Betriebsmodi des Prozessors

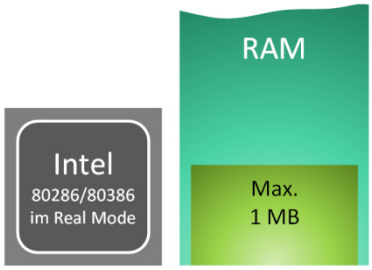
Allgemeines zu den Prozessor-Betriebsmodi

Seit der Entwicklung des 80286-Prozessors bieten die neueren Prozessortypen wesentlich mehr Möglichkeiten, als in der Regel genutzt werden. Eine wesentliche Rolle spielt hierbei das Betriebssystem DOS. DOS wurde für die 8086/88-CPU entwickelt und verschließt sich bis heute den wesentlichen Möglichkeiten der aktuellen Prozessoren.

Hauptsächlich war bei Intel mit der Vorstellung des 80286-Prozessors daran gedacht worden, in die Welt des Multitaskings einzusteigen. Die neuen Prozessortypen mussten in der Lage sein, einen 8086/88-Prozessor zu emulieren. Die Lösung war, die neueren Prozessortypen in verschiedene Betriebsmodi zu schalten.

Der Real (Address) Mode

Ein Prozessor der Klasse 80286 und höher verhält sich im Real Mode wie eine 8086/88-CPU. Die neueren Prozessoren sind aber gegenüber der 8086/88-CPU wesentlich leistungsfähiger und schneller. Für das Betriebssystem DOS macht es aber keinen Unterschied, ob es mit einem 8086/88 arbeitet oder mit einem höheren Prozessortyp.



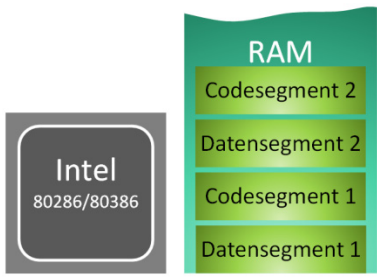
Der Real Mode

Nach dem Bootvorgang arbeitet ein Prozessor der Klasse 80286 und höher stets zuerst im Real Mode. Erst durch einen speziellen Programmbefehl wird der Prozessor in den erweiterten Modus (Protected Mode) geschaltet. Dies geschieht bei aktuellen Betriebssystemen schon ganz früh im Bootvorgang. Danach wird der Real Mode nicht mehr aktiviert.

Die größten Nachteile eines im Real Mode betriebenen Prozessors sind der nicht vorhandene Schutz der Programme voreinander (s. u.) sowie die Begrenzung des adressierbaren Speichers auf 1 MB, da in diesem Modus nur 20 Adressleitungen genutzt werden.

Der Protected (Virtual Address) Mode

Die erste neue Betriebsart, die mit dem 80286-Prozessor möglich wurde, ist der Protected Mode. Der Prozessor kann durch einen Maschinenbefehl umgeschaltet werden und verhält sich dann gänzlich anders als im Real Mode. Die 1-MB-RAM-Grenze und die feste Einteilung des Hauptspeichers sind aufgehoben.



Der Protected Mode

Alle wichtigen Daten können somit irgendwo im zur Verfügung stehenden Hauptspeicher abgelegt werden. Diese Tatsache birgt allerdings gewisse Risiken in sich. Es muss dafür gesorgt werden, dass die Daten im RAM nicht von einem anderen Programm plötzlich überschrieben werden. Zu diesem Zweck wurden Schutzmechanismen eingebaut, die dafür sorgen, dass die Daten auch wieder aufgefunden und vor allem nicht versehentlich überschrieben werden (Protection – Schutz).

Der Protected Mode bietet im Einzelnen folgende Schutzmechanismen:

Überwachung mittels Privilegstufen

Die Daten jedes laufenden Programms werden aufgeteilt in einen Bereich für den Programmcode, das Codesegment, und einen Bereich für die zu bearbeitenden Daten, das Datensegment. Diesen Code- bzw. Datensegmenten wird eine Privilegstufe von 0 bis 3 zugeordnet. Je niedriger die Privilegstufe ist, desto geschützter ist ein Programm bzw. sind dessen Daten.

Sollte ein Programm, dem die Privilegstufe 3 zugeteilt wurde, versuchen, auf ein Segment zuzugreifen, das durch die Privilegstufe 0 geschützt ist, erkennt der Prozessor eine Fehlersituation und meldet dies über einen Interrupt dem Betriebssystem. Dieses entscheidet, welche Aktionen erforderlich sind, und beendet in den meisten Fällen das fehlerhafte Programm.

Speicherbereichsschutz

Der Protected Mode ist für ein Multitasking-Betriebssystem ausgelegt. Demnach muss jedem laufenden Programm ein eigener, privater Speicherbereich zur Verfügung gestellt werden. Will ein Programm auf einen bestimmten Speicherplatz zugreifen, kann die CPU feststellen, ob dieser Speicherplatz zum privaten Bereich des Programms gehört.

Ist dies nicht der Fall, wird wiederum über einen Interrupt dem Betriebssystem dieser fehlerhafte Zugriff mitgeteilt und von diesem entsprechend behandelt; und gegebenenfalls wird das fehlerhafte Programm beendet.

Speichersegmentattribute

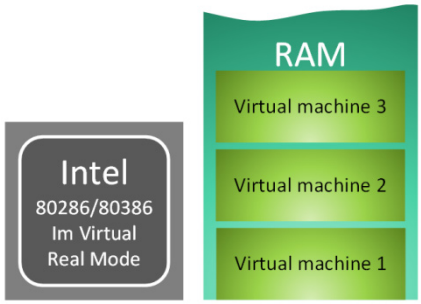
Verwendet ein Betriebssystem den Prozessor im Protected Mode, können an die Code- und Datensegmente bestimmte Attribute vergeben werden. Einem Segment kann z. B. das Attribut „nur Lesen“ zugeordnet werden. Sollte ein laufendes Programm versuchen, in ein solches „schreibgeschütztes“ Segment zu schreiben, wird wiederum über einen Interrupt die Kontrolle dem Betriebssystem übergeben.

Grundsätzlich erhält jedes Speichersegment ein Attribut, das es als Codesegment oder Datensegment kennzeichnet. Sollte versucht werden, ein Datensegment auszuführen oder ein Codesegment zu verändern, bedeutet dies wiederum eine Verletzung der Schutzmechanismen.

Der Virtual Real Mode

Ein weiterer Betriebsmodus für Intel-Prozessoren der 80386-Reihe, ist der virtuelle Real Mode. Dieser ist in der Lage mehrere 8086/88-CPUs nachzuahmen (emulieren).

In jedem emulierten Prozessor, kann ein Programm unabhängig von anderen ausgeführt werden. Ältere Windows-Betriebssysteme verwendeten diesen Modus, wenn sie DOS-Anwendungen ausführten. Heutige Betriebssysteme benutzen diesen Modus nicht mehr, sondern verwenden per Software emulierte virtuelle DOS-Maschinen. Diese eignen sich besser, da im Virtual Real Mode zwar mehrere Programme gestartet, jedoch nur das aktive Programm ausgeführt werden kann.



Der Virtual Real Mode