signature Date	

Figure 7.5: Change request Form

Most important is that changes should follow standard procedures for initiation, authorization, implementing, testing and documenting. All activities should be planned in the validation project plan and documented in the validation report.

After any changes the program should be tested. Full testing should be done for the part of the program that has been changed and regression testing should be done for the entire programme.

7.2.9 Validation report and Other Documents

When the validation project is completed a validation summary report should be generated by the system owner. The report documents the outcome of the validation project. The validation report should mirror the validation project plan and should include:

- A brief description of the system.
- Identification of the system and all software versions that were tested.
- Description of hardware used.
- Major project activities.
- Listing of test protocols, test results and conclusions.
- Statement on system status prior to release.
- List of all major or critical issues and deviations with risk assessment and corrective actions.
Statement that all tasks have been performed as defined in the project plan.
- Statement that validation has been performed according to the documented procedures.
- Listing of all deliverables.
- Final approval or rejection statement.

The validation report should be reviewed, approved and signed by QA and the system owner.

EXERCISE

- 1) What are the aspects of site preparation and design of computer rooms?
- 2) What is the following information required when site preparation requirements for a computer/server room are prepared?
- 3) What are the fitting requirements needed for the material to be used in the computer room?
- 4) What is the basic power requirements considered for computer room?
- 5) What are the steps needed for fire prevention and detection?

Multiple Choice Questions

1. Maintenance is defined as those activities and actions that directly retain the proper operation of an item or restore that operation when it is interrupted by failure or some other anomaly.
 - a) True
 - b) False
2. Maintenance types consist of a set of maintenance activities:
 - a) Inspection
 - b) Monitoring
 - c) Routine maintenance and repair
 - d) Overhaul and rebuilding
 - e) All of the above
3. What are the levels of maintenance to be carried out at a specific indenture level?
 - a) 4
 - b) 5
 - c) 3
 - d) 9
4. Mean Time Between Failure (MTBF) is a reliability term used loosely throughout many industries and has become widely abused.
 - a) True
 - b) False
5. Shielding theory is based on two fundamental mechanisms, reflection loss and absorption loss.
 - a) True
 - b) False
6. The fault location procedure will comprise a study of the literature relevant to:
 - a) Servicing, maintenance and repairs
 - b) Pinpointing the cause of the fault
 - c) a and b
 - d) None of the above

7. Fault Correction consists of replacing and repairing the faulty component.
 - a) True
 - b) False
8. The most commonly needed fault-finding aids are:
 - a) Service and maintenance manuals and instruction manuals
 - b) Test and measuring instruments
 - c) Special tools (instruments, mechanical tools)
 - d) All of the above
9. A majority of the system faults can be located and rectified by using these instruments:
 - a) Multimeter
 - b) Oscilloscope
 - c) Signal generator or pulse generator or function generator
 - d) All of the above
10. A few hardware diagnostic tools can be very helpful in isolating defective hardware components:
 - a) Software diagnostic disk
 - b) Multimeter
 - c) Cable tester
 - d) POST card
 - e) All of the above
11. An effective system of troubleshooting should be quite logical for the following these points:
 - a) Know your equipment
 - b) Think before you act
 - c) Establish a general troubleshooting procedure
 - d) All of the above
12. An electronic system may compromise several functional parts which may include:
 - a) Power supplies
 - b) Amplification
 - c) Generation
 - d) Transmission
 - e) All of the above
13. The half-split method is extremely useful when the system is made up of a large number of blocks in series.
 - a) True
 - b) False
14. In convergent paths, two or more input lines feed a circuit block.
 - a) True
 - b) False

15. The analysis of simple circuits was carried by:
 - a) Kirchhoff's laws
 - b) Ohm's law
 - c) None of the above
 - d) a and b
16. Modern motherboards include, at a minimum:
 - a) Sockets (or slots) in which one or more microprocessors are installed
 - b) Slots into which the system's main memory is installed (typically in the form of DIMM modules containing DRAM chips)
 - c) A chipset which forms an interface between the CPU's front-side bus, main memory, and peripheral buses
 - d) Non-volatile memory chips (usually Flash ROM in modern motherboards) containing the system's firmware or BIOS
 - e) All of the above
17. A floppy drive may not work because of one or more of the below reasons:
 - a) Bad floppy diskette
 - b) Not setup in CMOS
 - c) Conflicition with other hardware
 - d) Bad drivers and hardware
 - e) All of the above
18. A Hard Disk Drive (HDD) is commonly referred to as:
 - a) Hard drive
 - b) Hard disk
 - c) Fixed disk drive
 - d) All of the above
19. If the machine uses a SCSI drive, there are two factors with which to be concerned:
 - a) Termination
 - b) ID
 - c) a and c
 - d) None of the above
20. How many different types of printers are utilised that prints text or illustrations on paper?
 - a) 7
 - b) 5
 - c) 4
 - d) 2
21. An alternative method is the use of a type of saturating transformer called:
 - a) Ferro-resonant transformer
 - b) Constant-voltage transformer

- c) a and b
 - d) None of the above
22. The uses of CVT are:
- a) Office and business equipment
 - b) Process controls medical equipment
 - c) a and b
 - d) only a
23. The advantage of CVT is:
- a) Good isolation of load equipment from line noise and surges
 - b) Outage voltage regulation is smooth
 - c) Loose connections
 - d) Switch off the CVT when in use to reduce iron and heat losses
24. There are various common power problems that UPS units are used to correct:
- a) Power failure
 - b) Voltage sag and spike
 - c) Line noise
 - d) Harmonic distortion
 - e) All of the above
25. The general categories of modern UPS systems are:
- a) On-line
 - b) Line-interactive
 - c) Standby
 - d) All of the above
26. Environment Management is the management of the physical environment within which IT infrastructure is housed.
- a) True
 - b) False
27. The complexity of the IT infrastructure in use within the organisation include:
- a) PC desktops and peripherals
 - b) Computer services
 - c) Networking equipment, telephone equipment and cabling
 - d) Data backups (tapes, CDs)
 - e) All of the above
28. What are the different types of data center temperature and humidity tests suggested?
- a) Facility environmental tests
 - b) Equipment installation environmental tests
 - c) Equipment failure environmental tests
 - d) All of the above

29. What are the different types of sources o contaminants?
- a) Personnel activity
 - b) Hardware movement
 - c) Stored items
 - d) Cleaning activity
 - e) All of the above
30. Additional components requiring management for critical operations are:
- a) Electromagnetic interference (EMI)
 - b) Radio-frequency interference (RFI)
 - c) Vibration
 - d) Air quality
 - e) All of the above
31. Explain the aspects of a generic framework for various aspects of site preparation, specifically for setting up server rooms in a local area network enabled environment.
- a) Site selection
 - b) Fitting out requirements
 - c) Equipment layout planning
 - d) Electrical requirements
 - e) All of the above
32. In the computer room, rigid floor-to-ceiling perimeter walls/partitions having 2-hour fireproof rating should be erected.
- a) True
 - b) False
33. What are the benefits of a properly designed equipment layout?
- a) Easy equipment installation and maintenance
 - b) Efficient computer operation and air circulation
 - c) Tidy environment
 - d) Feasibility and flexibility of future expansion
 - e) All of the above
34. The air-conditioning system in the computer room must be able to control the temperature and relative humidity within the specific ranges automatically and independently.
- a) True
 - b) False
35. What are the parts that include assessment cost and the final procedure should be based on justified and documented risk assessment?
- a) Product risk
 - b) Vendor risk
 - c) a and b
 - d) None of the above

ANSWERS

1(a), 2(e), 3(b), 4(a), 5(a), 6(c), 7(a), 8(d), 9(d), 10(e), 11(d),
12(e), 13(a), 14(a), 15(d), 16(e), 17(e), 18(d), 19(c), 20(a), 21(c), 22(c),
23(a and b), 24(e), 25(d), 26(a), 27(e), 28(d), 29(e), 30(e), 31(e), 32(a),
33(e), 34(a), 35(c)

Glossary

Absolute Losses

Production deferred or lost due to the specified element or system, as a percentage of the total potential production.

$$\text{Absolute Losses} = \frac{\text{Production Defferedor Lost}}{\text{Potential Pr oduction}} \times 100\%$$

Activity-Based Costing (ABC)

A system that tracks costs based on the activities that are responsible for driving costs in the production of manufactured goods.

Analysis

- (1) A step-by-step process of determining the solution to a problem.
- (2) The collection, viewing, and examination of data and information.
- (3) The process of determining the composition of a substance or material using chemical or physical methods.

Availability

Availability is the probability that a system or component is performing its required function at a given point in time, or over a stated period of time when operated and maintained in a prescribed manner. In other words, the proportion of total time that an item of equipment is capable of performing its specified functions. The general observation of availability is:

$$\text{Availability} = \frac{\text{Scheduled Uptime}}{\text{Scheduled Uptime} + \text{Non - Sceduled Downtime}}$$

By taking different measures for uptime and downtime, different availability measures are obtained.

Availability (Inherent)

Inherent availability is defined as $\text{MTBF} / (\text{MTBF} + \text{MTTR})$. Availability increases by increasing reliability (MTBF) and maintainability ($1 / \text{MTTR}$). For example: MTBF = 1000 hours, MTTR = 48 hours. Then the availability is $1000 / 1048 = 95\%$. The inherent availability is solely based on the failure distribution and repair-time distribution, assuming no supply and maintenance delays, and no planned (preventive /

corrective) maintenance. It is considered as an *equipment design parameter*. Inherent availability fulfils the need to distinguish expected performance between planned shutdowns.

Autonomous Maintenance

Operators in independent groups carry out routine maintenance and preventive maintenance. These groups, which may include maintenance workers, solve problems without management intervention. The maintenance department is only called on for bigger problems that require more resources, technology, or downtime.

Backlog

Work that is not completed by the nominated “required by date.” The period each work order is overdue is defined as the difference between the current date and the “required by date.” All work that doesn’t have a specified required by date is generally included on the backlog. Backlog is often measured in crew-weeks, the total number of labor hours represented by the work on the backlog, divided by the number of labour hours available in an average week. As such, backlog is one of the common key performance indicators in maintenance.

Break Down Maintenance (BDM)

“Unplanned” corrective maintenance performed on equipment after the equipment has suffered a failure and has to be corrected during a break down of the equipment. Break down maintenance indicates a lack of planning.

Business Process Re-engineering (BPR)

Business Process Re-engineering or Business Process Reorganisation is itself a process that aims improving organisational performance by improving its business processes. BPR came into use after Michael Hammer and James Champy published their best-selling “Re-engineering the Corporation” in 1993. Re-engineering means ‘starting over’ and the defining words are fundamental, radical, dramatic and process. In short, starting with a clean piece of paper, to design an organisation to perform a process. Re-engineering is not about “continuous improvement”, which by definition is an examination and analysis of the *status quo* where minute improvements are continuously applied to the existing process. A combined approach of continuous improvement and radical change (where needed) is aimed in Business Process Management (BPM).

Condition Based Maintenance (CBM)

An equipment maintenance strategy based on measuring the condition of equipment to assess whether it will fail during some future period, and then taking appropriate action to avoid the consequences of that failure. The condition of equipment is monitored using a variety of objective technologies, through the use of statistical process control techniques, by monitoring equipment performance, or through the use of the human senses. The terms Condition Based Maintenance, On-condition Maintenance, and Predictive Maintenance are often used interchangeably.

Conformity

Fulfilment by a product, process, or service of the specified requirements.

Continuous Improvement

Reduction to maintenance input (hours, materials, management time) to provide a given level of maintenance service. Increases in the number of assets, or use of assets with fixed or decreasing inputs.

Core Damage

When a normally rebuildable component is damaged so badly that it cannot be repaired.

Corrective Maintenance

Any planned or unplanned maintenance activity required to correct a failure that has occurred or is in the process of occurring. This activity may consist of repair, restoration, or replacement of components.

Criticality

The priority rank of a failure mode, based on some assessment criteria such as operational and HSE (Health, Safety, Environment) consequences, and the likelihood of failure occurrence.

Criticality Analysis

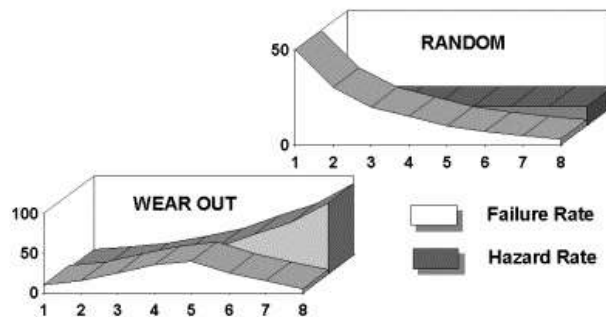
Criticality analysis is a method for identifying product or process criticality for the purpose of prioritising activities like design and maintenance. It is a process of decomposing product or process into hierarchical components, followed by study of their failure modes and effects, and (where appropriate) their causes. Criticality is the combined measure of the failure mode probability and the severity of its effects.

Preventive Maintenance (PM)

Preventive maintenance (PM) tasks that are initiated by a breakdown rather than a schedule. The PM is done on a whole machine, assembly line, or process after a section or subsection breaks down. This is a popular method with manufacturing cells where the individual machines are closely coupled. When one machine breaks, the whole cell undergoes a preventive maintenance activity. Future benefit PM is considered “packaging of opportunistic work” given that an opportunity has arisen to do that work (often due to the failure of an associated piece of equipment).

Hazard Rate

Hazard rate is the instantaneous speed of failure. Hazard rate is the ratio of failures that occur in an interval to the size of the population at the start of the interval, divided by the length of time.



Intervention (scheduled/planned)

Action taken systematically in a period of time independent of machine condition. The time period may be fixed (calendar based) or measured according to machine utilisation (running hours based).

Intrinsic Safety

Intrinsic safety is intended for products in which the level of electrical energy circulating or stored in the product is insufficient to ignite a surrounding explosive atmosphere even under fault conditions.

Kaizen Method

A term originating from Japanese industry relating to a philosophy for continual quality improvement (CQI). Individuals and teams feel empowered to take personal steps toward minimisation of:

- Defective finished products and inventory (zero defects).
- Inefficient work methods, and unnecessary movements and transfers while handling goods.
- Process and operational weaknesses.

Knowledge-Based Systems (KBS)

A wide range of software systems that support decision making for knowledge intensive tasks (i.e. failure diagnosis). The system is based on knowledge that resides in heuristic rules, cases, empirical test results, or partly physical models.

Life Cycle Cost

The total cost of a piece of equipment or system over its entire lifetime; the total of all costs generated or forecasted to be generated during the design, development, production, operation, maintenance, and support processes. Life cycle costs include direct, indirect, recurring, non recurring costs such as acquisition, installation, operating, maintenance, upgrades, and removal or disposal costs.

Maintainability

Maintainability is the probability that a failed component of system will be restored or repaired to a specified condition within a period of time when maintenance is performed according with prescribed procedures. The prescribed maintenance procedures include not only the manner in which repair is to be performed but also the availability of maintenance resources (people, spare parts, tools, and manuals), the preventive maintenance programme, skill levels of personnel, and the number of people assigned to the maintenance crew. Restoration times are commonly characterised by the log normal distribution.

Maintainability Improvement

A maintenance engineering activity that looks at the root cause of breakdowns and maintenance problems and designs a repair that prevents future breakdowns. Maintainability improvement places an emphasis on making equipment easier to maintain.

Maintenance

Combination of all technical, administrative, and managerial actions during the life cycle of an asset intended to retain it in, or restore it to, a state in which it can perform the required function. So, maintenance covers any activity carried out on an asset to repair equipment, or to ensure the asset continues to

perform its intended functions. Maintenance includes all actions taken to prevent or reduce the consequences of failure.

Maintenance Activity

Maintenance activities are the specific actions defined in a Computerised Maintenance Management System (CMMS), taken to prevent or reduce the consequences of failure. For example, component replacement, lubricant analysis, or vibration monitoring are maintenance activities.

Maintenance Categories

Maintenance categories describe the primary function of the maintenance activity. Maintenance categories include: inspection, condition monitoring, non-destructive testing, overhauls, and fault finding.

(Total) Maintenance Cost

All direct and indirect costs regarding maintenance activities. Direct costs are costs charged to a maintenance budget as fixed costs (e.g.: personnel, materials, subcontractors, and overhead). Indirect costs are related to loss of revenue due to unavailability.

Maintenance Management

All activities of the management that determine the maintenance objectives, strategies, and responsibilities, and implement them by means, such as maintenance planning, maintenance control and supervision, improvement of methods in the organisation, including economical, environmental, and safety aspects.

Maintenance Objectives

Targets assigned and accepted for maintenance activities. Targets may include availability, cost reduction, product quality, environmental preservation, safety, etc.

Maintenance Plan

Structured set of tasks that include the activities, procedures, resources, and time scale required to carry out maintenance.

Maintenance Record

Part of maintenance documentation that contains all failures, faults, and maintenance information related to an asset. This record may also include maintenance cost, asset availability or uptime, and any other data where relevant.

Maintenance Schedule

A list of planned maintenance tasks to be performed during a given time period, together with the expected start times and durations of each task. Schedules apply to different time periods (e.g. daily schedule, weekly schedule, etc.), or to specific plant items (e.g.; a machine manufacturer may supply a maintenance schedule with a new machine, related to which is a condition of warranty).

Maintenance Strategy

Management method that covers all aspects of maintenance activities, including firm action plans for achieving maintenance objectives.

Mean Cycles Before Failure (MCBF)

Mean Cycles Between Failures; the average number of equipment cycles between failures; total equipment cycles divided by the total number of failures during those cycles (includes both product and non-product cycles).

Mean Time Between Failures (MTBF)

Mean time between failures is calculated from the total accumulated operating time divided by the number of failures during the same period.

$$\text{MTBF} = \frac{\text{Total Accumulated Operating Time}}{\text{Number of Failures}}$$

Mean Time Between Critical Failure (MTBCF)

A measure of system reliability, which includes the effects of any fault tolerance that exist. The average time between failures that cause a loss of a system function defined as “critical” by the customer.

Mean Time Between Maintenance (MTBM)

A basic measure of reliability for repairable fielded systems. The average time between all system maintenance actions. Maintenance actions are for repair or preventive purposes.

Mean Time to Failure (MTTF)

Mean time to failure is calculated from the total elapsed time divided by the total number of failures.

$$\text{MTTF} = \frac{\text{Total Elapsed Time}}{\text{Number of Failures}}$$

While MTBF excludes time that the equipment is not available or in use, MTTF includes the full period of time regardless of actual operation time. It is common for these two terms to be confused or misunderstood. Failure rates reported or collected from maintenance management systems tend to be in terms of MTTF.

For example, for the rotating components in a machine, when you consider that MTBF is the total actual machine run hours between failures, say the MTBF is 2000 hours, it is not important if this took 1 year or 10 years to accumulate, just that it was 2000 hours. If on the other hand you look at the failure of a non-rotating component like coatings (paint), or metal casting in contact with the coolant or the atmosphere, the total hours the paint has been exposed to the atmosphere or the metal to the coolant is the key. In this instance, the assumption is (assuming $\text{MTTF} > \text{MTBF}$) based on how the failure is defined, first sign or rush, or coolant leaking from a hole in the casting. Notice that then the “interpretation” and hence “point of failure” may differ from user to maintainer etc. If so, the notion of critical, incipient, degraded types of failure can add some detail to that also.

It may be considerable to include the time needed for repair (MTTR) in a MTTF in the case of a coating or casting as illustrated above. The MTTR is not included in MTBF by definition. Imagine a machine is spared, the user may take 1 or 2 months to schedule a repair that could have taken 3 hours. This could significantly skew MTBF.

Mean Time to Repair (MTTR)

MTTR refers to the average total time duration required to physically repair or replace the failed item and to reinstate the operational functionality. Part of the system downtime may be due to time delays (spares, resources), which are not included in the MTTR.

Mean Time to Restore (MTR)

MTR refers to the average (unplanned) system downtime including delays for maintenance and supply resources. This is an appropriate measure when maintenance and supply resources are included as requirement for the maintainability.

Mean Time to Prepare (MTTP)

MTTP is the duration required to prepare for equipment restoration in the event of failure. This time should include all activities and preparations that can be carried out before physical repair activities begin, such as scaffolding, drawing spares from stores, locating tools, spares, and equipment at the job site.

Preparation time should not include lead times required for ordering spares from suppliers. Spare part ordering lead times should be recorded separately to facilitate spares holding policy analysis and the easy identification of long lead times. Although closely related, spares analysis and evaluation is a distinctly different activity to maintenance strategy analysis.

On-time Delivery Rate

The percentage of time that ordered products are received by customers by the specified time or date. Some plants will base this calculation on the date “promised” to customers, but better facilities typically will calculate it against dates “requested” by customers.

Operating Hours

The (accumulated) length of time that an item of equipment is actually operating.

Operational Consequences

A failure has operational consequences if it has a direct adverse impact on operational capability such as lost production, increased production costs, loss of product quality, or reduced customer service.

Operational Efficiency

Used in the calculation of overall equipment effectiveness. The actual output produced from an asset in a given time period divided by the output that would be produced from that asset in that period, had it produced at its maximum rated capacity. Normally expressed as a percentage.

Operator based Maintenance

A philosophy derived from TPM, whereby basic maintenance tasks are performed by operations / production personnel. Typically such activities include cleaning and subjective inspection. Sometimes referred to as Operator Maintenance.

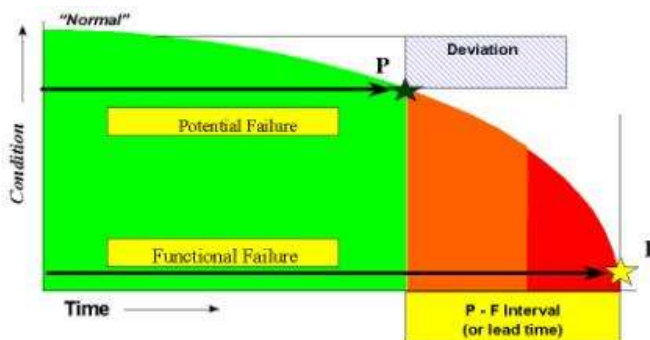
Performance based Contracting

In a performance-based contract, the fee paid to the contractor depends (at least partly) on the business results achieved within the contracted work. This means that apart from the quality, speed, etc., of the work itself, the results of positive and negative work achievements is shared. For example, in the case of

maintenance contracts, the mutual goal may be reduced mechanical equipment downtime (increased uptime). The benefits are long-term relationship and confidence building, reduced amount of contractors, mutual goals, and sharing the risks of unknown events. Overall cost reductions are mentioned from 9% to 30%. A collection of ten success factors is described.

P-F Interval

A term used in reliability-centered maintenance. The time from when a potential failure (P) is first detected on an asset or component using a selected predictive maintenance task, until the asset or component has failed (F). Reliability-centered maintenance principles state that the frequency with which a predictive maintenance task should be performed is determined by the P-F Interval.



Planned Downtime

The amount of time officially scheduled in the production plan, which includes, no orders, changeovers and planned maintenance. Planning and scheduling technologies. A variety of software-based advanced planning, scheduling, and optimisation systems.

Planned Maintenance

Any maintenance activity for which a pre-determined job procedure is documented, for which all labour, materials, tools, and equipment required to carry out the task are estimated, and their availability assured before commencement of the task.

Planned Maintenance is a term commonly used to describe tasks carried out on a regular, scheduled basis. These tasks may be predictive in nature (routine subjective inspections and/or formal condition monitoring activities), or they may be preventative in nature (cleaning / changing filters, checking/adjusting clearances; etc).

Planning

The process of determining the resources, methods, and processes needed to perform maintenance work efficiently and effectively.

Planned Maintenance (PM)

A term variously used as an acronym for Planned Maintenance or Preventative Maintenance. Sometimes used to describe the Work Order (documentation) associated with a routine maintenance task. This term has different meanings depending upon its context.

Potential Failure

A term used in Reliability-centered Maintenance. An identifiable condition that indicates a functional failure is about to occur, or in the process of occurring.

Predictive Maintenance (PdM)

A maintenance process based on machinery inspection, monitoring, and prediction. Machine stops for maintenance are planned depending on the predictions (condition-based). The terms Condition Based Maintenance, On-condition Maintenance and Predictive Maintenance are often used interchangeably.

Preventive Maintenance

A maintenance process based on preventing unexpected events from occurring by employing proper maintenance procedures, clean environment, etc. Maintenance is mostly done during planned machine stops (fixed intervals). Emphasis is placed on replacing, overhauling, or remanufacturing an item at a fixed interval, regardless of its condition at the time. Scheduled restoration tasks and scheduled discard tasks are both examples of Preventive Maintenance tasks.

Preventive Maintenance Schedule Compliance

The number of preventive maintenance work orders completed from the daily/weekly schedule divided by the total number of preventive maintenance work orders on the schedule.

Preventive/Predictive Work

Scheduled, preplanned preventive and predictive (condition-based) inspections and work orders.

Primary Failure

A failure not caused either directly or indirectly by another failure or fault.

Proactive

Action before a stimulus (opposite of reactive). A proactive maintenance department acts before a breakdown.

Proactive Maintenance

The combination of operator-performed maintenance, preventive maintenance, and predictive maintenance activities whereby maintenance is conducted to prevent, eliminate, delay or reduce maintenance before failure.

The application of analytical methods, tools, and techniques to eliminate failures, extend component life, mitigate consequences, minimise downtimes, and optimise all resources. It consists of systematic identification and elimination of potential problems in all aspects of reliability, availability and maintainability.

Process Manufacturing

The manufacturer of products such as chemicals, gasoline, beverages and food products that typically are produced in “batch” quantities rather than discrete units. Many process operations require inputs such as heat, pressure, and time (for thermal or chemical conversion).

Procurement Cycle Time

Total elapsed time from the initiation of a parts requisition until receipt of the part on-site.

Productive Time

A period of time when the equipment is performing its intended function. This includes regular production (including loading and unloading of product), rework, and work for third parties, and engineering runs done in conjunction with production.

Prognostics Preventive Maintenance Clock

The parameter that initiates the Preventive Maintenance (PM) task list for scheduling (usually buildings and assets in regular use). Assets that are used irregularly may use other production measures such as pieces, machine hours, or cycles. The ability to predict or forecast the future condition of a component, or system of components in terms of failures or degraded condition to satisfactorily conform to operational requirements.

Quality Rate

A term used in Total Productive Maintenance (TPM) to indicate the rate of approved product(s) with respect to products that do not comply with the relevant quality standards. Quality rate is expressed as a percentage.

Redundancy

The existence of one or more means (though not necessarily identical) for accomplishing a given function. Active redundancy has all items operating simultaneously, while standby redundancy has alternate means activated upon failure.

Re-engineering

A onetime fundamental rethinking and business process redesign to achieve dramatic improvements in performance and/or maintainability.

Relative Losses

The production deferred or lost due to the specified element or system, as a percentage of the total deferment or losses.

$$\text{Relative Losses} = \frac{\text{Production Differred or Lost}}{\text{Total Deferment or Loss}} \times 100\%$$

Reliability-Centered Maintenance (RCM)

A structured process, originally developed in the airline industry, to determine the equipment maintenance strategies required for any physical asset to ensure that it continues to fulfil its intended functions in its present operating context. The assets are decomposed, extensively analyzed and described, FMEA are made for the most critical components, and the maintenance organisation and processes are carefully (re)defined. RCM is particularly useful and feasible for maintenance of identical installations (like aircraft). A certain level of maintenance maturity is required to ensure accurate and complete asset data.

Risk

Risk is defined as: (1) Possibility of loss or injury; (2) Someone or something that creates or suggests a hazard; (3) The chance of loss to the subject matter of an insurance contract; (4) The degree of probability of such loss. Risk is being associated with a *possibility* of a *loss* due to a hazard exposure. A hazard is

defined as the source of the loss. There is a general baseline that risk includes the two characteristics uncertainty and loss (or gain).

Risk Analysis

The analysis of risk includes two phases, risk assessment and risk management. The risk assessment phase deals with the identification of initiating events towards the construction of the risk curves. The so-called quantitative Probability Risk Assessment (PRA) methodology is often used. PRA can include well-known techniques like preliminary risk analysis, failure modes and effects analysis, criticality analysis, hazards and operability study, event tree analysis, and fault tree analysis. The risk management phase deals with making trade-offs between alternatives influencing the risk scenarios and curves. Each alternative for actively or passively controlling the risk creates a specific risk curve. The curves are evaluated and decisions are made accordingly taking the cost of alternatives as trade-off. A risk-free alternative is often used as a reference point in evaluating alternatives.

Risk-Based Maintenance (RBM)

A maintenance improvement programme whereby the maintenance processes and procedures are planned based on (failure) risks, effects, and calculated cost. This is a financially based analysis technique which focuses on establishing the relative worth of maintenance. It was originally developed as a means of reviewing existing maintenance programmes, and in this mode it works well as a continuous improvement tool. RBM defines opportunities for incremental improvement through the elimination of tasks of low value and the introduction of tasks which address high commercial risk areas. As such, RBM is also valuable in transferring knowledge from existing installations to provide a baseline for new builds.

Route Maintenance

A mechanic's established route through a facility to fix the small problems. The route mechanic is usually very well equipped so he/she can deal with most small problems. Route maintenance and preventive maintenance activity are sometimes combined.

Routine Work

Work done on a routine basis where the work and material content is well known and understood (for example, daily or weekly line start-ups).

Routine Maintenance Task

Any maintenance task performed at a regular, predefined interval.

Run-To-Failure (RTF)

An equipment maintenance strategy, where no routine maintenance tasks are performed on the equipment. The only "planned" maintenance performed on the equipment is corrective maintenance after the equipment has suffered a failure. Run-To-Failure is a conscious decision as opposed to break down maintenance. Also related to "throwaway maintenance" (Run to failure followed by replacement), and "no scheduled maintenance".

Scheduled Downtime

A period of time when the equipment is not available to perform its intended function due to planned downtime events. These include maintenance delay (delay after an interrupt is reported, but before

anyone arrives to repair it); production test; preventive maintenance; change of consumables; setup; and facilities-related downtime.

Scheduled Maintenance

Any maintenance work that is planned and included on an approved maintenance schedule.

Scheduled Work

Work written up after an inspection and known about for a fixed period of time (e.g., 1 day) in advance. A maintenance scheduler or planner inputs the work into the schedule. Sometimes the inspection yields work that must be done immediately which becomes emergency or DIN. Scheduled work is part of a planned maintenance or corrective maintenance program.

Scheduling

The process of determining what maintenance jobs gets worked on, when, and by whom based on the priority and resource/equipment availability. This process should take place before the job is executed.

Secondary Failure

A failure caused either directly or indirectly by another failure or fault.

Short Repairs

Repairs that a preventive maintenance or route person can complete in less than 30 minutes with the tools and materials that he/she carries.

Shutdown

Outage scheduled in advance for maintenance or other services. Sometimes called *planned outage*.

Shutdown Maintenance

Maintenance that is only performed while equipment is shutdown.

Standby Time

A period of time, other than non-scheduled time, when the equipment is in a condition to perform its intended function, facilities are available, but it is not operated. This includes time when no operator is available, time when no product is available (no boards or components), and waiting on upstream or downstream equipment.

String-based Preventive Maintenance

Usually, this refers to simple preventive maintenance tasks that are strung together on several machines. Examples of string PM's include lubrication, filter change, or vibration routes.

Sudden Failure

A failure that could not be anticipated by previous examination or monitoring.

Survey

A formal look around. All of the aspects of the facility are recorded and defined. The survey looks at every machine, room, and throughout the grounds. The surveyor notes anything that looks like it needs work.

Symptom

A qualitative or quantitative measure that shows a particular equipment anomaly, directly or indirectly.

Systematic Preventive Maintenance

Maintenance that is planned and programmed in a fixed period of time independent of equipment condition.

Task

One line on a task list that gives the inspector specific instruction to do one thing.

Task List

In a maintenance inspection context, a task list provides directions about what to look for during an inspection. Tasks include inspecting, cleaning, tightening, adjusting, lubricating, replacing, etc. Tasks are specific, complete, and have a performance standard. Avoid ‘ticks’ as the only feedback that a task is completed.

Throwaway Maintenance

This represents a variation on the Run-to-Failure approach. It differs in that the decision is made in advance that the corrective action on failure will always be replacement rather than repair. This is a very common approach to maintenance of electronic components, which often exhibit random failure rates, and for which no repair is feasible.

Timed Availability

Available for unrestricted operation during a period of time in which operation is required. Sometimes referred to as Total Available Time (be careful total available time is also sometimes referred to as the total number of installed hours, basically being the number of hours in a year).

Total-Productive Maintenance (TPM)

This is a Japanese maintenance improvement programme used to change the maintenance processes and culture to increase productivity. It particularly focuses on aspects such as attitude, motivation, responsibilities, and performance of the workforce. Thus, everyone in the company must understand that their job performance impacts the performance of the asset. It empowers operators to take over maintenance tasks. The results are measured by the OEE rate.

TPM is a companywide management programme that emphasises production operator involvement in equipment maintenance, and continuous improvement approaches.

Total Quality Management (TQM)

A multifaceted, company-wide approach to improving all aspects of quality and customer satisfaction-including fast response and service, as well as product quality. TQM begins with top management and diffuses responsibility to all employees and managers who can have an impact on quality and customer satisfaction. It uses a variety of quality tools such as QFD, Taguchi methods, SPC, corrective-action response teams, cause-and-effect analysis, problem-solving methodologies, and fail-safe-ing (or “poka-yoke” methods).

Total Time

All time during the period being measured (at the rate of 24 hours per day, seven days per week.) Also equal to the sum of time spent in all six equipment time categories.

True Downtime Cost (TDC)

A method of recording and analyzing all significant cost metrics associated with equipment downtime in a building or manufacturing facility. TDC provides a way to assign time and/or monetary value to previously consider “non-tangible” cost of downtime. Also TDC includes downtime factors commonly overlook to arrive at a more true value for the cost of downtime.

Turnaround

A stop, or full or substantial interruption of plant production. Generally turnaround is considered to be a period longer than 24 hours.

Ultrasonic Inspection

A high frequency signal is sent and reflected by the component to be analysed. Ultrasonic inspection is especially meant to detect early, small fatigue cracks or material structure defects / changes. It is also generally applied for leak detection.

Unit

The asset the task list is written for in a preventive maintenance system. The unit is a machine, system, or component of a large machine.

Unplanned Maintenance

Any maintenance activity for which a pre-determined job procedure is not documented, or for which all labour, materials, tools, and equipment required to carry out the task are not estimated, and their availability assured before commencement of the task.

Unscheduled Downtime

A period of time when the equipment is not available to perform its intended function due to unplanned downtime events. These include maintenance delay, repair, change of consumables, out-of-spec input, and facilities-related downtime.

Unscheduled Maintenance

Any maintenance work not included on an approved maintenance schedule prior to its commencement. Note: this is not necessarily a breakdown, rather a break in the schedule of maintenance.

Unrevealed (Covert) Failure

A failure of a component or system that remains undetected until revealed by either proof testing or, more critically, once a demand is placed on the item to function as intended.

Up-time

The time that an item of equipment is in service and can perform its intended function, assuming that the external resources, if required, are provided. Notice that uptime may not be the same as operating time, which is the time that the equipment is performing its intended function.

User Maintenance (UM)

This is any maintenance request primarily driven by a user. It includes breakdown, routine requests, and DIN jobs.

Vibration Analysis

A detailed study of the individual characteristics of a machine's vibrations, with the intention of diagnosing specific machinery faults, usually at an early stage of development. This is typically achieved by studying vibration data in the frequency domain and may also include the study of time domain (time waveform) data. Such analysis may be undertaken routinely as an integral part of a vibration based Predictive Maintenance programme. It may also be undertaken for *ad-hoc* analysis of suspect rotating machinery, irrespective of the machine's inclusion in a formal monitoring programme.

Vibration Monitoring

Regular monitoring of machinery vibrations undertaken as part of a Predictive Maintenance Program. Readings are compared with past levels, with significant change as an indicator of developing machinery faults. The objective is to provide valuable lead-time for maintenance planning. A comprehensive monitoring programme usually includes vibration analysis.

Visual Inspection

Visual inspection refers to subjective inspection of machinery, and employs only the human senses. Sometimes it is referred to as "look-listen-feel" checks.

Warning Time

Warning time is considered equivalent to the P-F interval.

Wireless

In maintenance context, wireless units are defined wireless when they require neither power nor other data wiring. For example, wireless condition monitoring is applied where sensor and communication / analysis module cannot be located at the same place.

Index

A

Acclimatization, 128
Air-conditioning system, 137
Aisle airflow speed, 128
Antenna, 25
Apertures, 38
Autonomous management, 5
Availability, 9

B

Bonding, 31
Bonding jumpers, 31
Branch circuits, 31

C

Capacitors, 23
Chipset, 66
Circuit breaker, 31
Circuit tracing techniques, 18
Clock generator, 66
Condition based maintenance, 2
Condition monitoring, 17
Conduit and trunk, 134
Constant voltage transformer, 103
Constant-voltage transformer, 103
Contaminants, 128

Contracted maintenance, 5
Contrast, 36
Convergent paths, 55
Corrective maintenance, 5, 17

D

Daisy-wheel, 85
Dead cpu, 68
Deferred maintenance, 2
Dot-matrix, 85

E

Echelon, 5
Eddy currents, 37
Emergency lighting, 134
Emi filters, 36
Equipment, 31
Equipment layout planning, 134

F

Failure, 7
False ceiling, 134
Faraday's cage, 37
Fault correction, 3
Fault diagnosis, 3
Fault tree, 13

Ferro resonant transformer, 103
 Floppy disk, 71
 Floppy disk drive, 71
 Fmea (failure mode and effects analysis), 13
 Fmea / fmeca, 13
 Function check-out, 3

G

Grounding, 29
 Grounding conductor, 32
 Grounding electrode, 32

H

Halt: highly accelerated life testing (halt), 13
 Hrd5 hrd, 5 12
 Immediate maintenance, 2

I

Indenture level, 4
 Ink-jet, 85
 Inspection, 3
 Internal partitions, 132

L

Laser, 85
 Lcd & led, 85
 Led (light emitting diode), 8
 Line printer, 85
 Line-interactive ups, 117
 Loop, 25

M

Main board, 66
 Maintenance level, 4
 Maintenance prevention, 5
 Markov model, 13
 Matching, 26
 Mean time between failure, 9
 Mean time between failure (mtbf), 7

Mean time to repair (or recover), 10
 Meantime between failure, 7
 Meantime to repair (mttr) maintenance policy, 7
 Modems, 86
 Monitoring, 3
 Monitors, 89
 Mosfet, 95
 Motherboard, 66
 Mtbef, 7
 Mttr, 10

N

Node-voltage method, 56
 Non-volatile memory chips, 66
 Normal lighting, 134
 Normal mode noise, 40
 Norton, 57
 Offline, 117
 Online ups, 118
 On-site maintenance, 6
 Overhaul, 3
 Parts count prediction, 11
 Pcb, 18
 Plenum, 32
 Power conditioning, 122
 Power connector flickers, 66
 Power supply, 29
 Power supply unit, 91
 Predetermined maintenance, 2
 Predictive maintenance, 17
 Predictive maintenance, 2
 Preventive maintenance, 2
 Printed circuit board (pcb), 66
 Prototype!, 19

R

Raceway, 32
 Raid, 8
 Raised floor, 133

Ramp, 133
Rbd (reliability block diagram), 12
Rebuilding, 3
Reflections, 26
Reliability, 8, 9
Remote maintenance, 6
Resistance grounding, 35
Resistors, 23
Routine maintenance, 3

S

Safe programming, 65
Scheduled maintenance, 2
Separately derived system, 32
Server room, 122
Shielding, 29
Shielding effects, 36
Shielding theory, 35
Shock, 128
Slots, 66
Slots for expansion cards, 66

Sockets, 66
Standby, 117
Surface mount, 29
System, 90
System fault-tree analysis, 61
System-fault-tree, 62

T

Telcordia, 12
Thermal printer, 85
Thevenin, 57
Thevenin equivalent circuit, 57
Trace antennas, 24
Trace reflections, 26

U

Ungrounded system, 34
Uninterrupted power supply, 115
Ups, 117

V

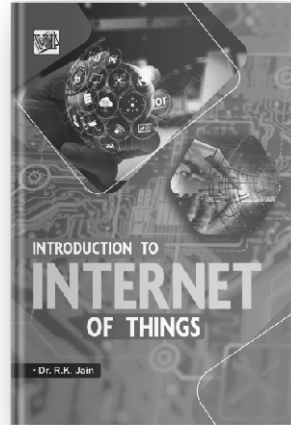
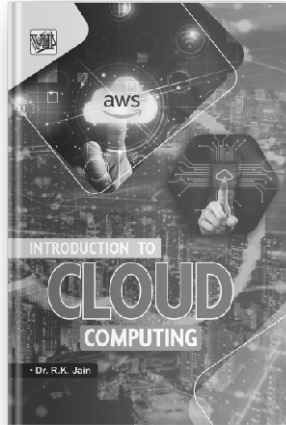
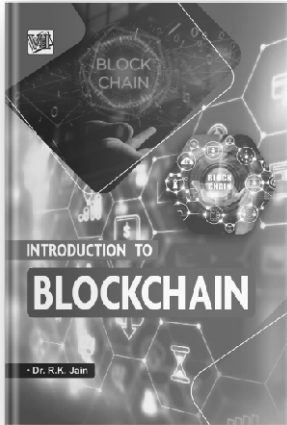
Vibration, 128
Video card, 90
Voltage stabilizer, 103

W

Wall finishing, 132
Walls/partitions, 132

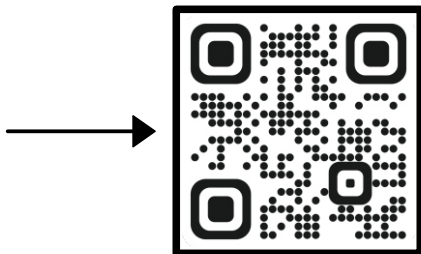
SPECIAL BONUS!

Want These 3 Bonus Books for free?



**Get FREE, unlimited access to these
and all of our new books by joining
our community!**

SCAN w/ your camera TO JOIN!



**OR Visit
freebie.kartbucket.com**