Was sind I/O-Ports:

Als I/O Ports werden die Schnittstellen zwischen CPU und Peripheriegeräten bezeichnet. Die Kommunikation erfolgt über spezielle Maschinenbefehle, wie zum Beispiel in und out.
Jedem Gerät wird dabei ein Bereich des I/O-Adressraums zugeordnet, und Lese- bzw. Schreibzugriffe werden an das Gerät weitergeleitet.
I/O-Port dient als Adressangabe eines Peripheriegerätes für die CPU. Die CPU kann mithilfe eines bestimmten I/O-Ports Daten an ein bestimmtes Gerät senden oder von einem Gerät empfangen.
Standardmäßig ist ein I/O-Port eine 16 Bit breite Adresse, es ergeben sic theoretisch also 65536 verschiedene Ports.

Was ist DMA:

Direct Memory Access (DMA, Speicherdirektzugriff) bezeichnet eine Zugriffsart, die über ein Bussystem direkt auf den Speicher zugreift.
DMA erlaubt angeschlossenen Peripheriegeräten (z.B. Netzwerkkarte) ohne Umweg über die CPU direkt mit dem Arbeitsspeicher zu kommunizieren.
Der Vorteil des DMA ist die schnellere Datenübertragung bei gleichzeitiger Entlastung der Prozessors.
Der Zugriff der unterschiedlichen Komponenten (Steckkarten) wird anhand des Index unterschieden.
Es gibt 8 DMA-Kanäle
Die Kanäle 0, 2 und 4 sind fest vergeben.
Die Kanäle 1, 3, 5, 6 und 7 können frei belegt werden.

Was sind IRQ

Jedes Computersystem besteht nicht nur aus Hauptprozessor (CPU) und Datenspeicher, sondern auch aus der Peripherie, die im Gehäuse eingebaut oder an den äußeren Schnittstellen angeschlossen ist. Bei diesen Geräten handelt es sich um Ein- und Ausgabegeräte. Sie können zum Beispiel Daten von außen entgegennehmen. Zum Beispiel typische Eingaben, wie Maus-Bewegung, Tastatur-Eingaben oder Netzwerk-Verkehr. Damit die CPU mitbekommt, dass Daten von außen anstehen, muss es die Möglichkeit geben, den Prozessor bei seiner Arbeit zu unterbrechen.
Hierzu gibt es die Möglichkeit, dass der Prozessor alle Eingabe-Geräte zyklisch abfragt (Polling). Was bei der Vielzahl an Komponenten in einem Computer bedeuten würde, dass der Prozessor mit nichts anderem mehr beschäftigt wäre.
Eine Alternative ist die sogenannten Unterbrechungsanforderung (to interrupt, unterbrechen), die dann eintritt, wenn Daten von außen anstehen. Dazu wurde die Möglichkeit geschaffen den Hauptprozessor auf definierte Weise bei der laufenden Arbeit zu unterbrechen.
Wenn ein Gerät Daten zur weiteren Verarbeitung zur Verfügung hat oder einfach nur eine Rückmeldung geben will, dann wird dem Prozessor in seiner laufenden Arbeit eine Unterbrechungsanforderung, also ein Interrupt-Request (IRQ) gesendet. Das passiert durch den Interrupt (Leitung), der dem betreffenden Gerät zugewiesen ist.
Wird zum Beispiel ein Taste auf der Tastatur gedrückt, dann schickt der Tastatur-Controller einen IRQ an den Prozessor. Der unterbricht seine aktuelle Tätigkeit und führt einen Befehl an einer bestimmten Speicheradresse aus, die vom IRQ-Eingang abhängig ist und auf den Tastatur-Treiber verweist. In den daraufhin ablaufenden Lese- und Schreiboperationen wird dafür gesorgt, dass der Buchstabe auf dem Bildschirm erscheint.

Interrupt-Auslösegründe

Bei jeder zeitkritischen Anwendung, bei der Daten an den Prozessor gesendet werden müssen, wird ein Interrupt ausgelöst. Für den IRQ können folgende Aktionen verantwortlich sein:

- Mausbewegung
- Datenempfang vom Modem
- Tastatureingabe
- Audioaufnahme durch die Soundkarte
- Lesen von Speichermedien
- Erfolgreicher Schreibvorgang

Damit aus Anwendersicht das System optimal funktioniert, ist die Gewichtung zwischen den Interrupts unterschiedlich. So kann sich die CPU um die wichtigen Aufgaben kümmern. Bei Überlastung kann es trotzdem dazu kommen, dass wichtige Daten nicht rechtzeitig oder nur verzögert vom Prozessor verarbeitet werden können.

Interrupt-Verwaltung

Als es noch ISA-Steckkarten gab, mussten die Interrupts per Jumper konfiguriert werden. Später mit den PCI-Steckkarten konnten die Interrupts per Software eingestellt werden. Mit APIC kann das Betriebssystem die Interrupts eigenständig verwalten. Der Anwender muss an dieser Stelle keine Hand mehr anlegen. Mit der vollautomatischen Interrupt-Verwaltung durch APIC und dem Betriebssystem wurde dem PC-Bastler eine der lästigsten Aufgaben abgenommen, die es jemals gab.

Was bedeutet Plug and Play

Plug and Play (englisch für „einstecken und abspielen“ oder „anschließen und loslegen“), auch Plug & Play und Plug-and-play (kurz PnP) genannt, ist ein Begriff aus dem Gebiet der Rechnertechnik, mit dem man die Eigenschaft eines Computers beschreibt, neue Geräte – meist Peripheriegeräte – anschließen zu können, ohne anschließend Gerätetreiber zu installieren oder Einstellungen vornehmen zu müssen.

Weitere Details

Es gibt verschiedene Bezeichnungen und Variationen des Begriffs, die ähnliche Eigenschaften beschreiben, etwa Hot-Plug. Der Begriff Plug and Play wird normalerweise mit dem Unternehmen Microsoft in Verbindung gebracht, dass diese Bezeichnung zuerst für sein Produkt Windows 95 gebrauchte.
Plug and Play funktioniert nur, wenn es sowohl von Hardware als auch von Software unterstützt wird. Die Hardware erstellt normalerweise einen Identifizierungscode, damit die Software das Gerät korrekt erkennen kann. Der inzwischen durch USB abgelöste Apple Desktop Bus (ADB) verwendete für diesen Zweck einen Code aus vier Bits, die meisten Systeme benutzen inzwischen längere Codes verschiedener Art, um mehr Informationen wie Gerätenamen oder Seriennummern übertragen zu können.
Auf der Hardwareseite ist erforderlich, dass der Computerbus Änderungen der Konfiguration erkennen muss, wenn Geräte hinzugefügt oder entfernt werden. Mit der Einführung von moderneren Systemen – insbesondere USB und FireWire – wurde gerade diese Fähigkeit in die Computerbustechnologie eingeführt.
Schließlich muss das Betriebssystem in der Lage sein, mit den Änderungen beim An- oder Abstecken von Geräten umzugehen. Das bedeutet, dass es einen Interrupt des Systembusses auslöst, der die Änderungen anzeigt, um dann festzustellen, was verändert wurde. Bei älteren Busdesigns mussten alle

Systeminformationen ausgelesen werden, um herauszufinden, was sich verändert hat. Bei Verwendung mehrerer Geräte kann das eine verhältnismäßig lange Zeit in Anspruch nehmen. Moderne Systeme werden daher so entwickelt, dass die Suche nach Änderungen möglichst wenig Zeit benötigt. Im Fall von USB wird dafür (sowie für andere Zwecke) ein Hub-System eingesetzt.
Wenn eine Änderung der Konfiguration festgestellt wird, liest das Betriebssystem die Informationen, die das neue Gerät zur Verfügung stellt, um es zu identifizieren. Als Nächstes muss es im laufenden Betrieb die für das Gerät notwendigen Treiber laden, sofern das noch nicht erfolgt ist.

BIOS: Die 4 Hauptfunktionen (Beschreibung):

Die 4 Hauptfunktionen des BIOS:

POST:

Der POST testet und initialisiert die Komponenten der System-Hardware (CPU, DMA-Controller, Tastatur-Controller, Interrupt Controller)
Dann werden auch die Peripheriegeräte (Tastatur, Laufwerk, etc.) in den Test einbezogen

SETUP:

Ist ein meist menüfähiges Programm zur Systemkonfiguration.
Konfiguration von:
Hauptplatine (Overclocking)
Chipsatz (Grafik OnBoard)
Uhrzeit und Datum
Laufwerken (Bootreihenfolge)

URLOADER:

Die Laufwerke werden nach einem gültigen Master-Bootsektor (MBR) durchsucht, der dann geladen und ausgeführt wird.

SYSTEM BIOS:

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.

UEFI

Unified Extensible Firmware Interface (UEFI) ist ein Softwareprogramm, das die Firmware eines Computers mit seinem Betriebssystem (OS) verbindet. UEFI wird das Basic Input/Output System (BIOS) ablösen, ist aber damit kompatibel.
UEFI funktioniert über eine spezielle Firmware, die auf der Hauptplatine eines Computers installiert ist. Wie das BIOS wird UEFI vom Hersteller installiert und ist das erste Programm, das beim Booten eines Computers startet. Es prüft, welche Hardwarekomponenten angeschlossen sind, weckt die Komponenten auf und übergibt sie an das Betriebssystem. UEFI umgeht mehrere Probleme, die es mit BIOS noch gab, beispielsweise die Größe der Festplattenpartition, um BIOS zu betreiben.
Die meisten Computer unterstützten lange sowohl BIOS als auch UEFI. Seit 2020 wurden aber so gut wie alle neuen Produkte auf UEFI umgestellt.

Was macht UEFI?

UEFI bezeichnet die neue Methode, mit der Betriebssysteme und Plattform-Firmware kommunizieren, und bietet eine leichtgewichtige Alternative zum BIOS, die nur die Informationen verwendet, da Betriebssystem für den Start braucht. Darüber hinaus bietet UEFI verbesserte Computersicherheitsfunktionen.
UEFI enthält plattformbezogene Datentabellen und Boot- und Laufzeitdienstaufrufe für den OS-Loader. Zusammengenommen definieren diese Informationen die Schnittstellen und Strukturen, damit UEFI auf der Hard- und Firmware laufen kann. UEFI ist programmierbar, sodass Entwickler von Originalgeräteherstellern Anwendungen und Treiber hinzufügen können.
UEFI ist also die aktuelle Technologie und BIOS wird allmählich obsolet. Aus Gewohnheit sagen jedoch viele IT-Profis BIOS oder UEFI-BIOS, wenn sie eigentlich UEFI meinen.

Der Boot-Vorgang: BIOS versus UEFI

Das Einschalten eines Computers startet eine Kette von Aktionen, noch bevor das Betriebssystem startet. Die Firmware veranlasst das Subsystem des Computers dazu, eine Reihe von Tests auszuführen, und lokalisiert den Bootloader, der wiederum den Betriebssystemkern startet.
BIOS und UEFI verwenden beide Low-Level-Software, um Startfunktionen vor dem Booten eines Betriebssystems zu verwalten; sie setzen dafür aber unterschiedliche Technologien ein.
Das BIOS befindet sich auf einem Chip auf der Hauptplatine des Geräts und initialisiert die Zentraleinheit, den Direktzugriffsspeicher, die Peripheral-Component-Interconnect-Express-Karten sowie die Netzwerkgeräte. Das BIOS führt eine Diagnosesequenz für den Power-On Self-Test (POST) aus. POST stellt sicher, dass die Hardware ordnungsgemäß konfiguriert ist und alle Komponenten wie vorgesehen funktionieren.
Das BIOS wird nur im 16-Bit-Prozessormodus ausgeführt. Das deckelt die Zahl der durchführbaren Softwarebefehle. Das BIOS weist 1 Megabyte Speicher für das Ausführen von Aufgaben zu. Schnittstellen und Geräte werden somit sequentiell initialisiert – das verlangsamt den Startvorgang.
Das BIOS schickt eine Anfrage an den Master Boot Record (MBR), um das Betriebssystem zu finden und den Bootloader zu starten. MBR verwendet 32-Bit-Werte, um den Offset und die Länge einer Partition zu beschreiben. BIOS-Systeme können daher nur mit Laufwerken mit 2 Terabyte (TB) und nicht mehr als vier Partitionen arbeiten.
UEFI verhält sich hingegen wie ein Mini-Betriebssystem, das sich zwischen Firmware und Betriebssystem befindet. Es führt die gleichen Diagnosen wie das BIOS beim Start durch, bietet aber mehr Flexibilität. UEFI speichert Initialisierungsdaten als EFI-Dateipartition in nichtflüchtigem Flash-Speicher, statt in der Firmware. UEFI kann auch während des Bootens von einem Laufwerk oder über eine Netzwerkfreigabe geladen werden. UEFI stellt auch ein flexibleres Partitionierungsschema als MBR bereit, bekannt als Globally Unique Identifier Partition Table oder GPT. GPT wurde ebenfalls von Intel als Teil von EFI erstellt. GPT verwendet 64-Bit-Werte, um bis zu 128 Partitionen zu unterstützen sowie Laufwerke mit 2 TB und mehr. Die EFI-Partition verwendet die Dateizuordnungstabelle, einschließlich FAT16, FAT32 oder virtuelles FAT.

Vorteile von UEFI

UEFI bietet viele bedeutende Verbesserungen gegenüber dem BIOS, einschließlich der folgenden:
Boot-Modus. Benutzer von Microsoft Windows haben die Wahl zwischen 32-Bit-UEFI oder 64-Bit-UEFI. Experten empfehlen, dass der Betriebssystem-Bitmodus und der Firmware-Bitmodus zusammenpassen sollten, um Kommunikationsprobleme während der Laufzeit zu vermeiden.
Laufwerke. Laut dem UEFI-Forum unterstützt UEFI Boot-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 Nur-Lese-Speicher (Read Only Memory, ROM) 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 einn Bootloader zulässt, können Benutzer mit UEFI Loader für Debian-basierte Ubuntu- und andere Linux-Varianten zusammen mit Windows-OS-Loadern 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 für Windows 8 oder neuere Windows-Versionen. 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.

UEFI-Nachteile – wann man vom BIOS booten sollte

Software ist immer ein Ziel für Bedrohungen – da ist auch UEFI keine Ausnahme. Ein solcher Angriff namens TrickBot tauchte im Dezember 2020 auf. TrickBot-Malware funktioniert, indem sie versucht, die Gerätefirmware auszuspionieren, so dass Angreifer den Startvorgang unterlaufen und Zugriff auf das Betriebssystem erhalten konnten.
Die TrickBot-Episode folgte den eine Veröffentlichung von ESET Research aus dem Jahr 2018, einem slowakischen Outlet für die Informationssicherheits-Community, das behauptete, ein Rootkit in freier Wildbahn entdeckt zu haben, mit dem Hacker UEFI-Firmware überwachen und bösartigen Code installieren.
Abgesehen von Sicherheitsproblemen, gehört zu UEFI auch, dass es manchmal teurer ist. Ja, es fährt schneller hoch. Dieser Vorteil amortisiert sich aber nicht auf älteren Systemen, deren Hardware man für UEFI erst einmal aufrüsten müsste.
Ein weiterer potenzieller Nachteil ist die Abhängigkeit vom FAT-Dateisystem. Größere Laufwerkspartitionen können einen großen System-Overhead hinzufügen, der die Leistungsvorteile wieder auffrisst. In dem Fall ist es sinnvoller, weiter BIOS zu benutzen, insbesondere für einen Computer, der eine ältere Betriebssystemversion und kleinere Festplatten verwendet.