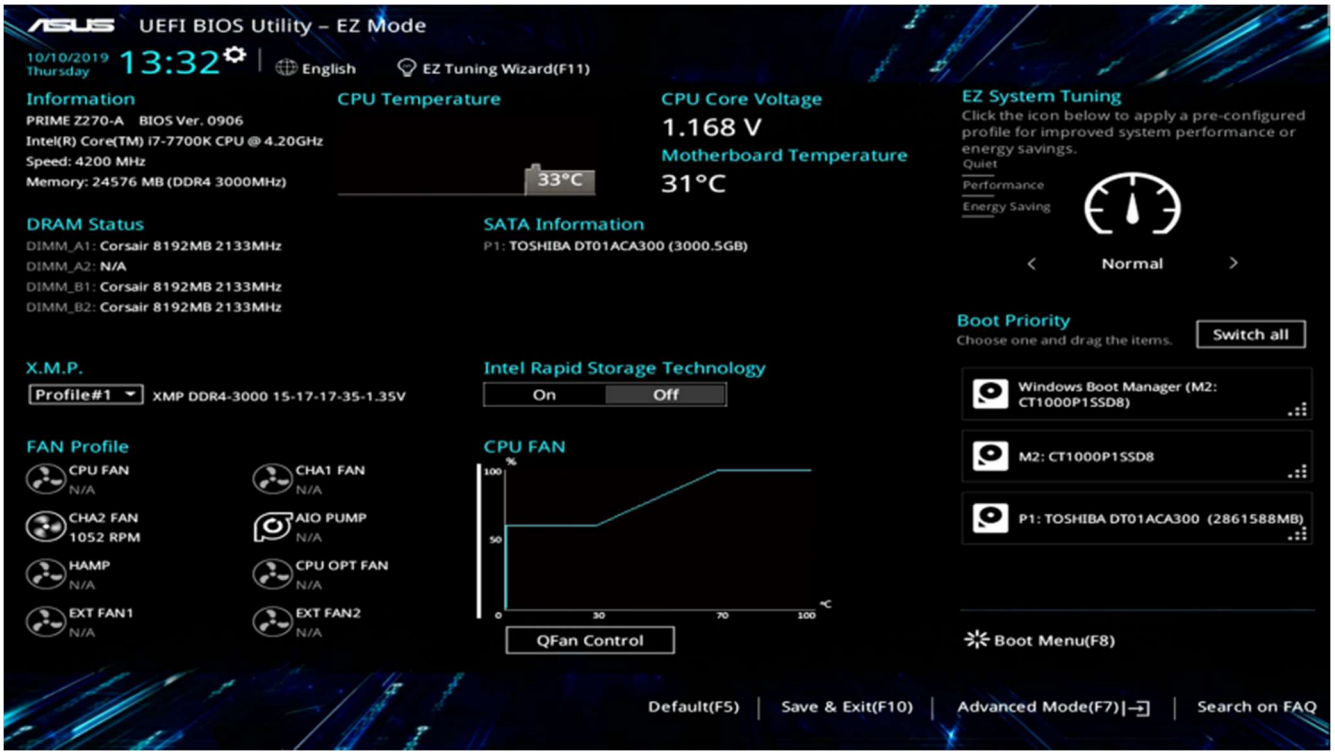
Systemressourcen



Mario Putz
IT 233

Inhaltsverzeichnis

I/O-Ports 3
DMA 3
IRQ 4
Plug & Play 5
BIOS Basic Input Output System 6
UEFI Unified Extensible Firmware Interface ... 5
UEFI und BIOS im Vergleich 7
  Update- BIOS / UEFI 8
BIOS – Startoptionen 8
  Die 4 Hauptfunktionen des BIOS: 8
  POST (Power on self Test) 8
  SETUP 9
  URLOADER 9
  SYSTEM BIOS 9
BIOS – Bootoptionen 9
  BOOT-Prozess 9

I/O-Ports

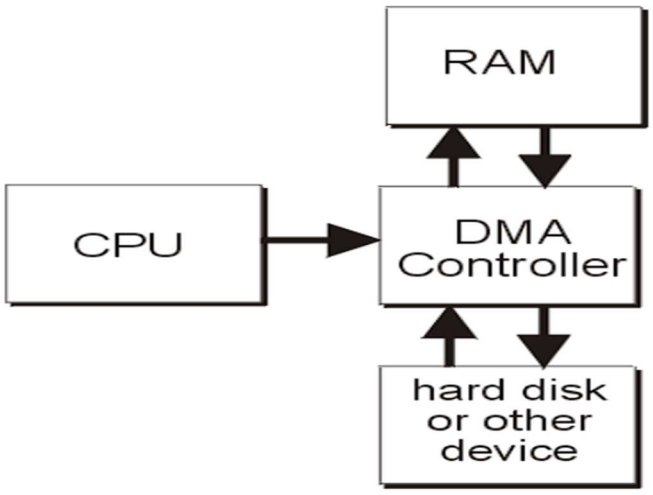
In Computern wird jedes Gerät außer der RAM von der CPU als Peripheriegerät behandelt. Der Datenaustausch zwischen dem Zentralprozessor und Peripheriegeräten erfolgt über Input-Output-Ports. I/O-Port ist ein Puffergerät oder Register, welches standardmäßig mit einer 16 Bit breiten Adresse die theoretisch 65536 verschiedene Ports ergeben. Über I/O-Ports werden eine Vielzahl von internen und externen Geräten mit dem System verbunden wobei jedem Gerät ein Bereich des I/O Adressraums zugeordnet wird. Es gibt interne sowie externe Ports welche Geräte wie Maus, Tastatur, Drucker oder auch Grafikkarten, Laufwerke und Festplatten werden via I/O-Ports mit der CPU verbunden.

DMA

Unter Direct Memory Access (Speicherdirektzugriff) versteht man, wenn Computer-Komponenten selbständig ohne Beteiligung der CPU-Daten übertragen können. Diese Technik erlaubt angeschlossenen Peripheriegeräten, wie z.B. Netzwerkkarte oder Soundkarte, ohne Umweg über die CPU direkt mit dem Arbeitsspeicher zu kommunizieren. Der Vorteil des DMA ist die schnellere Datenübertragung bei gleichzeitiger Entlastung des Prozessors.

Anders als der Name vermuten lässt, ist die wesentliche Eigenschaft von Direct Memory Access nicht der Speicherzugriff, sondern dass der Datentransfer von einem Peripheriegerät und nicht von der CPU selbst initiiert wird. Dabei braucht es zu keinen Speicherzugriffen zu kommen, es sind auch direkte Kommunikationen zwischen Peripheriegeräten möglich.

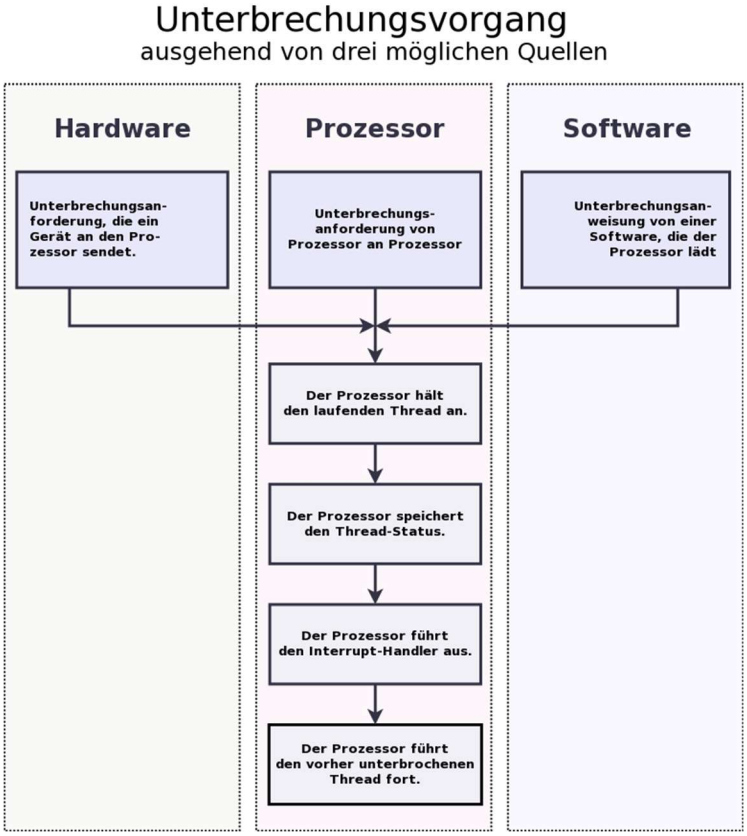
Es gibt 8 DMA-Kanäle: 0, 2 und 4 sind fest vergeben. Die Kanäle 1, 3, 5, 6 und 7 sind frei belegbar.



IRQ

In der Informatik versteht man unter einem Interrupt eine kurzfristige Unterbrechung der normalen Programmausführung, um einen in der Regel kurzen, aber zeitlich kritischen, Vorgang abzuarbeiten.
Das auslösende Ereignis wird Unterbrechungsanforderung genannt. Nach dieser Anforderung führt der Prozessor eine Unterbrechungsroutine aus. Die Unterbrechungsroutine wird mit erweiterten Privilegien ausgeführt. Im Anschluss an die Unterbrechungsroutine wird der vorherige Zustand des Prozessors inkl. Privilegierung wiederhergestellt und die unterbrochene Programmausführung dort fortgeführt, wo sie unterbrochen wurde.

Geräte, die eine Unterbrechungsanforderung senden sind z.B. Tastatur, Maus, Netzwerkkarte, Festplatte, GPU, Soundkare, Drucker, etc. Wenn ein Gerät Daten zur Verarbeitung zur Verfügung hat oder eine Rückmeldung geben will, wird dem Prozessor in seiner laufenden Arbeit eine Unterbrechungsanforderung also eine IRQ über die dem Gerät zugewiesene Leitung gesendet. Die CPU unterbricht seine aktuelle Tätigkeit und führt einen Befehl an einer bestimmten Speicheradresse aus, die vom IRQ-Eingang abhängig ist. In den folgenden Lese- und Schreiboperationen wird die IRQ abgearbeitet und die unterbrochene Programmausführung wird fortgeführt.



Plug & Play

Plug & Play manchmal auch abgekürzt mit PnP, bezeichnet eine Technologie, die es ermöglicht, mit minimalem Aufwand Peripheriegeräte an einen Computer anzuschließen und sofort zu nutzen. In der Regel genügt es, das Gerät mit einem freien Interface-Port des Rechners zu verbinden. Eine manuelle Konfiguration oder das Installieren eines Treibers ist nicht notwendig. Bevor Plug & Play in gängigen Betriebssystemen verfügbar war, mussten Erweiterungskarten und Peripheriegeräte für den Computer erst umständlich konfiguriert werden. Zudem war es notwendig, einen passenden Treiber einzuspielen. Bei Plug & Play erstellt stattdessen die anzuschließende Hardware einen eindeutigen Identifizierungscode. Anhand dieses Codes erkennt der Computer die Hardware und die angeforderten Rechnerressourcen. Er konfiguriert die für den Betrieb benötigten Parameter automatisch und lädt selbstständig einen geeigneten Treiber. Dadurch ist es möglich, neue Geräte an einen USB-Port anzuschließen und bereits nach wenigen Sekunden zu verwenden.

Das Plug & Play-Prinzip birgt allerdings auch Sicherheitsrisiken. Denn durch die automatische Konfiguration ist es prinzipiell möglich, einen Rechner durch einfaches Einstecken von Hardware zu kompromittieren: also Daten unbefugt zu lesen, zu speichern, zu löschen und zu verändern oder den Computer mit Schadsoftware zu infizieren. Hierfür könnte ein Angreifer zum Beispiel einen manipulierten USB-Stick verwenden. Aus diesem Grund ist die Plug & Play-Funktion von USB-Ports an professionell genutzten Rechnern oft besonders geschützt oder gleich ganz deaktiviert.

UEFI

Unified Extensible Firmware Interface

Das UEFI soll das klassische BIOS in PCs mit x86 und x64 Prozessoren ablösen, um mit den Unzulänglichkeiten eines veralteten BIOS aufzuräumen und neue Funktionen zu ermöglichen.
Die UEFI-Spezifikation definiert ein Embedded-System, das sich einfacher bedienen lässt, hochauflösende Grafikkarten unterstützt und netzwerkfähig ist. Die Software des UEFI ist in C geschrieben, durch die Simulation eines BIOS ist eine hohe Kompatibilität gegeben.

BIOS

Basic Input Output System

Hinter dem BIOS verbirgt sich eine Firmware, die sich auf dem Motherboard in einem nichtflüchtigen Speicher befindet. Im Gegensatz zum normalen Arbeitsspeicher wird der ROM-Baustein, auf dem das BIOS installiert ist, nach dem Ausschalten des PCs nicht gelöscht und steht daher direkt beim Start zur Verfügung. Anders als das Betriebssystem muss es nicht installiert werden, sondern ist in jedem Fall auf der Hardware des PCs vorhanden.

Das BIOS stellt die Grundfunktionen eines Computers bereit und prüft nach jedem Start des Rechners, ob die wichtigsten Teile wie Speicher, CPU und andere Hardware-Komponenten funktionsfähig sind. Dieser Test wird als **Power on Self Test** (POST) bezeichnet, stellt das BIOS im Zuge des POST einen Fehler fest, sendet es einen oder mehrere BIOS-Pieptöne über die Systemlautsprecher aus. Diese individuellen Signaltöne sollen dem Nutzer anzeigen, wo genau das Problem liegt. Der Code unterscheidet sich je nach Hersteller des BIOS.

Neben dem POST spielt es auch für die Energieverwaltung des Rechners eine wichtige Rolle, indem es für die Energiesteuerung notwendige ACPI-Tabellen generiert. Außerdem prüft es nicht nur eingebaute Festplatten, sondern auch angeschlossene Komponenten wie externe Laufwerke oder USB-Sticks auf ihre Funktionsfähigkeit. Nutzer können im BIOS einstellen, in welcher Reihenfolge die Speichergeräte angesprochen werden sollen. Das ist für solche Fälle interessant, in denen ein neues Betriebssystem von einer DVD oder einem bootfähigen USB-Stick geladen werden soll.

Das BIOS teilt dem System als Firmware mit wo das Betriebssystem zu finden ist und welche Software in den RAM geladen werden müssen. Gleichzeitig dient es als Vermittler zwischen CPU und Software. Das BIOS bildet eine Abstraktionsebene, den sogenannten **Hardware Abstraction Layer** (HAL), sodass eine Software die Details der Hardware nicht kennen muss, sondern sie standardisiert ansprechen kann.

UEFI und BIOS im Vergleich

UEFI bietet viele Verbesserungen gegenüber dem BIOS:

- **Boot-Modus**: Benutzer von Microsoft Windows haben die Wahl zwischen 32-Bit-UEFI oder 64-Bit-UEFI. Es empfiehlt sich, dass der Betriebssystem-Bitmodus und der Firmware-Bitmodus zusammenpassen, um Kommunikationsprobleme während der Laufzeit zu vermeiden.
- **Laufwerke**: UEFI-Boot unterstützt Laufwerke mit einer Kapazität von 2,2 TB und mehr, bis hin zu einer Kapazität von 9,4 Zettabyte. Damit besteht viel Luft nach oben für die Zukunft.
- **Treiber**: UEFI funktioniert mit diskretem Treiber, während die Unterstützung von BIOS-Laufwerken im ROM (Read Only Memory) gespeichert ist, was eine Abstimmung der Kompatibilität erfordert, wenn Sie Laufwerke austauschen oder Änderungen vornehmen.
- **Grafische Benutzeroberfläche (GUI)**. UEFI ermöglicht das einfachere Hinzufügen neuer Module zur GUI, einschließlich Gerätetreibern für Motherboards und angeschlossene Peripheriegeräte.
- **Mehr Auswahl beim Betriebssystem**. Während das BIOS nur einen Bootloader zulässt, können Benutzer mit UEFI Bootloader für Debian basierte Ubuntu und andere Linux-Varianten zusammen mit Windows-OS Bootloadern in derselben EFI-Systempartition installieren.
- **Programmierung**. Die UEFI-Firmware ist überwiegend in „C“ geschrieben, was es Benutzern ermöglicht, Funktionen mit weniger Programmierung hinzuzufügen oder zu entfernen als beim BIOS, das in einer Assembler-Sprache geschrieben ist, manchmal in Kombination mit C.
- **Sicherheit**. Secure Boot ist ein UEFI-Protokoll ab Windows 8, Secure Boot macht die Firmware eines Systems zum Vertrauensanker, um die Geräte- und Systemintegrität zu überprüfen. Das Ziel besteht darin, Hacker daran zu hindern, Rootkits in der Zeit zwischen dem Hochfahren und der Übergabe an das Betriebssystem zu installieren. Secure Boot ermöglicht es einem autorisierten Benutzer, Netzwerke zu konfigurieren und Probleme aus der Ferne zu beheben, wozu ein BIOS-Administrator physisch anwesend sein muss.

Update- BIOS / UEFI

Bei allen Programmen gilt die Empfehlung, ein neues Update einzuspielen, sobald es verfügbar ist. Beim BIOS / UEFI gilt das genaue Gegenteil. Updates werden hier nur empfohlen, wenn der PC nicht behebbare Probleme verursacht. BIOS- Updates werden vom Mainboard-Hersteller zur Verfügung gestellt, um zB. bekannte Bugs zu beheben oder das Funktionsspektrum auf neuere Prozessoren zu erweitern. Die Updates können entweder über einen USB mit der neuesten Version über BIOS-Flashback aktualisiert werden. Im UEFI selbst kann man über den Menüpunkt „respektive Tools“ die Umgebung aktualisieren. Manche Hersteller bieten eine Aktualisierung über das vorhandene Betriebssystem.

BIOS – Startoptionen

Die 4 Hauptfunktionen des BIOS:

- POST
- SETUP
- URLOADER
- SYSTEM BIOS

POST (Power on self Test)

Der POST ist ein Selbsttest, der noch vor dem Booten durchgeführt wird. Dabei wird geprüft ob die grundlegenden Komponenten des Gerätes funktionsfähig sind. Das BIOS meldet Fehler, die während des POST erkannt werden. Fehler, die vor der Prüfung der Grafikausgabe auftreten werden über die Systemlautsprecher, LED´s oder eine am Mainboard verbaute 7 Segment anzeige ausgegeben.

Die Überprüfung lässt sich in folgende Schritte unterteilen:

- Überprüfung der Funktionsfähigkeit der CPU
- Überprüfung der CPU nahen Bausteine
- Überprüfung des CMOS-RAM
- Überprüfung des CPU nahen Cache Speichers
- Überprüfung der ersten 64 Kilobyte des Arbeitsspeichers
- Überprüfung des Grafik Speichers und der Grafik Ausgabe
- Überprüfung des restlichen Arbeitsspeichers
- Überprüfung der Tastatur
- Überprüfung weiterer Peripheriegeräte (Laufwerke und Festplatten)

SETUP

Im BIOS-Setup sind einige Einstellungen möglich:

- Bootreihenfolge ändern (nicht genutzte Partitionen können deaktiviert werden, um den Systemstart zu beschleunigen)
- USB-Konfiguration (Einstellungen zum aktivieren und deaktivieren von USB-Ports)
- Energieverwaltungseinstellungen
- CPU prüfen und Übertakten
- Autostart Funktionen
- Arbeitsspeicher optimieren
- Zeiteinstellungen

URLOADER

Alle in den Bootoptionen aufgeführten Laufwerke werden nach einem gültigen Master-Bootsektor (MBR) durchsucht der dann geladen und ausgeführt wird.

SYSTEM BIOS

Bezeichnet die Treiber, die während des Systemstarts bereits als grundlegende Schnittstelle zwischen dem Betriebssystem und der Hardware agieren. Wenn Windows im abgesicherten Modus gestartet wird, läuft das System nahezu ausschließlich mit den BIOS-Treibern.

BIOS – Bootoptionen

Unter den Bootoptionen können einzelne Laufwerke ausgewählt oder übersprungen werden, sowie die Reihenfolge kann geändert werden. Booten bezeichnet den Prozess des Urladens des Betriebssystems auf einen PC.

BOOT-Prozess

1. Rechnerstart
2. POST
3. URLOADER sucht MBR
4. MBR wird ausgeführt
5. Lädt Betriebssystem spezifische Start Dateien
6. Start des Betriebssystems