Winter 5-2005

Dynamic modification of basic input/output system attributes via the operating system for Intel x86 architecture personal computers

Jabari R. Roberts
Southern University and A & M College

DYNAMIC MODIFICATION OF BASIC INPUT/OUTPUT SYSTEM ATTRIBUTES VIA THE OPERATING SYSTEM FOR INTEL x86 ARCHITECTURE PERSONAL COMPUTERS

A THESIS

Presented to the

Honors College at Southern University
Baton Rouge, Louisiana

In Partial Fulfillment of the Requirements for the
Honors College Degree

By

Jabari R. Roberts

May 2005

Honors College

Southern University and A and M College
Baton Rouge, Louisiana

CERTIFICATE OF APPROVAL

HONORS THESIS

This is to certify that the Honors Thesis of
Jabari R. Roberts
has been approved by the examining committee
for the thesis requirement for the Honors College degree
in Computer Science (Scientific emphasis)

Alonzo Johnson
Advisor

Joyce W.
Chairman, Honors Advisory Committee

Dean, Honors College

ACKNOWLEDGEMENT OF RESEARCH

This research was independently supported; no support, financial or otherwise, was given by an outside institution or agency.

DYNAMIC MODIFICATION OF BASIC INPUT/OUTPUT SYSTEM ATTRIBUTES VIA THE OPERATING SYSTEM FOR INTEL x86 ARCHITECTURE PERSONAL COMPUTERS

AN ABSTRACT OF A THESIS

Presented to the

Honors College at Southern University
Baton Rouge, Louisiana

In Partial Fulfillment of the Requirements for the
Honors College Degree

By

Jabari R. Roberts

May 2005

ABSTRACT

Currently in the world, computers are used in order to do numerous actions to benefit humanity at large. Part of the computer power is used within the realm of personal computer workstations, which is the most widely used type of computer. However, in a lot of ways, the current computer is inefficient. Much of the computer-buying populace buy newer computer systems that scientists in the 1970s and 1980s could only dream of, but use an average of only 20-30% of its full processing capabilities during its operation. In other words, many beginner and novice users simply don't use its full capabilities; a person does not need a computer operating at 2.80 GHz [gigahertz] (2,800 MHz [megahertz]), a very fast clock speed, to play Solitaire or browse a text page on the Internet. For those purposes, a 350 MHz computer is sufficient. With the above comparison in mind, 2.45 GHz (or 2,450 MHz) of the clock speed is simply used to speed up the process. A benchmark is needed for a full comparison, but currently this is a very wasteful use of resources, since newer computers more often need more electricity to power that much speed, which requires that more thermal discharge (i.e. heat) needs to be exhausted out of computer systems since heat is the "natural enemy" of most electronics. Also, some expert users would like to go above the ordinary clock speed capabilities of their processor, but do not have an easy to use utility for doing so. How can users easily minimize the amount of inefficiency and waste used by the newest personal computer dynamically by operating the computer within its needed capability and nothing more, while still allowing for advanced users to tweak the computer as they will as well as prohibiting the dynamic changes being made for the times that maximal computing

"Dynamic Modification of Basic Input/Output System Attributes via the Operating System for Intel x86 Architecture Personal Computers" was created.

Via thorough research and study into the technology of the Basic Input/Output System (BIOS) for the typical consumer personal computer, this study formed a conceptual basis for arriving to the solution to this problem. Also, this study deals with one of the most important pieces of software inside of the computer: the software, or "firmware" for the BIOS. The solutions include user applications for manipulating BIOS characteristics, or in layman's terms, "tweaking" the BIOS, through consumer operating systems; changing the structure of the BIOS to support the greater integration of external devices to the computer, such as manipulability-capable power supplies; and the discussion of using newer technology and its limitations to solving the problems presented by the BIOS structure on a personal computer, including a technology to replace the BIOS concept, called project Tiano, by Intel Corporation. Conclusions reached include the fact that the current BIOS structure has limitations, but by modifying certain characteristics of the x86 personal computer architecture to supplement greater control by the user over the computer hardware, users may now finally fine-tune the computer to what they wish based on the hardware (specifically, the processor and memory) level of a personal computer system.

AUTHOR'S ACKNOWLEDGEMENTS

The author of this thesis would like to acknowledge and thank the following for making the study, writing, and overall work of this thesis possible:

- Mr. Alonzo Johnson, for his advisement, patience, and understanding during this endeavor, as well as assistance in generating this thesis topic;
- Dr. Beverly Wade, Dean of the Honors College, for her patience and care of all of her students during the thesis studying period;
- The faculty and staff of the Department of Computer Science and of the Honors College for their assistance in making this thesis possible.

The author gives special thanks and dedications to the following:

- The author's family, especially the author's mother, Mrs. Pamela Redd, for without their care, love, and guidance, matriculation, let alone this thesis, would not have been possible;
- Mr. Mayo Brew, for his assistance and dedication to the care of the author and others in the Circle of Excellence program at Southern University;
- Dr. Edward Jackson, Chancellor of Southern University – Baton Rouge, for without his help matriculation would not occur at Southern University;
- The author's friends and colleagues, for without their love and assistance, matriculation would be terribly arduous, to say the least.

Dedicated to the concepts of Knowledge, Understanding, Peace, Love, and Balance…

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I
BACKGROUND OF THE STUDY

Introduction

Personal computers are used throughout the lives of most people for various purposes. Whether for leisure, business, or education, they constitute a part of daily life. This occurs whether a particular person is using the computer or not, as persons can be indirectly affected by another's use of a personal computer or workstation. One of those indirect effects that shall be addressed is efficiency, or the lack thereof, in personal computers. Too often, much raw computing power is wasted by the personal computer sitting idle, or there is too much power used for a low-power activity, such as browsing websites without much active content (i.e. a website containing animations, movies, and other multimedia objects). As an example, the full clock speed of a 2.8 GHz processor is not required for an activity that only needs 800 MHz (0.8 GHz) of processor clock speed to run. Also, power users, such as gamers, would like to have a better, easier solution to expand processing power beyond the rated capabilities of a processor. This is done using a process called "over clocking." To help remedy these situations, the concept of Dynamic Modification of the Basic Input/Output System Attributes via the Operating System (with a concentration on personal computers running on the 32-bit Intel x86 architecture, i.e. most "IBM-Compatible" personal computers) was theorized. To fully understand and to provide a rationale for the study of this concept, a background to this study is used to help answer the following issues central to this theory:

- *Issue 1.* How can users easily minimize the amount of inefficiency and waste used by the newest personal computer dynamically by operating the computer within its needed capability and nothing more?
- *Issue 2.* How can the specification in Issue 1 be implemented while still allowing for advanced users to tweak the processing power of their computer to their will?
- *Issue 3.* How can the specifications in both Issue 1 and Issue 2 be implemented at the same time that prohibit the dynamic changes being made for the times that maximal computing power is necessary?

Framework

To better understand the nature of this concept, as well as its conceptual and hypothetical implementation, the study of the Dynamic Modification of Basic Input/Output System Attributes must be organized. This study being done shall be organized in the following order of steps (shown here in outline form):

1. Formulate and refine the "Dynamic BIOS modification through the Operating System" concept for initial research
2. State the problem at hand with the implementation of the Dynamic BIOS modification concept
3. Give hypothesis on how the problem can be best approach to being solved (i.e. how best to implement this concept, which will lead to the usage of other conceptual solutions to this problem)

4. Give background and simplification for the non-computer science oriented person on the following aspects of computer hardware (not necessarily in the order given below):
    a. power modification to the processor
    b. bus speed modification
    c. processor clock speed step-up and step-down (i.e. processor clock speed scaling)
    d. power modification to the motherboard
    e. memory space considerations (such as ROM [read-only memory], RAM [random access memory], and NVRAM [non-volatile random access memory], all of which in computer hardware)
    f. Operating System (OS) considerations
    g. End-user considerations
5. Integrate concepts and research and offer enhanced concept
6. Experiment and attempt to implement concept in a prototype structure/machine (preferably for a real machine that I shall obtain and use for experimental purposes)
7. State results and observations throughout research period
8. Give conclusions, with further observations about feasibility done with current equipment, or if further modifications are required with the architecture. Also determine if further research is required for this endeavor.

In further detail, these steps are described as follows:

Conceptualization of the phenomenon seen in [illegible] computing systems and the phenomenon of processing power in relation to the complexity of the applications and processes executed on the personal computer, the phenomenon of the lack of efficiency was found and the problem is internalized.

- *Formation of the hypothetical solution to the phenomenon seen.* To resolve the problem of low efficiency in typical computing, the hypothetical solution of Dynamic Modification of Basic Input/Output System Attributes via the Operating System for Intel x86 Architecture Personal Computers was conceptualized.
- *Describe concepts relating to the solution.* For those who do not understand concepts used in computing, certain concepts outlined in step (4) above will be defined below in the section titled <u>Definition of Terms</u>. This is needed to fully understand the problem and solution in greater detail.
- *Research and formation of concepts, including refinement if necessary.* This is done to refine the solution and to begin the implementation of the concept.
- *Implementation of the concept after refinement.* An attempt will be made to experimentally place the concept in practice with test hardware of a typical personal computer system.
- *State results of the observations and testing of the experimental concept.*
- Formulate conclusions and accept, refine, or reject concept as necessary, which will also test for feasibility in real-world applications for different situations, as well as applicability.

The above steps are in similar fashion to the steps of the Scientific Method, which are typically composed of the following:

1. Observe and describe some phenomenon.
2. Form a hypothesis to explain the phenomenon and its relationship to other known facts, usually through some kind of mathematical formula.
3. Use the hypothesis to make predictions.
4. Test those predictions by experiments or further observation to see if they are correct.
5. If not, reject or revise the hypothesis. (Rampton and Stauber 196)

Definition of Terms

For full understanding of the concept of Dynamic BIOS modification via the OS, certain terms and acronyms such as BIOS and OS must be defined in detail, as they will be used frequently throughout this study. Here are the definitions of objects used in computer hardware and software (in alphabetical order):

- **Basic Input/Output System (BIOS):** The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

  The BIOS is typically placed on a ROM chip that comes with the computer (it is often called a ROM BIOS). This ensures that the BIOS will always be available and will not be damaged by such failures. It also makes it possible [illegible] to boot itself (BIOS FAQ).

- **Bus:** A communication pathway connecting two or more devices (Stallings 69).
- **Central Processing Unit (CPU):** Controls the operation of the computer and performs its data processing functions, often simply referred to as processor (9).
- **Operating System (OS):** A program that controls the execution of application programs and acts as an interface between the user of a computer and the computer hardware for ease-of-use and efficiency for the end-user (239).

Statement of Purpose

The purpose of this concept of BIOS modification (and therefore modification of the computer hardware characteristics) through the operating system is fourfold:

1. *To provide an easy-to-use, yet highly effective alternative for end-users to modify characteristics of their personal computer hardware without having to reboot the computer (i.e. end-users can operate this utility while the computer is in main operation) and having to use BIOS setup, which can be very difficult to access or confusing to the end-user.*
2. *To save resources associated with the operation of computer hardware, such as power usage of such materials (including, in concept, the main power supply for the computer), thereby saving money for the end user in terms of total cost-of-ownership of a personal computer system.*

unit [CPU], power supply, and motherboard components) by tuning computer hardware for the needs of the user, especially by minimizing thermal output for the situation of the usage of the computer.

4. *To provide for higher optimization and better use of software resources of the operating system, as well as to help make operating systems for computer better able to handle different computing situations.*

All of the above objectives are intended to assist the end-user in the enjoyment of the machine while economizing on resources when appropriate.

Detail of Hypothesis

With the issues and purpose of computer efficiency detailed, the hypothetical solution can now be defined in detail. Hypothetically, a solution to help resolve the problem of computer efficiency is the concept of Dynamic Modification of Basic Input/Output System Attributes via the Operating System for Intel x86 Architecture Personal Computers. This concept is defined as the modification of characteristics that affect the computer such as memory, central processing unit, and data interface attributes through the operating system (e.g. Microsoft Windows, Red Hat Linux) while the user is working in the personal computer's operating system. Also, the attributes can change dynamically; that is, automatically without user input being necessary. This can be utilized to increase or decrease processing power as needed for the particular application (or lack thereof) of the personal computer.

Limitations

This study seeks to formulate a method to dynamically modify the system BIOS attributes in the operating system that is easy for the end-user of the computer system to operate. As this is modifying some of the basic structure within the BIOS, there are a number of limitations within studying, and especially experimenting, upon this concept. This includes the following reasons:

- The different types, manufacturers, and revisions of BIOS software (commonly called "firmware" in this case) for each motherboard type and manufacturer
- Accessing proprietary information or code inside of the BIOS, which may be inaccessible
- Lack of thorough documentation of source code available for BIOS firmware (for proprietary use and reasons)
- Lack of suitable motherboards to test, which during the testing process may render them unbootable, and thus inoperable

It shall be known for the above reasons that this study is more of a conceptual than of a purely experimental basis, due to lack of accessible resources and documentation on modification through avenues other than the established routes. This study will seek to work around these limitations as much as possible.

Rationale

The rationale for the study is to solve these issues described above:

by the newest personal computer dynamically by operating the computer within its needed capability and nothing more?

- *Issue 2.* How can the specification in Issue 1 be implemented while still allowing for advanced users to tweak the processing power of their computer to their will?
- *Issue 3.* How can the specifications in both Issue 1 and Issue 2 be implemented at the same time that prohibit the dynamic changes being made for the times that maximal computing power is necessary?

Further rationale is given to solve the inefficiency problem described as such:

> “Much of the computer-buying populace buy newer computer systems that scientists in the 1970s and 1980s could only dream of, but use an average of only 20-30% of its full processing capabilities during its operation. In other words, many beginner and novice users simply don’t use its full capabilities; a person does not need a computer operating at 2.80 GHz [gigahertz] (2,800 MHz [megahertz]), a very fast clock speed, to play Solitaire or browse a text page on the Internet. For those purposes, a 350 MHz computer is sufficient. With the above comparison in mind, 2.45 GHz (or 2,450 MHz) of the clock speed is simply used to speed up the process. A benchmark is needed for a full comparison, but currently this is a very wasteful use of resources, since newer computers more often need more electricity to power that much speed, which requires that more thermal discharge (i.e. heat) needs to be exhausted out of computer systems since heat is the “natural enemy” of most electronics. Also, some expert users would

> like to go above the ordinary clock speed capabilities of their processor, but do not have an easy to use utility for doing so." (Prospectus)

With this study, an attempt shall be made to solve this problem and to help conserve precious resources, both electronic (such as memory) and environmental (such as minimizing the destruction of the Earth by using more electricity and Earth resources). When this hypothetical solution is in action, considering the numbers of computers used throughout the world, the potential in resource savings and the elimination of unnecessary consumption is enormous. This will also help in strengthening user choice by allowing an easier method for end users to modify or "tweak" their system as they see fit, thereby demystifying the inner workings of their computer.

CHAPTER II
REVIEW OF LITERATURE

Formulation of the Dynamic Basic Input/Output System (BIOS) modification through the Operating System (OS) concept was mainly an independent effort. In order to thoroughly document and supplement independent research for this endeavor, much research into the inner workings of the BIOS (and in turn, the computer) was undertaken. The following is initial research done in order to understand the concept of the Basic Input/Output System, its relation to attribute setting for computer system hardware, and its integration with other devices inside the computer essential for user input and output functions (I/O).

To understand the structure and function of the BIOS, a basic definition of it must be given. The general definition of the BIOS is stated as follows:

> "The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions. The BIOS is typically placed on a ROM chip that comes with the computer (it is often called a ROM BIOS). This ensures that the BIOS will always be available and will not be damaged by disk failures. It also makes it possible for a computer to boot itself."[1]

A more detailed definition is given as follows:

> "All computer hardware has to work with software through an interface. The BIOS gives the computer a little built-in starter kit to run the rest of softwares from floppy disks (FDD) and hard disks (HDD). The BIOS is responsible for booting the computer by providing a basic set of instructions. It performs all the

[1] From WimsBIOS.com: "BIOS FAQ." Internet Site: http://www.wimsbios.com/HTML1/faq.html#q1

> operating system from FDD or HDD). Furthermore, it provides an interface to the underlying hardware for the operating system in the form of a library of interrupt handlers. For instance, each time a key is pressed, the CPU (Central Processing Unit) perform an interrupt to read that key. This is similar for other input/output devices (Serial and parallel ports, video cards, sound cards, hard disk controllers, etc...). Some older PC's cannot co-operate with all the modern hardware because their BIOS doesn't support that hardware. The operating system cannot call a BIOS routine to use it; this problem can be solved by replacing your BIOS with an newer one, that does support your new hardware, or by installing a device driver for the hardware."[2]

In general, the BIOS is responsible for bringing the computer to "life" and assisting the operating system (which is the interface between the computer hardware/applications and the users) to contact the input devices (e.g. keyboard, mouse, joystick) and output devices (e.g. monitor, data files, status lights) for the personal computer system.

In terms of using the BIOS to manipulate hardware options and capabilities inside the personal computer system, there is also another component used, called the CMOS (Complementary Metal Oxide Semiconductor). A more detailed description of the CMOS and its functions, as well as how it interrelates to the BIOS, is given as follows:

> "To perform its tasks, the BIOS need to know various parameters (hardware configuration). These are permanently saved in a little piece (64 bytes) of CMOS RAM (short: CMOS). The CMOS power is supplied by a little battery, so its contents will not be lost after the PC is turned off. Therefore, there is a battery and a small RAM memory on board, which never (should...) lose its information. The memory was in earlier times a part of the clock chip, now it's part of such a highly Integrated Circuit (IC). CMOS is the name of a technology which needs very low power so the computer's battery is not too much in use. Your PC's performance can be highly affected by the CMOS settings. The reason for this is that the CMOS setup allows you to specify how fast your computer reads from memory, whether or not your cache is enabled or disabled, whether or not your CPU's cache is enabled or disabled, how fast your PCI bus communicates with its

[2] From SysOpt.Com: "What is the BIOS? – A BIOS Mini-FAQ." Internet Site: http://www.sysopt.com/biosdef.html

> specify disk drive and memory configuration. In order for your hard drive to work with your system, it must be configured in the CMOS setup. The exception to that rule is SCSI drives with adaptor cards, as most have their own built in BIOS. Floppy drives can be setup in the CMOS as well; a: can be made to be b: in many systems, and other configuration options can be changed as well."[3]

"CMOS Setup" is defined thusly:

> "Setup is the set of procedures enabling the configure a computer according to its hardware caracteristics. It allows you to change the parameters with which the BIOS configures your chipset. The original IBM PC was configured by means of DIP switches buried on the motherboard. Setting PC and XT DIP switches properly was something of an arcane art. DIP switches/jumpers are still used for memory configuration and clock speed selection. When the PC-AT was introduced, it included a battery powered CMOS memory which contained configuration information. CMOS was originally set by a program on the Diagnostic Disk, however later clones incorporated routines in the BIOS which allowed the CMOS to be (re)configured if certain magic keystrokes were used."[4]

("CMOS Setup" is also commonly known as "BIOS Setup." For simplicity, as well as using terminology that is utilized by most computer users, references to "BIOS Setup" will also mean "CMOS Setup" except when explicitly indicated otherwise. This is also the case with "BIOS Attributes" and "CMOS Attributes.") In summary, when the computer is turned on, the follow steps are undertaken by the BIOS in order to initialize the processor and to start (and continue to run) the computer:

1. Check the CMOS Setup for custom settings
2. Load the interrupt handlers and device drivers
3. Initialize registers and power management
4. Perform the power-on self-test (POST)
5. Display system settings
6. Determine which devices are bootable
7. Initiate the bootstrap sequence[5]

[3] Ibid.

[4] Ibid.

[5] Tyson, Jeff. How Stuff Works: "How BIOS Works." Internet Site: http://computer.howstuffworks.com/bios.htm

In detail, the BIOS controls and initializes other devices inside of a computer system, such as the various extension cards (e.g. video cards, sound cards, and other buses such as SCSI for disks), for the operating system to use. The operating system is defined as the interface between the user and the hardware/software inside of the computer system; it is the method of which the user can interact with the computer system. This is initialized after all other checks are satisfied in the computer system (i.e. step 7 above, in the "bootstrap" sequence more commonly known as the bootup process). Note that many of the auxiliary devices aforementioned have a BIOS of their own that is initialized during the bootup process; the dynamic modification of these type of BIOS is beyond the scope of this study. This study is concentrated on the main system BIOS of a personal computer on the Intel x86 architecture, which is the most common type of personal computer BIOS. Throughout the study, for simplicity, "BIOS" will refer to the system BIOS used in an Intel x86 architecture personal computer.

Commonly, settings configured in the BIOS setup menus affect how each component of hardware inside the personal computer system is utilized. This is true for modern systems, since older systems, such as the example in the above quote with the original IBM PC introduced in 1981, did not have this capability to use a setup inside the BIOS. Not until the late 1980s – early 1990s were users allowed to change BIOS attributes without the aid of a specialized computer disk or manipulating manually DIP switches (small "on/off" switches) mounted on the motherboard (the main system board which computer hardware is mounted). There is one caveat with the BIOS setup system currently in place: the computer must either be shut off (for example, to change central processing unit (CPU) clock speed functions) or restarted to gain access to the BIOS Setup utility. For the purposes of this research endeavor, the concept of "BIOS/CMOS setup" shall be taken further to not only allow to change attributes while the user is within the operating system environment, but also to dynamically change BIOS/CMOS information in real time, therefore eliminating the need for the computer to be restarted and allowing the ability to manipulate attributes such as processor speed in real time. This will fulfill the first objective of this research endeavor:

> To provide an easy-to-use, yet highly effective alternative for end-users to modify characteristics of their personal computer hardware without having to reboot the computer (i.e. end-users can operate this utility while the computer is in main operation) and having to use BIOS setup, which can be very difficult to access or confusing to the end-user.

The BIOS integrates with other system devices with providing, as described above, an interrupt handler for various hardware in the computer system. Virtually all computers provide a mechanism by with other modules (I/O, memory) may interrupt the processing of the processor.[6] Interrupts are provided primarily as a way to improve processing efficiency. For example, most external devices (i.e. hardware other than the processor or internal memory) are much slower than the processor.[7] Simply speaking, an interrupt stops processor operation for the external device to "catch up" or to finish its command. In order for most users to see what they are doing or to input information into the computer, interrupts must be made several times per processor command, or cycle. Everything from information I/O to a particular output port to a tick in the computer

[6] Stallings, William. "Computer Organization and Architecture." 6th ed., p.58.
[7] Ibid.

system clock triggers an interrupt on the processor. Because of the extremely fast nature of the processor, this is invisible to the end-user. The BIOS acts as a handler to these interrupts for the devices to interact with the CPU. Thus, the BIOS acts in tandem with the CPU, computer hardware, and CMOS as a valuable asset to the function of computer hardware. It is this concept and function that shall be extended to dynamically modify the hardware attributes inside the personal computer.

"Hardware Attributes" include, but are not limited to:

- Memory (RAM, or Random Access Memory) timing
- Voltage regulation
- CPU and RAM voltage
- Power Management timing, interrupts, and actions
- Special processor features

Different characteristics of the computer hardware (such as the mainboard/motherboard, the CPU, and other hardware) can be changed by modifying the CMOS settings accessible through the BIOS. It is the pursuit of doing these dynamically, for several purposes, that is within the range of this study and which merits further investigation.

CHAPTER III
MATERIALS & METHODS

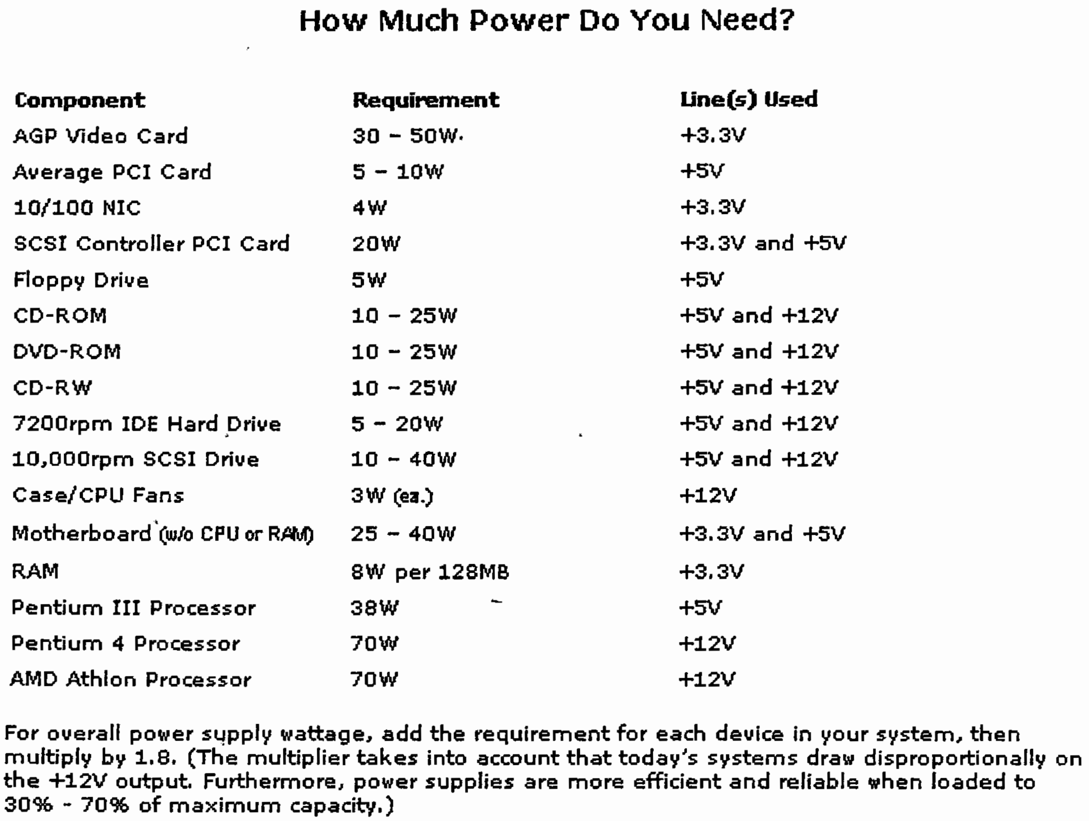
The main, or system, Basic Input/Output System in Intel x86 architecture personal computers is responsible for many of the activities that go on beyond the mere startup of the computer. For the purposes of this study, the system BIOS can be used in order to modify settings (system attributes) for the enhancement of computing performance or the conservation of energy used in a computer. It is these activities, as well as the ability for the operating system to modify settings, and to do them dynamically, that will be examined here.

Power Usage

The first activity that will be discussed in terms of modification of system attributes is power usage by the computer's hardware components, and the regulation of the power usage by the BIOS to either enhance or conserve the computer's abilities. Power usage of several sample personal computer devices is shown in Figure 1 (page 18). Each standard (ATX) power supply installed in a typical modern x86 architecture personal computer uses several lines of direct current voltage: a +3.3V line, a +5V line, and a +12V line, among others (see Figure 2, page 19). The latter voltage is used for disk drive motors and system fans, while the others are for digital circuitry.[1] From these,

[1] Brown, Gary. "How PC Power Supplies Work." How Stuff Works: http://computer.howstuffworks.com/power-supply.htm/printable.

several devices, depending on how they use power, can draw a certain amount of wattage (power) from the main computer system.



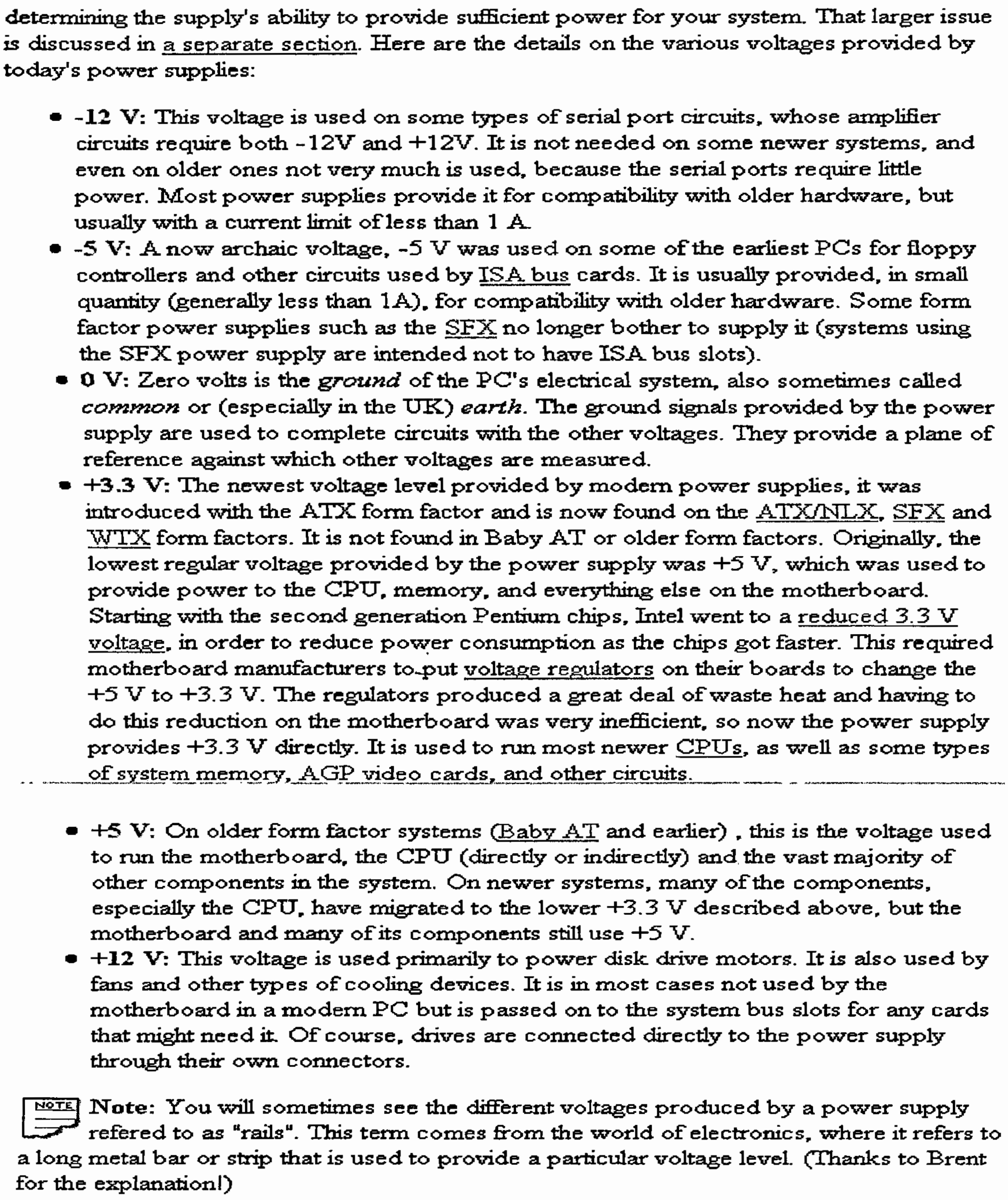
How Much Power Do You Need?

Component	Requirement	Line(s) Used
AGP Video Card	30 - 50W	+3.3V
Average PCI Card	5 - 10W	+5V
10/100 NIC	4W	+3.3V
SCSI Controller PCI Card	20W	+3.3V and +5V
Floppy Drive	5W	+5V
CD-ROM	10 - 25W	+5V and +12V
DVD-ROM	10 - 25W	+5V and +12V
CD-RW	10 - 25W	+5V and +12V
7200rpm IDE Hard Drive	5 - 20W	+5V and +12V
10,000rpm SCSI Drive	10 - 40W	+5V and +12V
Case/CPU Fans	3W (ea.)	+12V
Motherboard (w/o CPU or RAM)	25 - 40W	+3.3V and +5V
RAM	8W per 128MB	+3.3V
Pentium III Processor	38W	+5V
Pentium 4 Processor	70W	+12V
AMD Athlon Processor	70W	+12V

For overall power supply wattage, add the requirement for each device in your system, then multiply by 1.8. (The multiplier takes into account that today's systems draw disproportionally on the +12V output. Furthermore, power supplies are more efficient and reliable when loaded to 30% - 70% of maximum capacity.)

Figure 1. Power requirements and voltage lines used by personal computer devices.[2]

[2] Source: PC Power and Cooling, Inc. http://www.pcpowercooling.com/maxpc/index_cases.htm



determining the supply's ability to provide sufficient power for your system. That larger issue is discussed in a separate section. Here are the details on the various voltages provided by today's power supplies:

- **-12 V:** This voltage is used on some types of serial port circuits, whose amplifier circuits require both -12V and +12V. It is not needed on some newer systems, and even on older ones not very much is used, because the serial ports require little power. Most power supplies provide it for compatibility with older hardware, but usually with a current limit of less than 1 A.
- **-5 V:** A now archaic voltage, -5 V was used on some of the earliest PCs for floppy controllers and other circuits used by ISA bus cards. It is usually provided, in small quantity (generally less than 1A), for compatibility with older hardware. Some form factor power supplies such as the SFX no longer bother to supply it (systems using the SFX power supply are intended not to have ISA bus slots).
- **0 V:** Zero volts is the *ground* of the PC's electrical system, also sometimes called *common* or (especially in the UK) *earth*. The ground signals provided by the power supply are used to complete circuits with the other voltages. They provide a plane of reference against which other voltages are measured.
- **+3.3 V:** The newest voltage level provided by modern power supplies, it was introduced with the ATX form factor and is now found on the ATX/NLX, SFX and WTX form factors. It is not found in Baby AT or older form factors. Originally, the lowest regular voltage provided by the power supply was +5 V, which was used to provide power to the CPU, memory, and everything else on the motherboard. Starting with the second generation Pentium chips, Intel went to a reduced 3.3 V voltage, in order to reduce power consumption as the chips got faster. This required motherboard manufacturers to put voltage regulators on their boards to change the +5 V to +3.3 V. The regulators produced a great deal of waste heat and having to do this reduction on the motherboard was very inefficient, so now the power supply provides +3.3 V directly. It is used to run most newer CPUs, as well as some types of system memory, AGP video cards, and other circuits.
- **+5 V:** On older form factor systems (Baby AT and earlier) , this is the voltage used to run the motherboard, the CPU (directly or indirectly) and the vast majority of other components in the system. On newer systems, many of the components, especially the CPU, have migrated to the lower +3.3 V described above, but the motherboard and many of its components still use +5 V.
- **+12 V:** This voltage is used primarily to power disk drive motors. It is also used by fans and other types of cooling devices. It is in most cases not used by the motherboard in a modern PC but is passed on to the system bus slots for any cards that might need it. Of course, drives are connected directly to the power supply through their own connectors.

Note: You will sometimes see the different voltages produced by a power supply refered to as "rails". This term comes from the world of electronics, where it refers to a long metal bar or strip that is used to provide a particular voltage level. (Thanks to Brent for the explanation!)

Figure 2. Information about computer power supply voltages.[3]

[3] Source: Kozierok, Charles M. "Standard Output Voltages." PCGuide: http://www.pcguide.com/ref/power/sup/func_Voltages.htm.

It is important at this point to define voltage and wattage to avoid confusion:

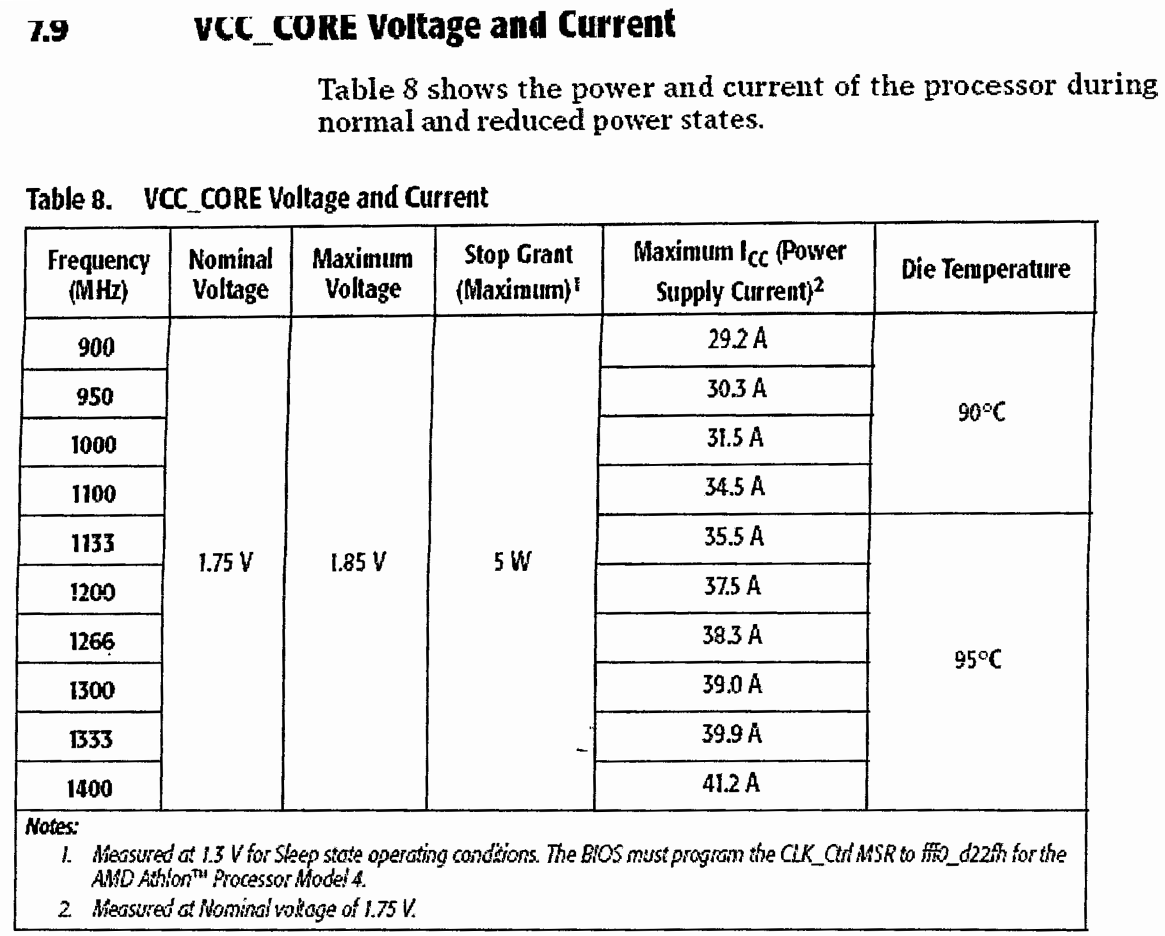
- *Wattage:* the power produced by a current of one ampere across a potential difference of one volt; it is calculated by the multiplication of current and voltage (or potential difference); that is, **P = I * V**.[4]
- *Voltage:* unit of potential equal to the potential difference between two points on a conductor carrying a current of 1 ampere when the power dissipated between the two points is 1 watt.[5]
- *Ampere:* the practical mks unit of electric current that is equivalent to a flow of one coulomb per second or to the steady current produced by one volt applied across a resistance of one ohm.[6]

Each component inside of a computer system uses a set supply of wattage for power, as well as current (necessary for calculation of the wattage required). Table 1 below shows this calculation of the maximum allowed wattage with an example power supply in possession, the TTGI TT-300SS ATX personal computer power supply (note that the voltage output and amperage for each line were provided by the manufacturer):

[4] From *Merriam-Webster's Medical Dictionary.* Source: Dictionary.com, http://dictionary.reference.com/search?q=watt.

[5] From *WordNet ® 2.0 by Princeton University.* Source: Dictionary.com, http://dictionary.reference.com/search?q=volt.

[6] From *Merriam-Webster's Medical Dictionary.* Source: Dictionary.com, http://dictionary.reference.com/search?q=ampere.



7.9 VCC_CORE Voltage and Current

Table 8 shows the power and current of the processor during normal and reduced power states.

Table 8. VCC_CORE Voltage and Current

Frequency (MHz)	Nominal Voltage	Maximum Voltage	Stop Grant (Maximum)[1]	Maximum I_{CC} (Power Supply Current)[2]	Die Temperature
900	1.75 V	1.85 V	5 W	29.2 A	90°C
950				30.3 A	
1000				31.5 A	
1100				34.5 A	
1133				35.5 A	95°C
1200				37.5 A	
1266				38.3 A	
1300				39.0 A	
1333				39.9 A	
1400				41.2 A	

Notes:

1. *Measured at 1.3 V for Sleep state operating conditions. The BIOS must program the CLK_Ctrl MSR to fff0_d22fh for the AMD Athlon™ Processor Model 4.*
2. *Measured at Nominal voltage of 1.75 V.*

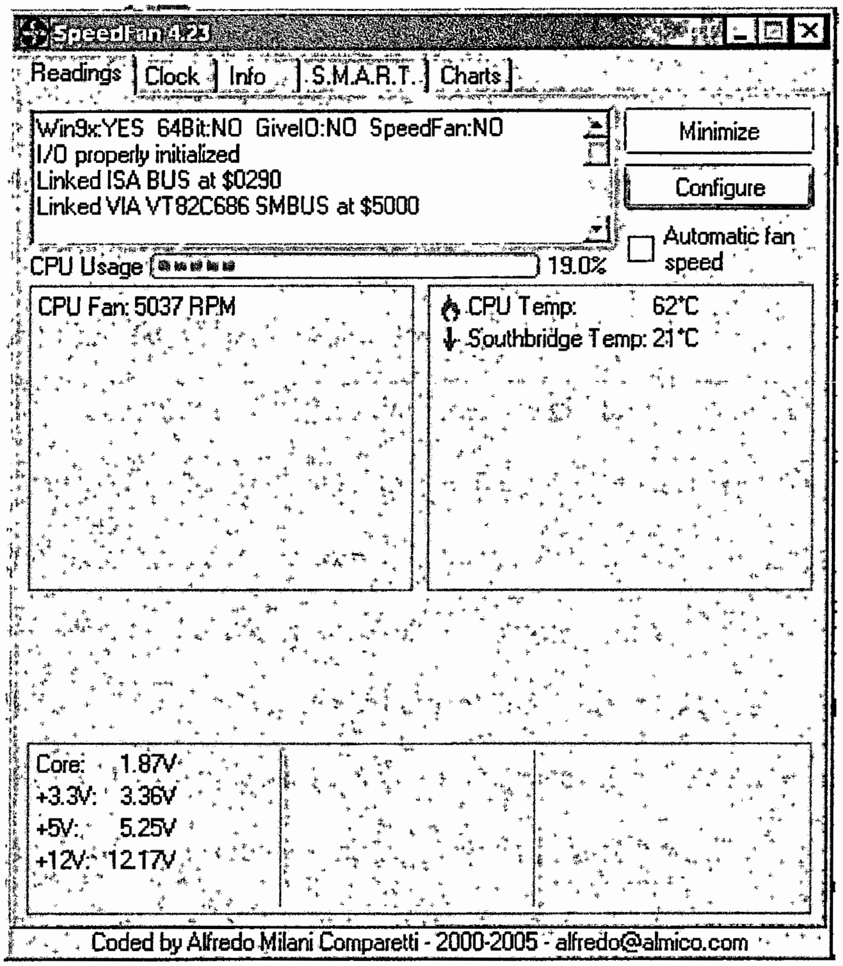
Figure 3. Power and current usage of the AMD Athlon (model 4) processor.[7]

As an example calculation, the wattage required for a 1,400 MHz Athlon Model 4 processor, using the figure above, would be (at maximum) 72.1W (using the equation P = I * V, P = 41.2 * 1.75). Compared to the 1,333 MHz processor above it, operating at 69.825W (using the same equation while plugging its respective variables)

For a "real-world" machine (i.e. under daily usage), the above processor actually works at a higher voltage than recorded in the above datasheet, according to the

[7] "AMD Athlon Processor Model 4 Data Sheet." Revision K. Advanced Micro Devices, Inc.: http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/23792.pdf, p. 41.

processor used in the "test case" computer (as shall be described below), the processor operates outside of specifications:



```
Win9x:YES 64Bit:NO GiveIO:NO SpeedFan:NO
I/O properly initialized
Linked ISA BUS at $0290
Linked VIA VT82C686 SMBUS at $5000
```

```
CPU Usage 19.0%
CPU Fan: 5037 RPM
CPU Temp:          62°C
Southbridge Temp: 21°C
Core:   1.87V
+3.3V:  3.36V
+5V:    5.25V
+12V:  12.17V
```

Coded by Alfredo Milani Comparetti - 2000-2005 - alfredo@almico.com

Figure 4. Application "SpeedFan" used to measure voltage core of AMD Athlon Model 4 processor on "test-case" computer.[8]

The "Test-Case" computer used for this example is equipped as follows:

- 1,400 MHz AMD Athlon Model 4 Processor
- Biostar M7MIA-R motherboard

[8] "SpeedFan" application is by Alfredo Milani Comparetti, http://www.almico.com/speedfan.php.

- ATI All-in-Wonder Radeon multifunction graphics board
- US Robotics 2976 FaxModem board
- Linksys Network Everywhere 10/100 Fast Ethernet board
- Artec VOM-12E48X DVD-RW drive
- Sony CRX160E CD-RW drive
- Toshiba SD-M1502 DVD-ROM drive
- Maxtor 4K080H4 IDE hard disk drive
- Seagate ST33220A IDE hard disk drive

The "Test-Case" computer is fully functional under all normal parameters of running a personal computer (e.g. booting, running the operating system, running applications, etc.). Paying close attention to the core voltage specified in Figure 4, and assuming that the hardware sensors on the motherboard of the "test-case" computer are correct, then the processor voltage is 1.87V (during normal usage) with a clock speed of 1,400 MHz. Due to the lack of suitable equipment (and non-feasibility involved in attempting to measure current of a currently used computer, since using an ammeter requires breaking a circuit first), the current was extrapolated because that, in general, as the voltage increases, so does the current. Therefore, using a proportion ([1.75V / 41.2A] = [1.87V / x], x being the estimated amperage of the "test-case" processor), the amperage is estimated to be 44.0251A, which would make the estimated wattage by using the equation (P = 1.87 * 44.0251) to be 82.327W. The relevance of this case is twofold: as the voltage increases, so does the power required to operate the particular hardware device. Also, the array of different computer configurations and quality of the hardware within them differs greatly, and thus can skew "normal" results.

Voltages are important in regards to the CPU since the frequency, or "clock speed" of the processor is dependent upon the voltage of the CPU. In general, the greater the voltage, the faster the processor (or other hardware inside of a computer) will run, but at the cost of more power. There are other factors involved, such as system bus speeds that also are relevant to this issue. Dynamically modifying the BIOS/CMOS attributes while working in the operating system will be necessary for power regulation as needed.

Access to the BIOS and CMOS

Secondly, the methods to access BIOS and CMOS information are important to know so that the hardware attributes can be viewed and edited outside of its own setup utility. Due to standardization, the BIOS is in a specific address:

> "When you first turn on your PC, the processor is "raring to go", but it needs some instructions to execute. However, since you just turned on the machine, your system memory is empty; there are no programs to run. To make sure that the BIOS program is always available to the processor, even when it is first turned on, it is "hard-wired" into a read-only-memory (ROM) chip that is placed on your motherboard.
> A uniform standard was created between the makers of processors and the makers of BIOS programs, so that the processor would always look in the same place in memory to find the start of the BIOS program. The processor gets its first instructions from this location, and the BIOS program begins executing. The BIOS program then begins the system boot sequence which calls other programs, gets your operating system loaded, and your PC up and running.
> The BIOS program is always located in a special reserved memory area, the upper 64K of the first megabyte of system memory (addresses F000h to FFFFh). Some BIOSes use more than this 64K area."[9]

[9] Source: Kozierok, Charles M. "The BIOS Program." PCGuide: http://www.pcguide.com/ref/mbsys/bios/func.htm.

> the area between C800:0000h to DF80:0000h will be searched in 2 K increments, looking for other ROMs. They, too, will be initialised after a checksum test. The memory area at 0000:0472h contains a flag which will tell the BIOS if a cold or warm boot has occurred (a value of 1234h means it is a warm boot. Being in little endian format, where the least significant byte comes first, it will be in memory as 3412). A warm boot means that most of the POST can be skipped. Once the POST is over, the BIOS looks for an operating system in various locations. Traditionally, the order is the first floppy then the first hard drive, but you can change all that in the CMOS, to include CD ROM drives, Zip drives, etc. If the floppy drive has a bootable disk in it, the BIOS will load sector 1, head 0, cylinder 0 into memory, starting at 0000:7C00h."[12]

As stated earlier, most programs that can directly access the memory of the computer (including DOS "debug") have the capability to change settings of what the computer observes in the BIOS data area and the CMOS memory.

Changing BIOS Settings for the End-User Dynamically

Lastly, the methods for accessing hardware attributes for the system BIOS and CMOS can be modified for the end-user, with certain limitations. First, since each motherboard manufacturer, and each motherboard from that manufacturer is different, care should be taken in making an end-user program change vital settings in the BIOS or CMOS since one memory location may not be the same for a specific advanced setting. An example of this is in the BIOS data area, in which addresses from 0040:00ACh to 0040:00EFh are reserved for further use by companies or for the computer system.[13] Secondly, the program must be user-friendly and come with many warnings regarding the possible breakage of system devices if a setting for a particular hardware attribute is set outside of its limits. Finally, due to the lack of information or suitable documentation

[12] Ibid., p.21.

[13] Ibid., p. 20.

from manufacturers of the x86 BIOS and the interfaces between them, it is very difficult for a programmer who is not allied with a major manufacturer to create a product to modify sensitive BIOS information. Several user programs, including TweakBIOS and cmospwd, are involved in this way in being limited to change certain hardware attributes. By design, most modifications, for example memory timing, voltage, and characteristics can be changed “on-the-fly” and are thus “dynamic” if a program can be made to keep a particular setting in a homeostatic range; that is, at a declared “normal” setting, higher or lower as needed. Also, a CLI (command-line interface, e.g. the DOS or command prompt) or GUI (graphical user interface, such as Windows and XOrg), depending on the particular application of the machine, would be vital. With homeostatically-inclined modifications to programming for a particular BIOS chipset, dynamic modification of hardware attributes can be done.

CHAPTER IV
CONCLUSION

The methods of creating a computer program to dynamically modify Basic Input/Output System attributes are in the framework of the BIOS itself. With the correct, user-friendly program, it is possible to modify settings certain system settings. However, how can the program be made homeostatic, but allows high performance when needed? The following concept will attempt to answer this question.

For example, suppose an end-user needed to leave a computer idle for 30 minutes or more, and then Disk Defragmenter runs 45 minutes after the user has left. In this case, the computer, under a homeostatic environment, would "sleep" by reducing voltages and throttling processes during the "sleep" period. When Disk Defragmenter, a highly CPU-intensive Windows program, begins the process of running, an interrupt can be called to gradually reset the CPU back to normal levels and then run the program. "Gradually" can be a defined amount of time, based on testing, as little as one second if need be.

On first glance, this matter seems to have been taken care of by the concept of Advanced Power Management, in which processors have several states to bring the processor into "sleep" mode. However, the dynamic BIOS modification concept would allow the computer to operate slower if determined by user behavior (by the program learning about the user's habits and reacting accordingly), or user-controlled. Unlike the Intel Corporation's SpeedStep technology, it can be used on desktop computers, gaining the benefits that laptop users have while the computer is operating on battery power.

Large corporations can also benefit from this technology as well. By allowing infrequently used computers to throttle down to 50% of available power for mundane tasks such as word processing and Internet browsing, a corporation can reap significant energy savings. For example, following from the table given in Figure 3 in Chapter III, if an Athlon processor that is rated for 1,400 MHz was able to slow down by reducing the wattage, to become equivalent to the 900 MHz processor, the difference in wattage used would be 72.1 – 51.1 = 21W. Multiplied by a typical large corporation, which hypothetically may have 500 computers in its various departments inside of a building, and the savings in wattage becomes 10,500W. If this throttling by dynamic modification of the BIOS were to hold for one hour, the savings would be 10.5kWh to a corporation, which is a significant savings on an energy bill when further multiplied by more computers and more hours where computers would not be in operation.

In conclusion, it has been shown conceptually that dynamic modification of BIOS attributes via the operating system for Intel x86 personal computers is possible. Unanswered questions in the research still exist, such as how to access and/or implement methods to "step down" the voltage on a CPU without having to go through the BIOS setup to do so. This is a result of non-disclosure policies affecting the major corporations, such as Phoenix Technologies, manufacturing BIOS software. Still, the concept of dynamic modification of BIOS attributes is an idea that has gathered steam, in our rush to conserve energy on the planet, or to eke out every last ounce of performance by increasing the voltage on the CPU, called "overclocking." Whatever the case may be for the use of this concept, it is the ability for users to take the use of their computer into their hands and to make the right choice.

BIBLIOGRAPHY

Blasewitz, Robert M. Microcomputer systems: hardware/software design. 1982.

Bournellis, Cynthia. "Desktop tools can audit PC BIOS." Computerworld; October 5th 1998, Vol. 32 Issue 40, p. 47.

Brown, Gary. "How PC Power Supplies Work." How Stuff Works: http://computer.howstuffworks.com/power-supply.htm/printable. Online. Internet. 4/15/2005.

Cannon, Don L. Fundamentals of microcomputer design: system hardware and software. 1982.

Clements, Alan. The principles of computer hardware. 1985.

Cripps, Martin. An introduction to computer hardware. 1977.

Croucher, Phil. "The BIOS Companion." EBook (PDF Format), available via http://www.miro.pair.com/tweakbios/bioscomp.html. 2004 ed.

Feibus, Mike. "If you liked the Pet Rock, you'll love flash BIOS." PC Week; November 8th 1993, Vol. 10 Issue 44, p. A14.

Halfhill, Tom R. "Transforming the PC: Plug and play." Byte.com; September 1994, Vol. 19 Issue 9, p. 78.

Hsu, John Y. Computer Architecture: software aspects, coding, and hardware. CRC Press, 2001.

Kozierok, Charles M. "The BIOS Program." PCGuide: http://www.pcguide.com/ref/mbsys/bios/func.htm. Online. Internet. 4/15/2005.

Kozierok, Charles M. "Standard Output Voltages." PCGuide: http://www.pcguide.com/ref/power/sup/func_Voltages.htm. Online. Internet. 4/15/2005.

Novogrodsky, Seth. The complete IBM Personal Computer: the authoritative guide to hardware for expanding the IBM PC, XT, AT, and compatibles.
1985.

Quinlan, Tom. "Intel acts to acquire BIOS technologies."
InfoWorld; January 8th 1996, Vol. 18 Issue 2, p. 27.

Sloan, Martha E. Computer hardware and organization: an introduction.
1983.

Stallings, William. Computer organization and architecture.
Prentice Hall, 2000, 5th ed.

SysOpt.Com: "What is the BIOS? – A BIOS Mini-FAQ."
http://www.sysopt.com/biosdef.html. Online. Internet. 4/15/2005.

Toy, Wing N. Computer hardware/software architecture.
1986.

Tyson, Jeff. "How BIOS Works."
How Stuff Works: http://computer.howstuffworks.com/bios.htm. Online. Internet. 4/15/2005.

WimsBIOS.com: "BIOS FAQ."
http://www.wimsbios.com/HTML1/faq.html#q1. Online. Internet. 4/15/2005.

"AMD Athlon Processor Model 4 Data Sheet."
Revision K. Advanced Micro Devices, Inc.: http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/23792.pdf. Online. Internet. 4/15/2005.

"LinuxBIOS."
LinuxBIOS.org. http://www.linuxbios.org/. Online. Internet. 4/15/2005.

APPROVAL OF SCHOLARLY DISSEMINATION

The author grants to the Honors College the right to reproduce, by appropriate methods, upon request, any or all portions of this thesis.

It is understood that “request” consists of agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without the written approval of the author of the thesis.

The author of this thesis reserves the right to publish freely, in the literature, at any time, any or all portions of this thesis.

Author Juli N. M

Date May 4th, 2005