

# **CHAPTER 1**

## **INTRODUCTION**

## **INTRODUCTION**

**1.1 AIM:** The aim of the project is to develop a PC based simulator jig for testing a sub-system called synthetic channel of an Electronic Warfare system.

### **1.2 TOOLS REQUIRED**

#### **SOFTWARE:**

- C language used in PC
- Embedded/Assemble C used in Micro-controller
- VHDL used in PROM for FPGA

#### **HARDWARE:**

- RS 232
- MAX 235
- BUFFER
- MICROCONTROLLER
- FPGA (4013 SERIES)
- PROM (AT171v256)
- HEX DISPLAY (4N54)
- CRISTAL OSCILLATOR (10MHz)

### **1.3 NEED FOR THE PROJECT**

Simulator for a synthetic module can also be referred as a TEST JIG for the LRU (Line Replacement Unit) of an Electronic Warfare System. Test Jig is nothing but the testing device used to test a particular module.

In this report we deal with the assembling of this test jig for the Electronic Warfare System. We have named this jig as a SIMULATOR for easy understanding. Simulator is an electronic device used for testing a system to obtain the desired output by giving its required input. And simulation is the name of the process performed by the simulator.

The required RF modulation data is to be selected from the PC. PC communicates to the micro-controller through the RS232 interface. PC gives the required data to the micro-controller of the simulator PCB through the level converter (RS-232 standard). Microcontroller generates the address, data and controls on the address, data and I/O bus of micro controller based on the selection from PC. FPGA latches the required address, data and controls and give different lines of address (10 bits), data (16 bits) and controls (8 bits) to the synthetic module through inter-connecting cable.

As an electronic counter measure we will design a module which will generate noise signals as a part of jamming techniques and will send to the opponent's radar so that they can't detect our ship or aircraft. This module consists of many sub modules (12 to be precise) and if all the sub modules work together then only the module will generate noise signals for jamming. One of those modules is the synthetic module.

In this project we develop a simulator which is used to check whether the synthetic module is working or not. We will give the random frequencies as the inputs and a certain jamming technique and see whether it's working or not. The main purpose of the synthetic module is to generate RF frequency.

In This project we will be using certain terms which are related to the synthetic module like THREAT and CHANNEL. Threat means how many radars the module can handle at a time i.e. how many radars it can confuse by sending the noise signal effectively at a time. Channel means the synthetic module contains 3 channels. We will mainly use channels one and two for 8-18 GHz frequency and channel 3 for 18-40 GHz frequency. We will use only 1-4 threats to channel- 1 and 6-9 threats to channel 2 and 5,10 threats are used for channel 3. There will be 10 numbers of threats.

## **CHAPTER 2**

### **LITERATURE SURVEY**

## **LITERATURE SURVEY**

### **2.1 RADAR**

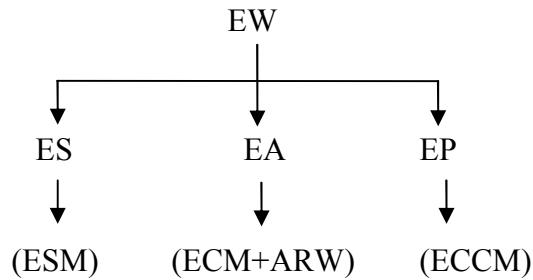
Radar is an object detection system that uses electromagnetic waves to identify the range, altitude, direction, or speed of both moving and fixed objects such as aircraft, ships, motor vehicles, weather formations, and terrain. The term *RADAR* was coined in 1940 by the U.S. Navy as an acronym for ***R**adio **D**etection **A**nd **R**anging*. The term has since entered the English language as a standard word, *radar*, losing the capitalization. Radar was originally called RDF (Range and Direction Finding) in the United Kingdom, using the same acronym as Radio Direction Finding to preserve the secrecy of its ranging capability.

A radar system has a transmitter that emits radio waves. When they come into contact with an object they are scattered in all directions. The signal is thus partly reflected back and it has a slight change of wavelength (and thus frequency) if the target is moving. The receiver is usually, but not always, in the same location as the transmitter. Although the signal returned is usually very weak, the signal can be amplified through use of electronic techniques in the receiver and in the antenna configuration. This enables radar to detect objects at ranges where other emissions, such as sound or visible light, would be too weak to detect. Radar uses include meteorological detection of precipitation, measuring ocean surface waves, air traffic control, police detection of speeding traffic, military applications, or to simply determine the speed of a baseball.

### **2.2 ELECTRONIC WARFARE SYSTEMS**

Electronic warfare is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

Electronic Warfare doctrine is a key element in the army's ongoing effort to rebuild and modernizes its warfare capability. Electronic warfare consists of three divisions:



### 2.2.1 ELECTRONIC WARFARE SUPPORT

In military telecommunications, the terms **Electronic Support** (ES) or **Electronic Support Measures** (ESM) describe the division of electronic warfare involving actions taken under direct control of an operational commander to detect, intercept, identify, locate, record, and/or analyze sources of intentional and unintentional radiated electromagnetic energy for the purposes of immediate threat recognition (such as warning that fire control RADAR has locked on a combat vehicle, ship, or aircraft), targeting or longer-term operational planning. Thus, Electronic Support provides a source of information required for decisions involving Electronic Attack (EA), Electronic Protection (EP), avoidance targeting, and other tactical employment of forces. Electronic Support data can be used to produce signals intelligence (SIGINT), communications intelligence (COMINT) and electronics intelligence (ELINT).

Electronic warfare support systems collect data and produce information or intelligence to—

- Corroborate other sources of information or intelligence.
- Conduct or direct electronic attack operations.
- Initiate self-protection measures.
- Task weapon systems.
- Support electronic protection efforts.
- Create or update EW databases.
- Support information tasks.

ESM gather intelligence through passive "listening" to electromagnetic radiations of military interest. Electronic support measures can provide (1) initial detection or knowledge of foreign systems, (2) a library of technical and operational data on foreign systems, and (3)

tactical combat information utilizing that library. ESM collection platforms can remain electronically silent and detect and analyze RADAR transmissions beyond the RADAR detection range because of the greater power of the transmitted electromagnetic pulse with respect to a reflected echo of that pulse.

Desirable characteristics for electromagnetic surveillance and collection equipment include (1) wide-spectrum or bandwidth capability because foreign frequencies are initially unknown, (2) wide dynamic range because signal strength is initially unknown, (3) narrow band pass to discriminate the signal of interest from other electromagnetic radiation on nearby frequencies, and (4) good angle-of arrival measurement for bearings to locate the transmitter. The frequency spectrum of interest ranges from 30 MHz to 50 GHz. Multiple receivers are typically required for surveillance of the entire spectrum, but tactical receivers may be functional within a specific signal strength threshold of a smaller frequency range.

### **2.2.2 ELECTRONIC ATTACK**

Electronic attack is a division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Electronic attack includes—

- Actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception.
- Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).
- Offensive and defensive activities including countermeasures.

Directed energy is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. A directed-energy weapon uses directed energy primarily as a direct means to damage or destroy an enemy's equipment, facilities, and personnel. In addition to destructive effects, directed-energy weapon systems support area denial and crowd control.

Countermeasures are that form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. They can be deployed preemptively or reactively. Devices and techniques used for EW countermeasures include electro-optical-infrared countermeasures and radio frequency countermeasures.

Electro-optical-infrared countermeasures consist of any device or technique employing electro optical-infrared materials or technology that is intended to impair or counter the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Electro-optical-infrared is the part of the electromagnetic spectrum between the high end of the far infrared and the low end of ultraviolet. Electro-optical-infrared countermeasures may use laser and broadband jammers, smokes/aerosols, signature suppressants, decoys, pyrotechnics/pyrophorics, high-energy lasers, or directed infrared energy countermeasures.

Radio frequency countermeasures consist of any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of or counter enemy activity, particularly with respect to precision guided weapons and sensor systems.

Common types of electronic attack include spot, barrage, and sweep electromagnetic jamming. It also include various electromagnetic deception techniques such as false target or duplicate target generation.

Examples of offensive electronic attack include—

- Jamming enemy radar or electronic command and control systems.
- Using anti-radiation missiles to suppress enemy air defenses (anti-radiation weapons use radiated energy emitted from the target as their mechanism for guidance onto targeted emitters).
- Using electronic deception techniques to confuse enemy intelligence, surveillance, and reconnaissance systems.
- Using directed-energy weapons to disable an enemy's equipment or capability.



Defensive electronic attack uses the electromagnetic spectrum to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and other protection measures such as use of expendables (flares and active decoys), jammers, towed decoys, directed-energy infrared countermeasure systems, and counter-radio-controlled improvised-explosive-device systems.

### **2.2.3 ELECTRONIC PROTECTION**

Electronic protection is a division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. For example, electronic protection includes actions taken to ensure friendly use of the electromagnetic spectrum, such as frequency agility in a radio, or variable pulse repetition frequency in radar. Electronic protection should not be confused with self-protection. Both defensive electronic attack and electronic protection protect personnel, facilities, capabilities, and equipment. However, electronic protection protects from the effects of electronic attack (friendly and enemy), while defensive electronic attack primarily protects against lethal attacks by denying enemy use of the electromagnetic spectrum to guide or trigger weapons.

During operations, electronic protection includes, but is not limited to, the application of training and procedures for countering enemy electronic attack. Army commanders and forces understand the threat and vulnerability of friendly electronic equipment to enemy electronic attack and take appropriate actions to safeguard friendly combat capability from exploitation and attack. Electronic protection measures minimize the enemy's ability to conduct electronic warfare support and electronic attack operations successfully against friendly forces. To protect friendly combat capabilities, units.

- Regularly brief force personnel on the EW threat.
- Ensure that electronic system capabilities are safeguarded during exercises, workups, and pre-deployment training.
- Coordinate and de-conflict electromagnetic spectrum usage.
- Provide training during routine home station planning and training activities on appropriate electronic protection active and passive measures.

- Take appropriate actions to minimize the vulnerability of friendly receivers to enemy jamming (such as reduced power, brevity of transmissions, and directional antennas).

Electronic protection also includes spectrum management. The spectrum manager plays a key role in the coordination and de-confliction of spectrum resources allocated to the force. Spectrum managers or their direct representatives participate in the planning for EW operations.

The development and acquisition of communications and electronic systems includes electronic protection requirements to clarify performance parameters. Army forces design their equipment to limit inherent vulnerabilities. If electronic attack vulnerabilities are detected, then units must review these programs.

## **2.3 JAMMING**

Electronic jamming refers to radio frequency signals originating from sources outside the radar(our radar), transmitting in the enemy radar's frequency and thereby masking targets of interest. Jamming may be intentional, as with an electronic warfare (EW) tactic, or unintentional, as with friendly forces operating equipment that transmits using the same frequency range. Jamming is considered an active interference source, since it is initiated by elements outside the radar and in general unrelated to the radar signals.

Jamming is problematic to radar since the jamming signal only needs to travel one-way (from the jammer to the radar receiver) whereas the radar echoes travel two-ways (radar-target-radar) and are therefore significantly reduced in power by the time they return to the radar receiver. Jammers therefore can be much less powerful than their jammed radars and still effectively mask targets along the line of sight from the jammer to the radar. Jammers have an added effect of affecting radars along other lines of sight, due to the radar receiver's side lobes. The two main technique styles are noise jamming and deception jamming.

### **2.3.1 Noise Jamming:**

The three types of noise jamming are spot, sweep, and barrage.

- **Spot jamming** occurs when a jammer focuses all of its power on a single frequency. While this would severely degrade the ability to track on the jammed frequency, frequency agile radar would hardly be affected because the jammer can only jam one frequency. While multiple jammers could possibly jam a range of frequencies, this would consume a great deal of resources to have any effect on a frequency-agile radar, and would probably still be ineffective. The bandwidth of interest is 10, 20, 40, 60. There by it uses very less bandwidth, so AFC is required.
- **Barrage jamming** is the jamming of multiple frequencies at once by a single jammer. The advantage is that multiple frequencies can be jammed simultaneously; however, the jamming effect can be limited because this requires the jammer to spread its full power between these frequencies. So the more frequencies being jammed, the less effectively each is jammed. The bandwidth of interest is 100, 200, 300, 400.
- **Sweep jamming** is when a jammer's full power is shifted from one frequency to another. While this has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. Although, depending on the error checking in the device(s) this can render a wide range of devices effectively useless. The bandwidth of interest is 500, 1000, 1500, 200. And it is wide range of bandwidth, so AFC operation not required.

In radio equipment, **Automatic Frequency Control** (AFC) is a method (or device) to automatically keep a resonant circuit tuned to the frequency of an incoming radio signal. It is primarily used in radio receivers to keep the receiver tuned to the frequency of the desired station. In radio communication AFC is needed because, after the band pass frequency of a receiver is tuned to the frequency of a transmitter, the two frequencies may drift apart, interrupting the reception. This can be caused by a poorly controlled transmitter frequency, but the most common cause is drift of the center band pass frequency of the receiver, due to thermal or mechanical drift in the values of the electronic components. Assuming that a receiver is nearly tuned to the desired frequency. The AFC circuit in the receiver develop an error voltage proportional to the degree to which the receiver is mistuned. This error voltage is the fed back to the tuning circuit in such a way that the tuning error is reduced.

### 2.3.2 Deception Jamming:

Deception jamming is nothing but false targeting. False targeting is divided into Range, Velocity, Angle.

- **Range :** RGPO, RGPI
- **Velocity:** VGPO, VGPI
- **Angle :** SRM, SSRM, Blink

### 2.4 SYNTHETIC MODULE

Synthetic module is basically a Frequency Generator. It generates the frequencies in the range of 8-18 GHz. The functionality of the Synthetic module is to generate the modulated RF in the above said range. Depending upon the frequencies, its related data, address and controls are generated from its preceding modules. These are given to the synthetic module for RF generation. Synthetic module is a unit of the Electronic warfare system, typically it is the module connected to the radar of the NAVY VESSEL.

It consists of an interface card and an RF generator. Interface card acts as an interface between the synthetic module and the preceding modules. RF generator consists of DTO's, PCB's and other RF components. The frequency generated by the DTO's is sent through the VCO's for FM modulation.

When an enemy ship is approaching our ship, their radar can detect the actual position of our ship and destroy us, we don't want this to happen. Thus to fail this even, one has to confuse the enemy radar with certain measures. In such scenario synthetic module helps in confusing the enemy radar. In the Radar System there are two measures known as ESM and ECM, the former is used to receive and analyze the signals coming from the enemy radar and the other is used to confuse the enemy radar, and thus named as counter measure. Counter measures can be taken in two ways, one is by deceiving the enemy radar by changing the PRI (Pulse Repetition Interval) and the other is by sending noise in its echo signal. By changing PRI, the actual location of our ship is not revealed and thus we are in safe mode. And if the noise is sent through the echo signal, it is not possible to track our vessel.

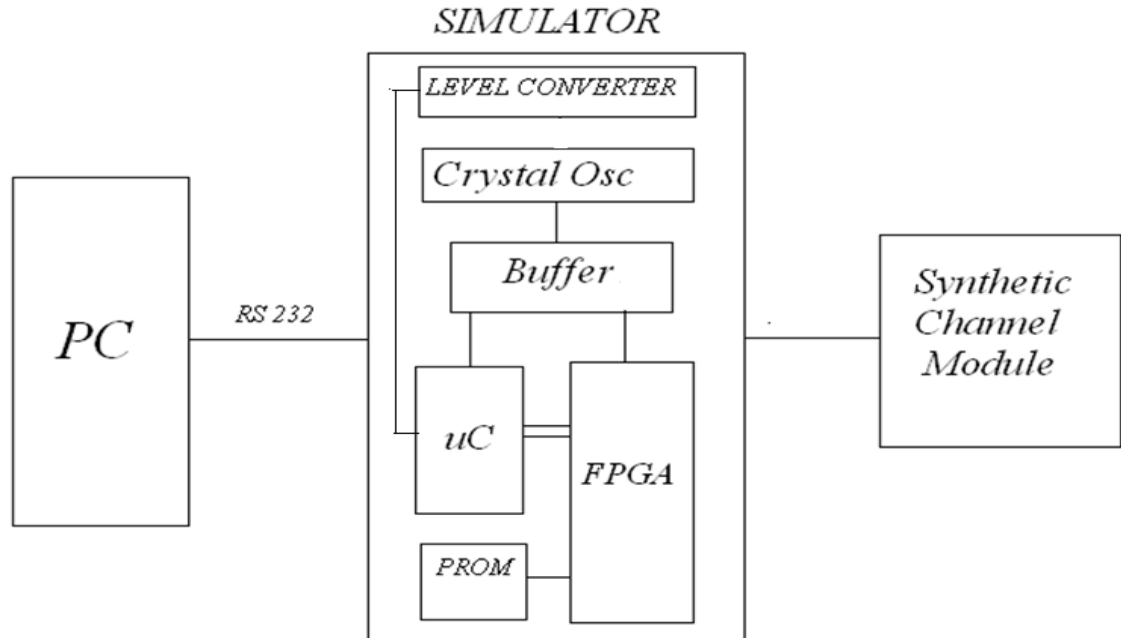
All these measures are taken up by ECM and fed to the synthetic module for RF generation, in this synthetic module, required RF is generated, with included noise or with changed PRI.

## **CHAPTER 3**

### **THEORETICAL ANALYSIS**

## THEORETICAL ANALYSIS

### 3.1 BLOCK DIAGRAM



**Fig 3.1 Block diagram of simulator for synthetic module**

In this block diagram PC communicates to the micro-controller through the RS232 interface. PC gives the required data to the micro-controller of the simulator PCB through the level converter (RS-232 standard). Microcontroller along with FPGA uses crystal oscillator for generating clock frequency. Buffer is used to increase fan-out capacity of crystal oscillator. Microcontroller generates the address, data and controls on the address, data and I/O bus of micro controller based on the selection from PC. PROM is used to store FPGA code as its volatile FPGA latches the required address, data and controls and gives different lines of address (10 bits), data (16 bits) and controls (8 bits) to the synthetic module through inter-connecting cable.

## **3.2 SERIAL COMMUNICATION USING RS232**

### **3.2.1 INTRODUCTION**

Serial communication is a way enables different equipments to communicate with their outside world. It is called serial because the data bits will be sent in a serial way over a single line. A personal computer has a serial port known as communication port or COM Port used to connect a modem for example or any other device, there could be more then one COM Port in a PC.

Serial ports are controlled by a special chip called UART (Universal Asynchronous Receiver Transmitter). Different applications use different pins on the serial port and this basically depend of the functions required. If you need to connect your PC for example to some other device by serial port, then you have to read instruction manual for that device to know how the pins on both sides must be connected and the setting required.

### **3.2.2 COMMUNICATION METHODS**

There are two methods for serial communication, Synchronous & Asynchronous.

#### **(A) Synchronous serial communication:**

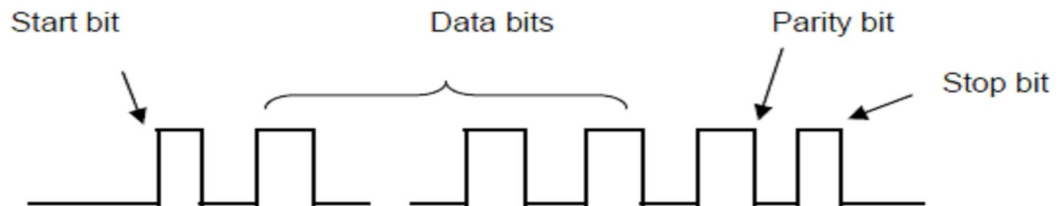
In Synchronous serial communication the receiver must know when to “read” the next bit coming from the sender, this can be achieved by sharing a clock between sender and receiver.

In most forms of serial Synchronous communication, if there is no data available at a given time to transmit, a fill character will be sent instead so that data is always being transmitted. Synchronous communication is usually more efficient because only data bits are transmitted between sender and receiver, however it will be more costly because extra wiring and control circuits are required to share a clock signal between the sender and receiver.

#### **(B) Asynchronous serial communication:**

Asynchronous transmission allows data to be transmitted without the sender having to send a clock signal to the receiver. Instead, special bits will be added to each word in order to synchronize the sending and receiving of the data.

When a word is given to the UART for Asynchronous transmissions, a bit called the "Start Bit" is added to the beginning of each word that is to be transmitted. The Start Bit is used to alert the receiver that a word of data is about to be sent, and to force the clock in the receiver into synchronization with the clock in the transmitter.



After the Start Bit, the individual bits of the word of data are sent, each bit in the word is transmitted for exactly the same amount of time as all of the other bits.

When the entire data word has been sent, the transmitter may add a Parity Bit that the transmitter generates. The Parity Bit may be used by the receiver to perform simple error checking. Then at least one Stop Bit is sent by the transmitter.

If the Stop Bit does not appear when it is supposed to, the UART considers the entire word to be garbled and will report a Framing Error. The standard serial communications hardware in the PC does not support Synchronous operations.

D-type 9-pin no.	Abbreviation	Full Name	Function
Pin-1	CD	Carrier Detect	When the modem detects a carrier from the modem at other end of the phone line, this line become active.
Pin-2	RD	Receive Data	Serial Data Input(RXD).
Pin-3	TD	Transmit Data	Serial Data output(TXD)..
Pin-4	DTR	Data terminal Ready	This is the opposite to DSR. This tells the modem that the UART is ready to link.
Pin-5	SG	Signal ground	Ground the signal.
Pin-6	DSR	Data set ready	This tells the UART that the modem is ready to establish a link.
Pin-7	RTS	Request to send	This line informs modem that UART is ready to exchange data.
Pin-8	CTS	Clear to send	This line indicates that the modem is ready to exchange data.
Pin-9	RI	Ring Indicator	Goes active when modem detects a ringing signal from PSTN.

**Table 3.2 Connector pin description and functions**



### 3.2.3 SERIAL PINOUT(D9 CONNECTOR)

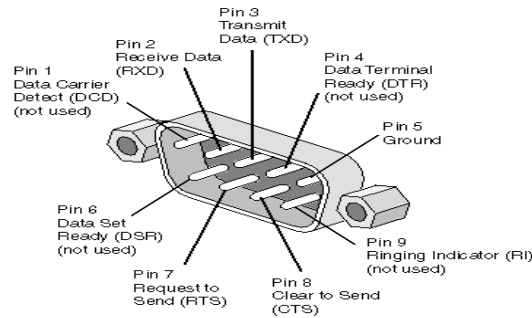


Fig 3.2 Connector serial pinout

### 3.3 LEVEL CONVERTOR (MAX 235)

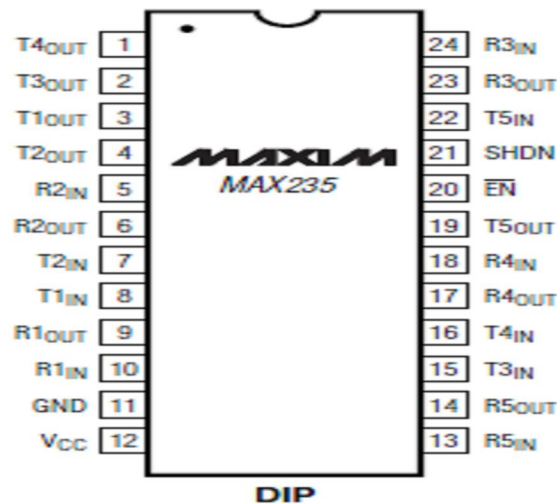


Fig 3.3 Max235 pin diagram

#### 3.3.1 GENERAL DESCRIPTION

The MAX220–MAX249 family of line drivers/receivers is intended for all EIA/TIA-232E and V.28/V.24 communications interfaces, particularly applications where  $\pm 12\text{V}$  is not available. These parts are especially useful in battery-powered systems, since their low-power shutdown mode reduces power dissipation to less than  $5\mu\text{W}$ . The MAX225, MAX233, MAX235, and MAX245/MAX246/MAX247 use no external components and are recommended for applications where printed circuit board space is critical.

### **3.3.2 APPLICATIONS**

- Portable Computers
- Low-Power Modems
- Interface Translation
- Battery-Powered RS-232 Systems
- Multidrop RS-232 Networks

### **3.3.3 DUAL CHARGE-PUMP VOLTAGE CONVERTER**

The MAX220–MAX249 has two internal charge-pumps that convert +5V to  $\pm 10\text{V}$  (unloaded) for RS-232 driver operation. The first converter uses capacitor C1 to double the +5V input to +10V on C3 at the V+ output. The second converter uses capacitor C2 to invert +10V to -10V on C4 at the V- output. A small amount of power may be drawn from the +10V (V+) and -10V (V-) outputs to power external circuitry except on the MAX225 and MAX245–MAX247, where these pins are not available. V+ and V- are not regulated, so the output voltage drops with increasing load current. Do not load V+ and V- to a point that violates the minimum  $\pm 5\text{V}$  EIA/TIA-232E driver output voltage when sourcing current from V+ and V- to external circuitry. When using the shutdown feature in the MAX222, MAX225, MAX230, MAX235, MAX236, MAX240, MAX241, and MAX245–MAX249, avoid using V+ and V<sub>to</sub> power external circuitry. When these parts are shut down, V- falls to 0V, and V+ falls to +5V. For applications where a +10V external supply is applied to the V+ pin (instead of using the internal charge pump to generate +10V), the C1 capacitor must not be installed and the SHDN pin must be tied to VCC. This is because V+ is internally connected to VCC in shutdown mode.

## **3.4 BUFFER (54F541)**

### **3.4.1 GENERAL DESCRIPTION**

The 'F540 and 'F541 are similar in function to the 'F240 and 'F244 respectively, except that the inputs and outputs are on opposite sides of the package. This pin out arrangement makes these devices especially useful as output ports for microprocessors, allowing ease of layout and greater PC board density.

### 3.4.2 FEATURES

- TRI-STATE outputs drive bus lines.
- Inputs and outputs opposite side of package, allowing easier interface to microprocessors.

### 3.4.3 PIN DIAGRAM

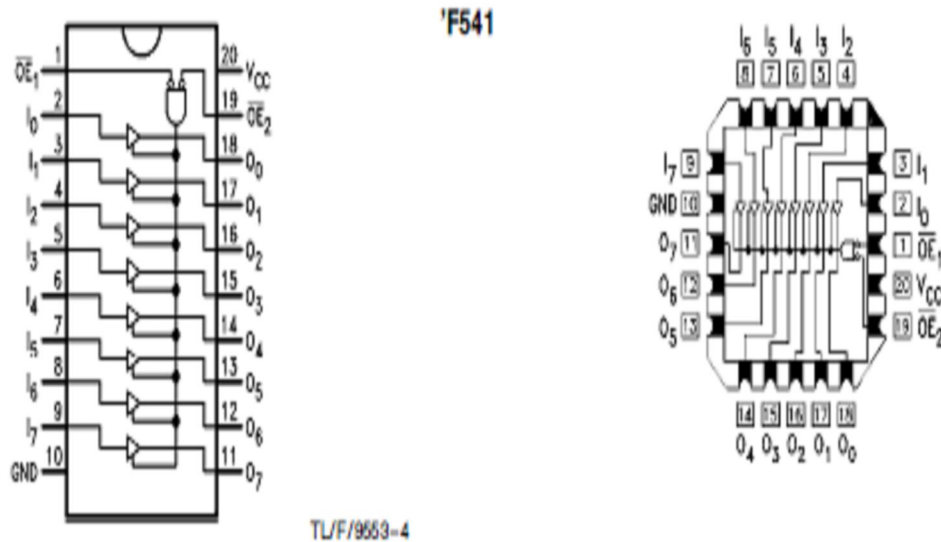


Fig 3.4 pin diagram of 54F541

## 3.5 MICROCONTROLLER (M87C51FB)

### 3.5.1 DESCRIPTION

The Intel M87C51FB is a single-chip control-oriented microcontroller which is fabricated on Intel's reliable CHMOS III-E technology. Being a member of the MCS 51 family of microcontrollers, the M87C51FB uses the same powerful instruction set, has the same architecture, and is pin-for-pin compatible with the existing MCS 51 microcontroller family of products. The M87C51FB is an enhanced version of the M87C51. Its added features make it an even more powerful microcontroller for applications that require Pulse Width Modulation, High Speed I/O, and up/down counting capabilities such as motor control. It also has a more versatile serial channel that facilitates multi-processor communications.

Port 0 pins that have 1's written to them float, and in that state can be used as high-impedance inputs. Port 0 is also the multiplexed low-order address and data bus during accesses to external Program and Data Memory. In this application it uses strong internal pull-ups when emitting 1's and can source and sink several LS TTL inputs. Port 0 also receives the code bytes during EPROM programming, and outputs the code bytes during program verification. External pull-ups resistors are required during program verification.

Port 1 is an 8-bit bidirectional I/O port with internal pull-ups. The Port 1 output buffers can drive LS TTL inputs. Port 1 pins that have 1's written to them are pulled high by the internal pull-ups, and in that state can be used as inputs. As inputs, Port 1 pins that are externally being pulled low will source current (IIL, on the data sheet) because of the internal pull-ups.

Port 2 is an 8-bit bidirectional I/O port with internal pull-ups. The Port 2 output buffers can drive LS TTL inputs. Port 2 pins that have 1's written to them are pulled high by the internal pull-ups, and in that state can be used as inputs. As inputs, Port 2 pins that are externally being pulled low will source current (IIL, on the data sheet) because of the internal pull-ups. Port 2 emits the high-order address byte during fetches from external Program Memory and during accesses to external Data Memory that use 16-bit addresses (MOVX @DPTR). In this application it uses strong internal pull-ups when emitting 1's. During accesses to external Data Memory that use 8-bit addresses (MOVX @R<sub>i</sub>), Port 2 emits the contents of the P2 Special Function Register.

Port 3 is an 8-bit bidirectional I/O port with internal pull-ups. The Port 3 output buffers can drive LS TTL inputs. Port 3 pins that have 1's written to them are pulled high by the internal pull-ups, and in that state can be used as inputs. As inputs, Port 3 pins that are externally being pulled low will source current (IIL, on the data sheet) because of the pull-ups.

### 3.5.2 FEATURES

- Three 16-Bit Timer/Counters
- Programmable Counter Array
- High Speed Output
- Watchdog Timer capabilities
- Up/Down Timer/Counter
- 16K On-Chip EPROM
- 256 Bytes of On-Chip Data RAM
- 32 Programmable I/O Lines

### 3.5.3 PIN DIAGRAM

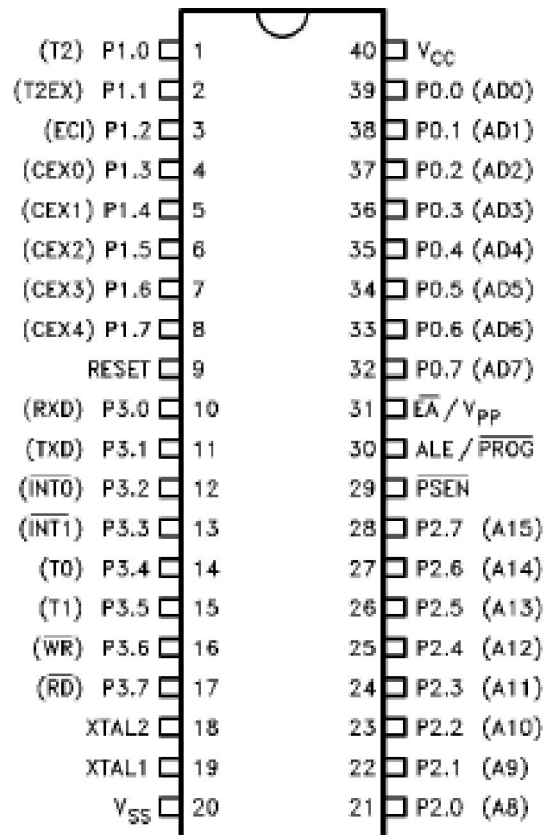


Fig 3.4 pin diagram of microcontroller

### 3.5.4 BLOCK DIAGRAM

## **3.6 FPGA (XC4013E)**

### **3.6.1 INTRODUCTION**

XC4000 Series high-performance, high-capacity Field Programmable Gate Arrays (FPGAs) provide the benefits of custom CMOS VLSI, while avoiding the initial cost, long development cycle, and inherent risk of a conventional masked gate array. The result of thirteen years of FPGA design experience and feedback from thousands of customers, these FPGAs combine architectural versatility, on-chip Select-RAM memory with edge-triggered and dual-port modes, increased speed, abundant routing resources, and new, sophisticated software to achieve fully automated implementation of complex, high-density, high-performance designs.

### **3.6.2 DESCRIPTION**

XC4000 Series devices are implemented with a regular, flexible, programmable architecture of Configurable Logic Blocks (CLBs), interconnected by a powerful hierarchy of versatile routing resources, and surrounded by a perimeter of programmable Input/output Blocks (IOBs). They have generous routing resources to accommodate the most complex interconnect patterns. The devices are customized by loading configuration data into internal memory cells. The FPGA can either actively read its configuration data from an external serial or byte-parallel PROM (master modes), or the configuration data can be written into the FPGA from an external device (slave and peripheral modes).

XC4000 Series FPGAs are supported by powerful and sophisticated software, covering every aspect of design from schematic or behavioral entry, floor planning, simulation, automatic block placement and routing of interconnects, to the creation, downloading, and read back of the configuration bit stream. Because Xilinx FPGAs can be reprogrammed an unlimited number of times, they can be used in innovative designs where hardware is changed dynamically, or where hardware must be adapted to different user applications. FPGAs are ideal for shortening design and development cycles, and also offer a cost-effective solution for production rates well beyond 5,000 systems per month. For lowest high-volume unit cost, a design can first be implemented in the XC4000E or XC4000X, then migrated to one of Xilinx compatible Hardwire mask-programmed devices.

### **3.6.3 FUNCTIONAL DESCRIPTION**

XC4000 Series devices achieve high speed through advanced semiconductor technology and improved architecture. The XC4000E and XC4000X support system clock rates of up to 80 MHz and internal performance in excess of 150 MHz. Compared to older Xilinx FPGA families, XC4000 Series devices are more powerful. They offer on-chip edge-triggered and dual-port RAM, clock enables on I/O flip-flops, and wide-input decoders. They are more versatile in many applications, especially those involving RAM. Design cycles are faster due to a combination of increased routing resources and more sophisticated software.

### **3.6.4 BASIC BUILDING BLOCKS**

Xilinx user-programmable gate arrays include two major configurable elements: configurable logic blocks (CLBs) and input/output blocks (IOBs).

- CLBs provide the functional elements for constructing the user's logic.
- IOBs provide the interface between the package pins and internal signal lines. Three other types of circuits are also available:
- 3-State buffers (TBUFs) driving horizontal long lines are associated with each CLB.
- Wide edge decoders are available around the periphery of each device.
- An on-chip oscillator is provided. Programmable interconnect resources provide routing paths to connect the inputs and outputs of these configurable elements to the appropriate networks. The functionality of each circuit block is customized during configuration by programming internal static memory cells. The values stored in these memory cells determine the logic functions and interconnections implemented in the FPGA.

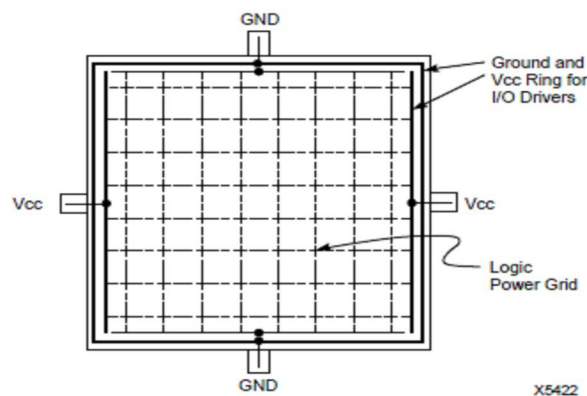
### **3.6.5 CONFIGURABLE LOGIC BLOCKS (CLBS)**

Configurable Logic Blocks implement most of the logic in an FPGA. Two 4-input function generators (F and G) offer unrestricted versatility. Most combinatorial logic functions need four or fewer inputs. However, a third function generator (H) is provided. The H function generator has three inputs. Either Zero, one, or two of these inputs can be the outputs of F and G; the other input(s) are from outside the CLB. The CLB can, therefore, implement certain functions of up to nine variables, like parity check or expandable-identity comparison of two sets of four inputs. Each CLB contains two storage elements that can be used to store the



function generator outputs. However, the storage elements and function generators can also be used independently. These storage elements can be configured as flip-flops in both XC4000E and XC4000X devices; in the XC4000X they can optionally be configured as latches. DIN can be used as a direct input to either of the two storage elements. H1 can drive the other through the H function generator. Function generator outputs can also drive two outputs independent of the storage element outputs. This versatility increases logic capacity and simplifies routing. Thirteen CLB inputs and four CLB outputs provide access to the function generators and storage elements. These inputs and outputs connect to the programmable interconnect resources outside the block.

Power for the FPGA is distributed through a grid to achieve high noise immunity and isolation between logic and I/O. Inside the FPGA, a dedicated Vcc and Ground ring surrounding the logic array provides power to the I/O drivers. An independent matrix of Vcc and Ground lines supplies the interior logic of the device. This power distribution grid provides a stable supply and ground for all internal logic, providing the external package power pins are all connected and appropriately de-coupled. Typically, a 0.1 mF capacitor connected between each Vcc pin and the board's Ground plane will provide adequate de-coupling. Output buffers capable of driving/sinking the specified 12 mA loads under specified worst-case conditions may be capable of driving/sinking up to 10 times as much current under best case conditions. Noise can be reduced by minimizing external load capacitance and reducing simultaneous output transitions in the same direction. It may also be beneficial to locate heavily loaded output buffers near the Ground pads. The I/O Block output buffers have a slew-rate limited mode (default) which should be used where output rise and fall times are not speed-critical.



**Fig 3.6 XC4000 Series Power Distribution**

### **3.6.6 PIN DESCRIPTIONS**

There are three types of pins in the XC4000 Series devices:

- Permanently dedicated pins
- User I/O pins that can have special functions
- Unrestricted user-programmable I/O pins.

Before and during configuration, all outputs not used for the configuration process are 3-stated with a 50 kW - 100 kW pull-up resistors. After configuration, if an IOB is unused it is configured as an input with a 50 kW - 100 kW pull-up resistors. XC4000 Series devices have no dedicated Reset input. Any user I/O can be configured to drive the Global Set/Reset net, GSR. XC4000 Series devices have no Power down control input, as the XC3000 and XC2000 families do. The XC3000/XC2000 Power down control also 3-stated all of the device I/O pins. For XC4000 Series devices, use the global 3-state net, GTS, instead. This net 3-states all outputs, but does not place the device in low-power mode.

## **3.7 PROM (AT17LV256)**

A programmable read-only memory (PROM) or field programmable read-only memory (FPROM) or one-time programmable non-volatile memory (OTP NVM) is a form of digital memory where the setting of each bit is locked by a fuse or anti fuse. Such PROMs are used to store programs permanently. The key difference from a strict ROM is that the programming is applied after the device is constructed.

These types of memories are frequently seen in video game consoles, mobile phones, radio-frequency identification (RFID) tags, implantable medical devices, high-definition multimedia interfaces (HDMI) and in many other consumer and automotive electronics products.

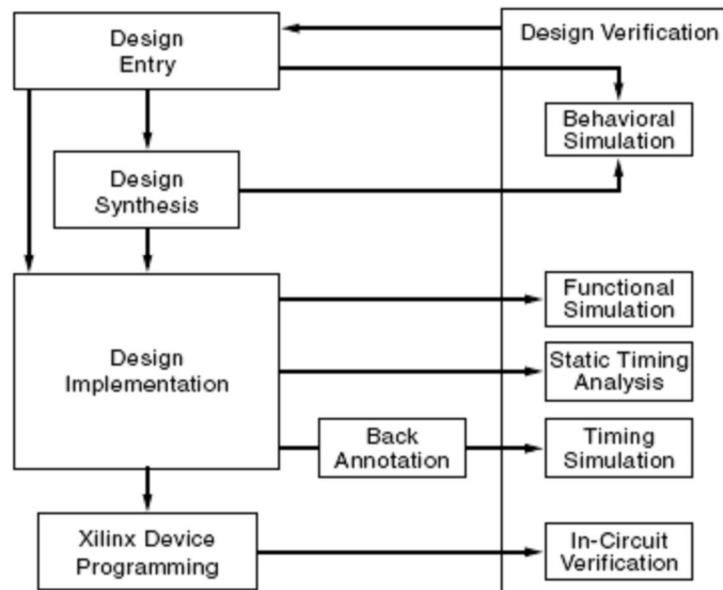
### **3.7.1 PROGRAMMING**

A typical PROM comes with all bits reading as 1. Burning a fuse bit during programming causes the bit to read as 0. The memory can be programmed just once after manufacturing by "blowing" the fuses, which is an irreversible process. Blowing a fuse opens a connection while programming an antifuse closes a connection (hence the name).

The bit cell is programmed by applying a high-voltage pulse not encountered during normal operation across the gate and substrate of the thin oxide transistor (around 6V for a 2nm thick oxide, or 30MV/cm) to break down the oxide between gate and substrate. The positive voltage on the transistor's gate forms an inversion channel in the substrate below the gate, causing a tunneling current to flow through the oxide. The current produces additional traps in the oxide, increasing the current through the oxide and ultimately melting the oxide and forming a conductive channel from gate to substrate. The current required to form the conductive channel is around  $100\mu\text{A}/100\text{nm}^2$  and the breakdown occurs in approximately 100 $\mu\text{s}$  or less.

### 3.8 XILINX

The Integrated Software Environment (ISE™) is the Xilinx® design software suite that allows you to take your design from design entry through Xilinx device programming. The ISE Project Navigator manages and processes your design through the following steps in the ISE design flow.



**Fig3.8 ISE design flow**

### **3.8.1 DESIGN ENTRY**

Design entry is the first step in the ISE design flow. During design entry, you create your source files based on your design objectives. You can create your top-level design file using a Hardware Description Language (HDL), such as VHDL, Verilog, or ABEL, or using a schematic. You can use multiple formats for the lower-level source files in your design.

### **3.8.2 SYNTHESIS**

After design entry and optional simulation, you run synthesis. During this step, VHDL, Verilog, or mixed language designs become netlist files that are accepted as input to the implementation step.

**Note:** If you are working with a synthesized EDIF or NGC/NGO file, you can skip design entry and synthesis and start with the implementation process.

### **3.8.3 IMPLEMENTATION**

After synthesis, you run design implementation, which converts the logical design into a physical file format that can be downloaded to the selected target device. From Project Navigator, you can run the implementation process in one step, or you can run each of the implementation processes separately. Implementation processes vary depending on whether you are targeting a Field Programmable Gate Array (FPGA) or a Complex Programmable Logic Device (CPLD).

### **3.8.4 VERIFICATION**

You can verify the functionality of your design at several points in the design flow. You can use simulator software to verify the functionality and timing of your design or a portion of your design. The simulator interprets VHDL or Verilog code into circuit functionality and displays logical results of the described HDL to determine correct circuit operation. Simulation allows you to create and verify complex functions in a relatively small amount of time. You can also run in-circuit verification after programming your device.

### **3.9 KEIL SOFTWARE**

Keil is an IDE (Integrated Development Environment) which is used to develop an application program, compile and run it. Even the code can be debugged. It is a simulator where we can check the application code even in the absence of the hardware board. Keil is also a cross compiler. The process of development of the soft code on a processor for a particular application and which can be implemented on the target processor is known as Cross Development. In our design the main heart of the hardware module is the micro controller which is the programmable IC. The programming language used for developing the software to the micro controller is Embedded C /Assembly.

The embedded C is an extension of the conventional C. i.e Embedded C has all the features of normal C, but has some extra added features which are not available in C. Many functions in C do not support Reentrant concept of functions. C is not memory specific. i.e variables cannot be put in the desired memory location but the location of variable can be found out. In embedded C this can be done using specific inbuilt instructions. C depends on particular processor or application. Embedded C is Controller or target specific. Embedded C allows direct communication with memory.

## **CHAPTER 4**

# **EXPERIMENTAL ANALYSIS**

## EXPERIMENTAL ANALYSIS

### 4.1 CIRCUIT DIAGRAM

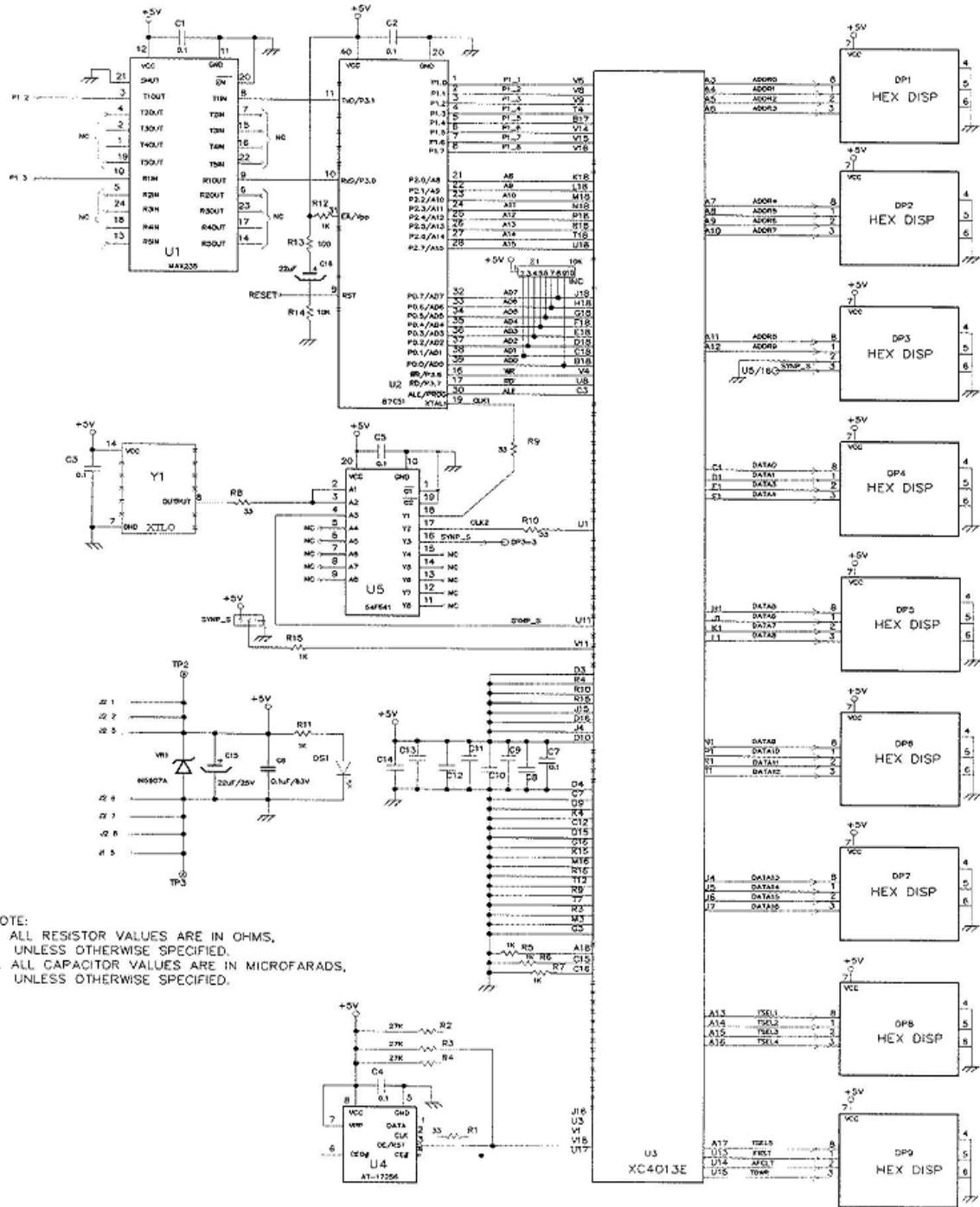


Fig 4.1 circuit diagram

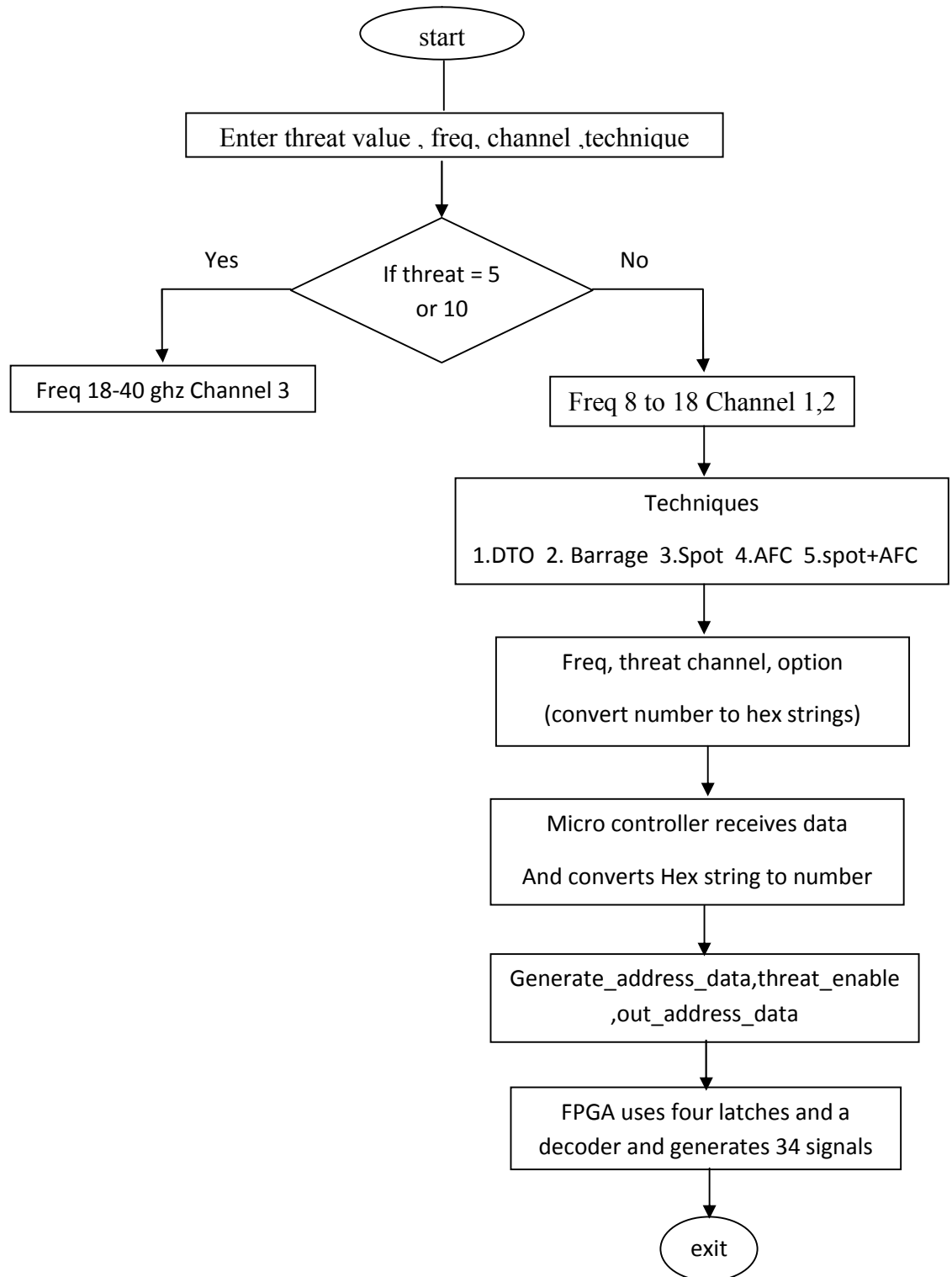
#### 4.1.1 LIST OF COMPONENTS USED

S.NO	DESCRIPTION	CKT.REF	QTY
1	MAX 235	U1	1NO
2	μC 87C51FB	U2	1NO
3	FPGA 4013E	U3	1NO
4	PROM 17256	U4	1NO
5	54FCT541	U5	1NO
6	XTLO 10MHz	Y1	1NO
7	HEX DISPLAY	DP1-DP9	9NO'S
8	LED 5V	DS1	1NO
9	1N 5907	VR1	1NO
10	CAP 0.1μF	C1-C14	14NO'S
11	CAP 22μF	C15,C16	2NO'S
12	RESISTOR 33Ω	R1,R8,R9,R10	4NO'S
13	RESISTOR 27KΩ	R2,R3,R4	3NO'S
14	RESISTOR 1KΩ	R5,R6,R7,R11,R12,R15	6NO'S
15	RESISTOR 100Ω	R13	1NO
16	RESISTOR 10KΩ	R14	1NO
17	RESISTOR N/W 10KΩ	Z1	1NO
18	9PIN FEMALE CONN	J1	1NO

**Table 4.1 List of Components used**



## 4.2 FLOW CHART



## **CHATER 5**

### **RESULT AND ANALYSIS**

## RESULT AND ANALYSIS

### 5.1 TEST SETUP

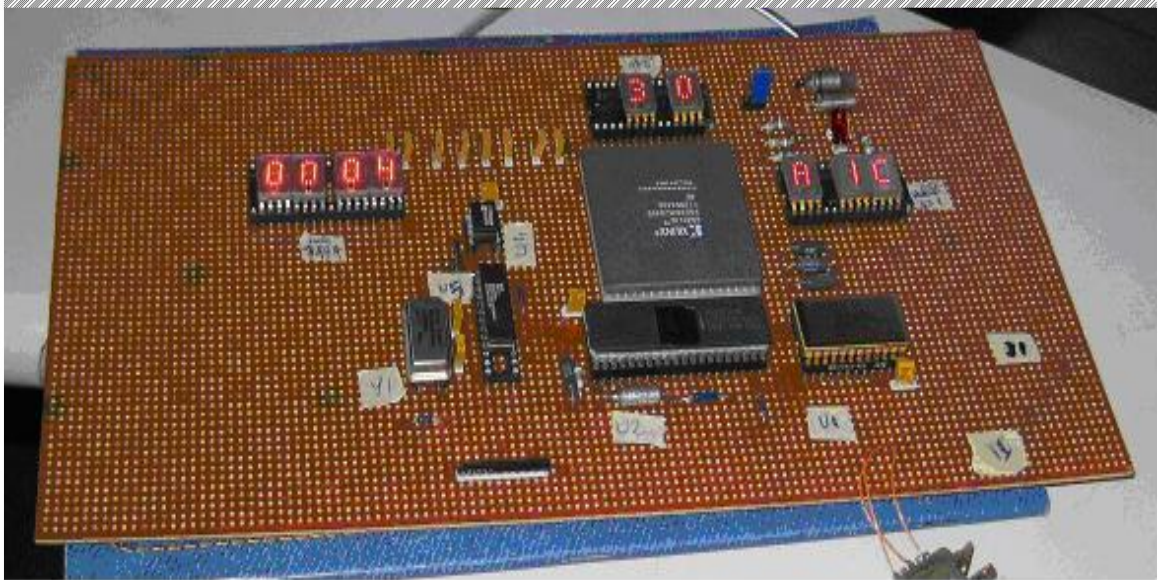


Fig 5.1.1 PCB designed TEST JIG

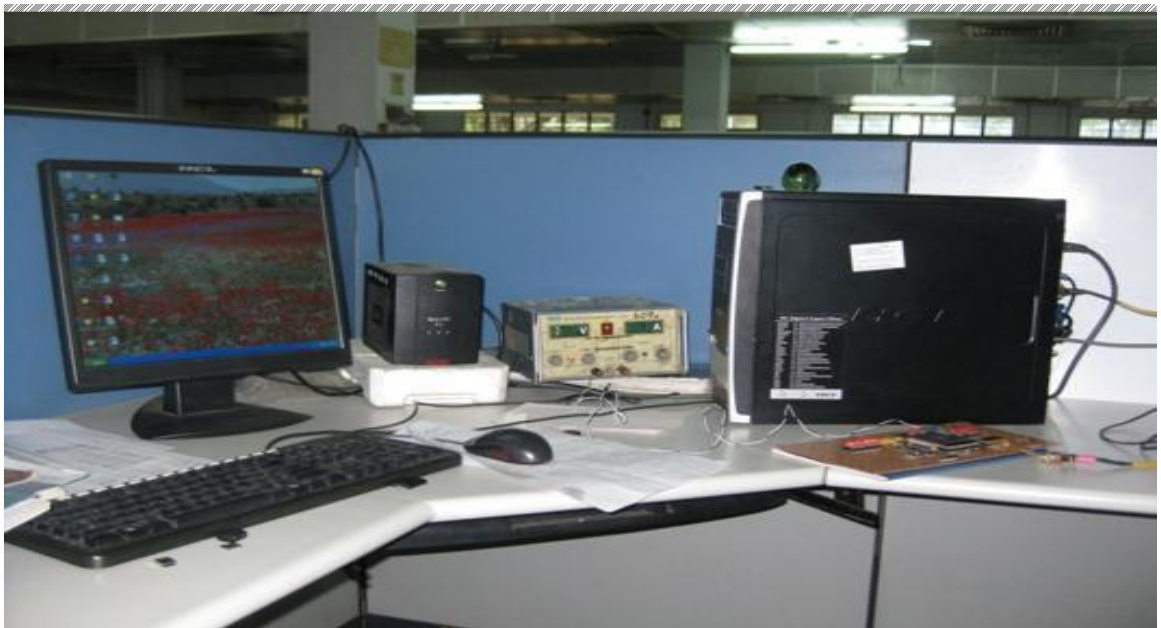


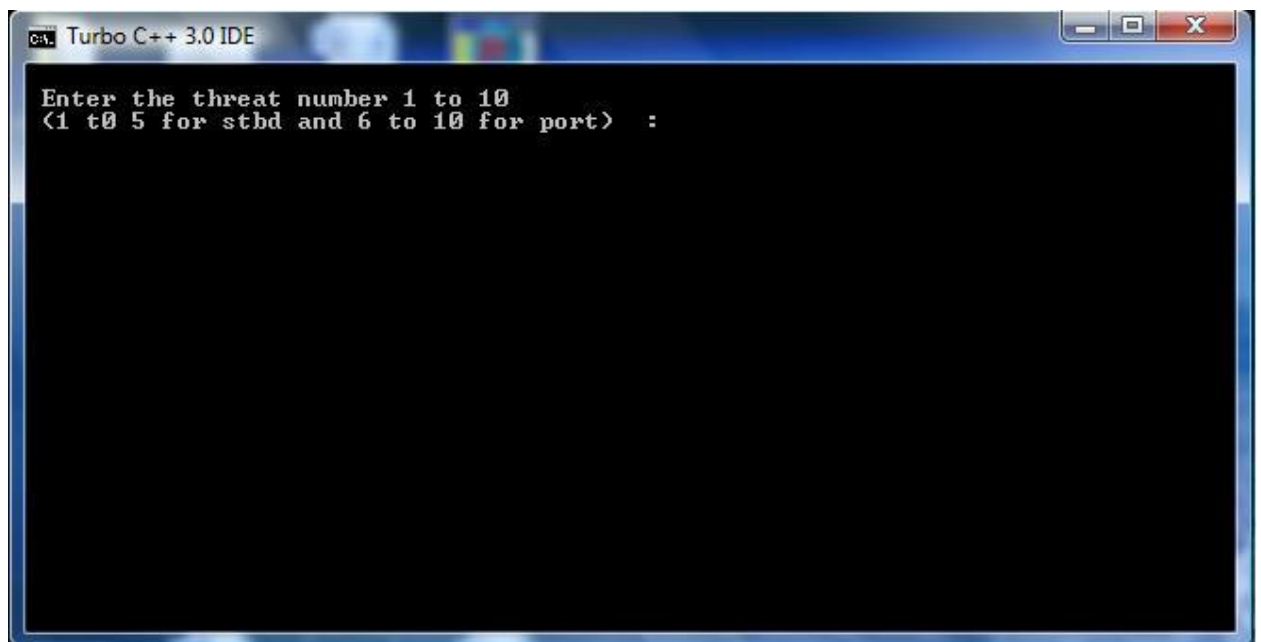
Fig 5.1.2 Experimental Test Setup

## 5.2 SNAP SHOTS

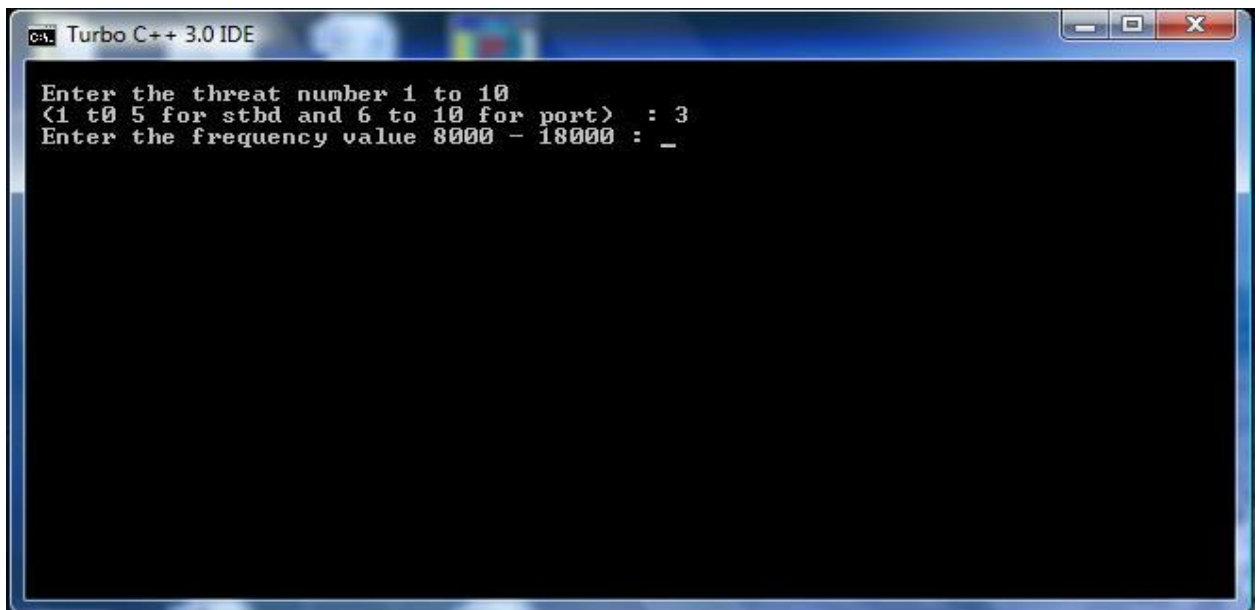
### SELECTING THE COMPORT



### SELECTING THE THREAT VALUE



### ENTERING THE FREQUENCY VALUE



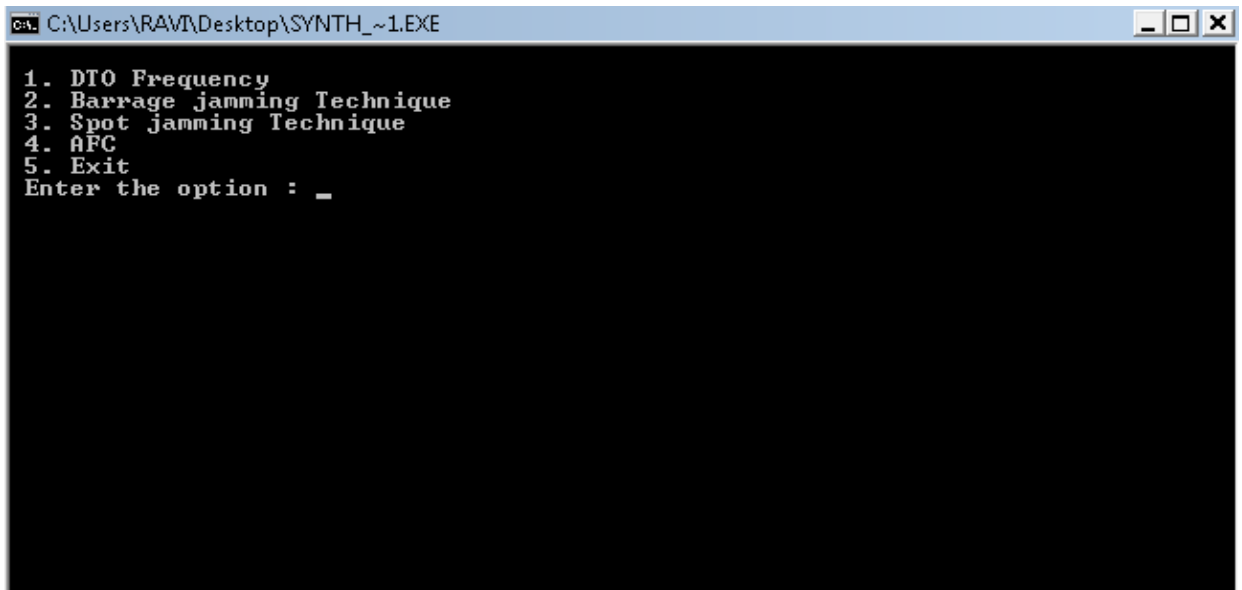
The screenshot shows the Turbo C++ 3.0 IDE window. The title bar reads "C:\ Turbo C++ 3.0 IDE". The main text area contains the following text:  
Enter the threat number 1 to 10  
<1 to 5 for stbd and 6 to 10 for port> : 3  
Enter the frequency value 8000 - 18000 : \_

### SELECTING CHANNEL VALUE

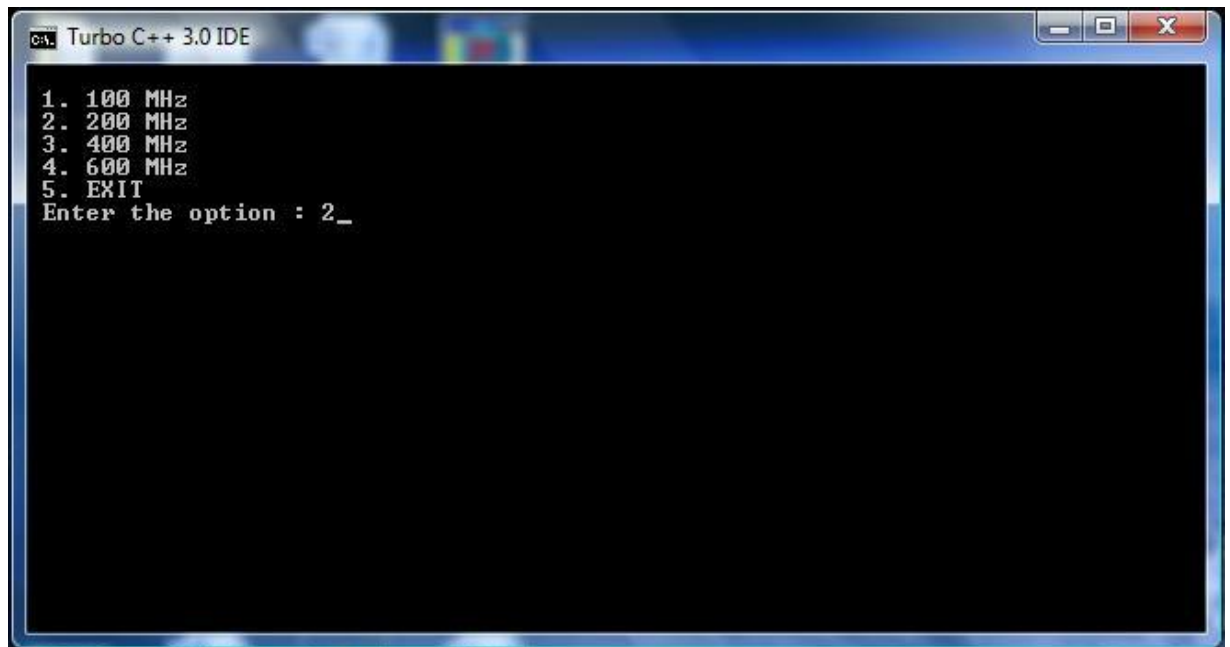


The screenshot shows the Turbo C++ 3.0 IDE window. The title bar reads "C:\ Turbo C++ 3.0 IDE". The main text area contains the following text:  
Enter the threat number 1 to 10  
<1 to 5 for stbd and 6 to 10 for port> : 3  
Enter the frequency value 8000 - 18000 : 10000  
Enter the channel number 1 Or 2 : \_

## SELECTING TECHNIQUE



## SELECTING JAMMING FREQUENCY



After selecting these values corresponding address, data, control signal will be generated.

### 5.2.1 FEW EXAMPLES

SYN P_S	THREAT	FREQ	CHNL	TECH	B.W	ADDRES	DATA	CNTR
P	T1	8000	1	DTO	--	200	81AF	21
P	T2	9000	2	Barrage	100	204,219,207	A4F1,0004,0010	22
P	T3	10000	1	Spot	20	208,21A,20B	8832,0004,0004	24
P	T4	11000	2	AFC	--	20C,215,216	AB73,0AAA,007B	68
P	T5	18000	--	DTO	--	210	A597	30
S	T6	12000	1	DTO	--	A20	900F	21
S	T7	13000	2	Barrage	400	A24,A39,A27	B2A9,0004,0018	22
S	T8	14000	1	Spot	60	A28,A3A,A2B	9544,0004,000C	24
S	T9	15000	2	AFC	--	A2C,A15,A16	B7DF,0492,007B	68
S	T10	20000	--	Barrage	200	A30,A3C,A3D	AC1A,0004,0014	30

## **CHAPTER 6**

### **SUMMARY, FUTURE SCOPE AND CONCLUSION**



## **SUMMARY, FUTURE SCOPE AND CONCLUSION**

### **SUMMARY:**

Basically the synthetic module has 3 Radio Frequency channels. Channel 1,2 generate 8 to 18 GHz range frequencies and channel 3 generates frequencies in the range of 18 to 40 GHz. The synthetic module is enabled using the 3<sup>rd</sup> channel. But the simulator works in the range of 8GHz to 18GHz. Thus up conversion methodologies are implemented in the synthetic module. The actual bits needed as output from the simulator module are 10 bit address, 16 bit data and 8 control bits. Here the 8 control bits are 5 threat signals, a write signals, 1 reset signal and 1 look through signal bits.

The Port 1, port 2 is used from controller to drive these 34 signals thus we make use of additional components namely 4 latches, 1 AND gate, and a decoder. These additional components are designed on the FPGA for the generation of the required 34 signal lines and then either given to the synthetic channel directly or to display module for checking pattern. Thus the FPGA basically acts as a pattern generator.

Here the mentioning of 5 threat signals defines the capability of the channels to drive particular frequency signals. Each threat command is capable of generating 4 different frequencies through one channel and the threat data being 5 hardware select pins any one must be enabled at a time. Thus we make use of a decoder. In this module we design a 3 to 5 decoder.

The latches designed on the FPGA are designed in modules. There are 4 such latch modules on the FPGA. Each latch module has 8 latches in it and the latches being single bit gate structures, the 1<sup>st</sup> latch IC gives 8 lower address bits, the 2<sup>nd</sup> latch IC gives 8 higher address bits, the 3<sup>rd</sup> latch IC gives 8 higher data bits and the fourth latch IC gives the 8 lower data bits.

**CONCLUSION:**

We have designed simulator for testing synthetic module by giving the inputs through the pc and saw the outputs in the hex displays. In the displays we can see the addresses of the inputs which are stored in the microcontroller. For a particular input one specific address is generated. Thus the required bit pattern is displayed according to the user selected frequency and threat is further given to the synthetic channel for the generation of the selected jamming technique.

**FUTURE SCOPE:**

Further advancements in electronic technology may result in allocation of higher bandwidth for the synthetic channel. The present technology in Indian Defence Systems has an operation frequency of 40GHz. Whereas the US Defence system works in the range of 60GHz. And research for further increase in the operational frequency i.e. up to 100 GHz is going on worldwide. In that case there is no need to change the hardware, just modify the program only that is software.

## REFERENCES

1. D. C. Schelher (1986), *Introduction to Electronic Warfare*, Dedham, MA: Artech House.
2. (1999), *Electronic Warfare in the Information Age*, Norwood, MA: Artech House.
3. J. B. Tsui (1986), *Microwave Receivers with Electronic Warfare Applications*, New York: John Wiley & Sons.
5. Peter J. Ashenden (1998), *The student's guide to VHDL (systems on silicon)*, Paperback.
6. [www.xilinx.com/support/documentation/white\\_papers/wp245.pdf](http://www.xilinx.com/support/documentation/white_papers/wp245.pdf)
7. [http://en.wikipedia.org/wiki/Electronic\\_Support\\_Measures](http://en.wikipedia.org/wiki/Electronic_Support_Measures)