第 3 章　计算机体系结构及物理安全

3.1　计算机系统组成

3.1.1　图灵模型

1936 年，阿兰·图灵提出了一种抽象的计算模型——图灵机（Turing Machine），见图 3-1。图灵的基本思想是用机器来模拟人们用纸笔进行数学运算的过程，他把这样的过程构造出一台假想的机器，该机器由以下几个部分组成。

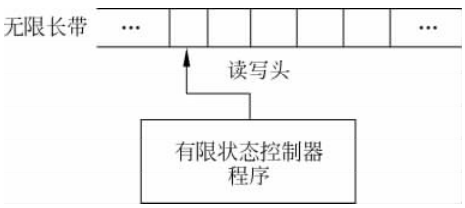

图 3-1　图灵模型

（1）一条无限长的纸带（Tape）。纸带被划分为一个接一个的小格子，每个格子上包含一个来自有限字母表的符号，字母表中有一个特殊的符号，表示空白。纸带上的格子从左到右依次被编号为 0，1，2，…，纸带的右端可以无限伸展。

（2）一个读写头（Head）。该读写头可以在纸带上左右移动，它能读出当前所指格子上的符号，并能改变当前格子上的符号。

（3）一套控制规则（Table）。它根据当前机器所处的状态以及当前读写头所指格子上的符号来确定读写头下一步的动作，并改变状态寄存器的值，令机器进入一个新的状态。

（4）一个状态寄存器。它用来保存图灵机当前所处的状态。图灵机的所有可能状态的数目是有限的，并且有一个特殊的状态，称为停机状态。

这个机器的每一部分都是有限的，但它有一个潜在的无限长的纸带，因此这种机器只是一个理想的设备。图灵认为，这样的一台机器就能模拟人类所能进行的任何计算过程。

3.1.2　冯·诺依曼模型

20 世纪 30 年代中期，美籍科学家冯·诺依曼大胆地提出：抛弃十进制，采用二进制作为数字计算机的数制基础。同时，他还说预先编制计算程序，然后由计算机来按照人们事前制定的计算顺序来进行数值计算工作。人们把冯·诺依曼的这个理论称为冯·诺依曼体系结构，也称为普林斯顿体系结构。从 ENIAC 到当前最先进的计算机都采用的是冯·诺依

曼体系结构。所以冯·诺依曼是当之无愧的“电子计算机之父”。

冯·诺依曼结构处理器具有以下几个特点：①必须有一个存储器；②必须有一个控制器；③必须有一个运算器，用于完成算术运算和逻辑运算；④必须有输入设备和输出设备，用于进行人机通信。另外，程序和数据统一存储并在程序控制下自动工作。

为了完成上述功能，计算机必须具备五大基本组成部件，包括：输入数据和程序的输入设备；记忆程序和数据的存储器；完成数据加工处理的运算器；控制程序执行的控制器；输出处理结果的输出设备。

3.1.3　计算机系统组成

计算机系统包括硬件系统和软件系统两大部分。硬件是指组成计算机的各种物理设备，由五大功能部件组成，即运算器、控制器、存储器、输入设备和输出设备，如图 3-2 所示。这五大部分相互配合，协同工作。

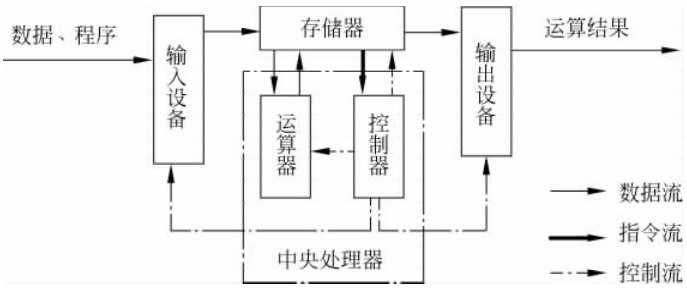

图 3-2　五大功能部件

其工作原理为：首先由输入设备接收外界信息(程序和数据)，控制器发出指令将数据送入(内)存储器，然后向内存储器发出取指令命令。在取指令命令下，程序指令逐条送入控制器。控制器对指令进行译码，并根据指令的操作要求向存储器和运算器发出存数、取数命令和运算命令，经过运算器计算并把计算结果存储在存储器内。最后在控制器发出的取数和输出命令的作用下，通过输出设备输出计算结果。

3.1.4　微型计算机结构

1. 主机

主机指计算机用于放置主板及其他主要部件的容器(Mainframe)，通常包括 CPU、内存、硬盘、光驱、电源以及其他输入输出控制器和接口，如 USB 控制器、显卡、网卡、声卡等。位于主机箱内的部件通常称为内设，而位于主机箱之外的部件通常称为外设(如显示器、键盘、鼠标、外接硬盘、外接光驱等)，见图 3-3。

计算机主机的组成部分如下。

(1) 机箱，装主机配件的箱子，没有机箱不影响使用。

(2) 电源，主机供电系统，没有电源不能使用。

(3) 主板，连接主机各个配件的主体，没有主板主机不能使用。

(4) CPU，主机的心脏，负责数据运算。不可缺少，属于重要设备。

图 3-3 计算机主机

(5) 内存,存储主机调用文件,不可缺少。

(6) 硬盘,主机的存储器,独立主机不可缺少。

(7) 声卡,某些主板集成。

(8) 显卡,某些主板集成,显示器控制。

(9) 网卡,某些主板集成,没有网卡计算机无法访问网络,是联络其他主机的渠道。

(10) 光驱,没有光驱,主机无法读取光碟上的文件。

(11) 一些不常用设备,如视频采集卡、电视卡、SCSI 卡等。

2. 外设

外部设备简称“外设”,是指连在计算机主机以外的硬件设备。对数据和信息起着传输、转送和存储的作用,是计算机系统中的重要组成部分。按照功能的不同,大致可以分为输入设备、显示设备、打印设备等,见图 3-4。

图 3-4 外部设备

(1) 键盘、鼠标,是人或外部与计算机进行交互的一种装置,用于把原始数据和处理这些数据的程序输入到计算机中。

(2) 显示器,是计算机的输出设备之一,它可以显示操作和计算结果。目前计算机显示设备主要有 CRT 显示器、LCD 显示、等离子显示器和投影机。

(3) 打印机,也是计算机的输出设备之一,它将计算机的运算结果或中间结果以人所能识别的数字、字母、符号和图形等,依照规定的格式印在纸上的设备。

3.2　计算机组成原理

3.2.1　系统总线

1. 系统总线概述

系统总线，又称内总线或板级总线，是用来连接微机各功能部件而构成一个完整微机系统。系统总线上传送的信息包括数据信息、地址信息、控制信息。因此，系统总线包含有3种不同功能的总线，即数据总线(Data Bus，DB)、地址总线(Address Bus，AB)和控制总线(Control Bus，CB)，见图 3-5。

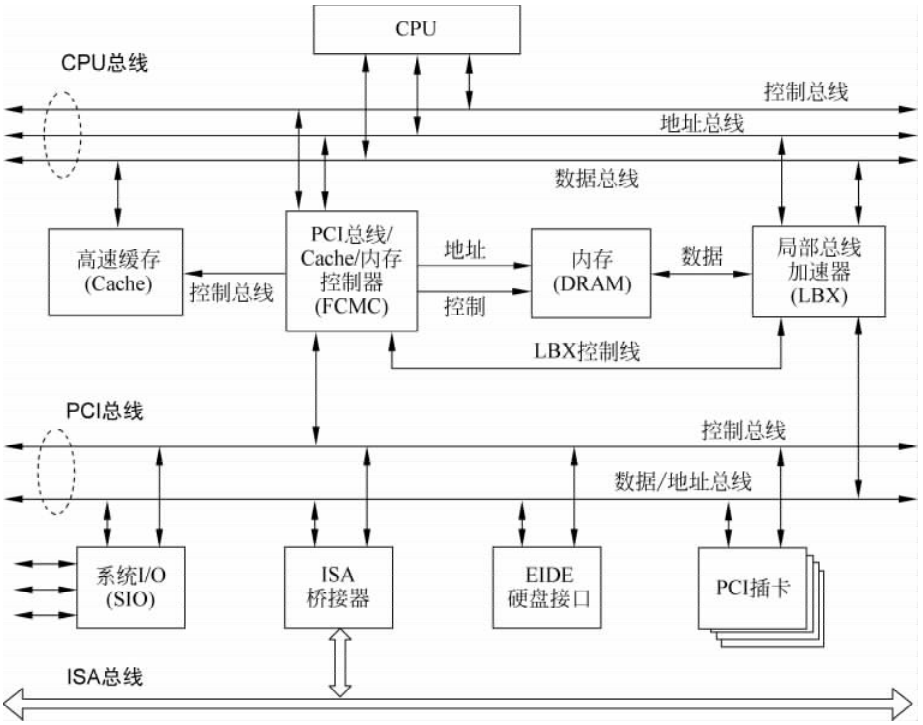

图 3-5　系统总线

2. 工作原理

CPU 通过系统总线对存储器的内容进行读、写，同样通过总线，实现将 CPU 内数据写入外设或由外设读入 CPU。总线就是用来传送信息的一组通信线。微型计算机通过系统总线将各部件连接到一起，实现了微型计算机内部各部件间的信息交换。一般情况下，CPU 提供的信号需经过总线形成电路形成系统总线。系统总线按照传递信息的功能来分，可分为地址总线、数据总线和控制总线。这些总线提供了微处理器(CPU)与存储器、输入输出接口部件的连接线。可以认为，一台微型计算机就是以 CPU 为核心，其他部件全“挂接”在与 CPU 相连接的系统总线上。

3. 功能分类

(1) 数据总线 DB。用于传送数据信息。数据总线是双向三态形式的总线,既可以把 CPU 的数据传送到存储器或输入输出接口等其他部件,也可以将其他部件的数据传送到 CPU。数据总线的位数是微型计算机的一个重要指标,通常与微处理器的字长相一致。例如,Intel 8086 微处理器字长 16 位,其数据总线宽度也是 16 位。需要指出的是,数据的含义是广义的,它可以是真正的数据,也可以指令代码或状态信息,有时甚至是一个控制信息,因此,在实际工作中数据总线上传送的并不一定仅仅是真正意义上的数据。

(2) 地址总线 AB。它是专门用来传送地址的,由于地址只能从 CPU 传向外部存储器或输入输出端口,所以地址总线总是单向三态的,这与数据总线不同。地址总线的位数决定了 CPU 可直接寻址的内存空间大小,比如 8 位微机的地址总线为 16 位,则其最大可寻址空间为 $2^{16}=64$KB,16 位微型机的地址总线为 20 位,其可寻址空间为 $2^{20}=1$MB。

(3) 控制总线 CB。用来传送控制信号和时序信号。控制信号中,有的是微处理器送往存储器和输入输出接口电路的,如读/写信号、片选信号、中断响应信号等;也有的是其他部件反馈给 CPU 的,如中断申请信号、复位信号、总线请求信号、设备就绪信号等。因此,控制总线的传送方向由具体控制信号而定,一般是双向的,控制总线的位数要根据系统的实际控制需要而定。实际上,控制总线的具体情况主要取决于 CPU。

3.2.2 CPU

1. CPU 定义

中央处理器(Central Processing Unit,CPU)是一台计算机的运算核心和控制核心。CPU、内部存储器和输入输出设备是电子计算机三大核心部件。其功能主要是解释计算机指令以及处理计算机软件中的数据。CPU 由运算器、控制器和寄存器及实现它们之间联系的数据、控制及状态的总线构成。几乎所有的 CPU 的运作原理可分为 4 个阶段,即提取(Fetch)、解码(Decode)、执行(Execute)和写回(Writeback)。CPU 从存储器或高速缓冲存储器中取出指令,放入指令寄存器,并对指令译码、执行指令。计算机的可编程性主要是指对 CPU 的编程。

2. 工作原理

CPU 从存储器或高速缓冲存储器中取出指令,放入指令寄存器,并对指令译码。它把指令分解成一系列的微操作,然后发出各种控制命令,执行微操作系列,从而完成一条指令的执行。指令是计算机规定执行操作的类型和操作数的基本命令。指令是由一个字节或者多个字节组成,其中包括操作码字段、一个或多个有关操作数地址的字段以及一些表征机器状态的状态字和特征码。有的指令中也直接包含操作数本身。

3. 基本结构

CPU 包括运算逻辑部件、寄存器部件和控制部件,见图 3-6。

(1) 运算逻辑部件,可以执行定点或浮点的算术运算操作、移位操作及逻辑操作,也可执行地址的运算和转换。

(2) 寄存器部件,包括通用寄存器、专用寄存器和控制寄存器。

(3) 控制部件,主要负责对指令译码,并且发出为完成每条指令所要执行的各个操作的控制信号。

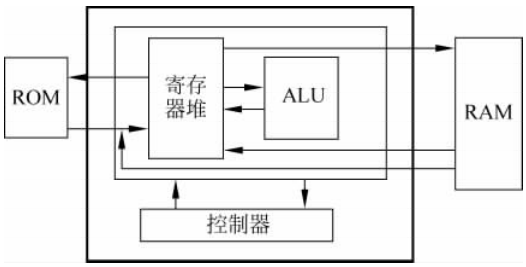

图 3-6　CPU 结构

3.2.3　存储器

1. 存储器概述

存储器(Memory)是计算机系统中的记忆设备,用来存放程序和数据。计算机中全部信息,包括输入的原始数据、计算机程序、中间运行结果和最终运行结果都保存在存储器中。它根据控制器指定的位置存入和取出信息。有了存储器,计算机才有记忆功能,才能保证正常工作。按用途存储器可分为主存储器(内存)和辅助存储器(外存),也有分为外部存储器和内部存储器的分类方法。外存通常是磁性介质或光盘等,能长期保存信息。内存指主板上的存储部件,用来存放当前正在执行的数据和程序,但仅用于暂时存放程序和数据,关闭电源或断电数据会丢失。

2. 存储器的构成

构成存储器的存储介质,目前主要采用半导体器件和磁性材料。存储器中最小的存储单位就是一个双稳态半导体电路或一个 CMOS 晶体管或磁性材料的存储元,它可存储一个二进制代码。由若干个存储元组成一个存储单元,然后再由许多存储单元组成一个存储器。一个存储器包含许多存储单元,每个存储单元可存放一个字节(按字节编址)。每个存储单元的位置都有一个编号,即地址,一般用十六进制表示。一个存储器中所有存储单元可存放数据的总和称为存储容量。假设一个存储器的地址码由 20 位二进制数(即 5 位十六进制数)组成,则可表示为 2^{20},即 1M 个存储单元地址。每个存储单元存放一个字节,则该存储器的存储容量为 1MB。

存储器的主要功能是存储程序和各种数据,并能在计算机运行过程中高速、自动地完成程序或数据的存取。存储器是具有“记忆”功能的设备,它采用具有两种稳定状态的物理器件来存储信息。这些器件也称为记忆元件。在计算机中采用只有两个数码(“0”和“1”)的二进制来表示数据。记忆元件的两种稳定状态分别表示为“0”和“1”。日常使用的十进制数必须转换成等值的二进制数才能存入存储器中。计算机中处理的各种字符,如英文字母、运算符号等,也要转换成二进制代码才能存储和操作。

3. 存储器用途

根据存储器在计算机系统中的作用,可分为主存储器、辅助存储器、高速缓冲存储器、控制存储器等。为了解决对存储器要求容量大、速度快、成本低三者之间的矛盾,目前通常采用多级存储器体系结构,即使用高速缓冲存储器、主存储器和外存储器,见图 3-7。

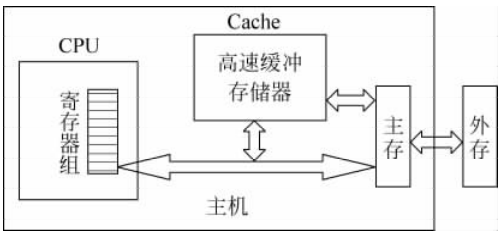

图 3-7 多级存储器体系结构

高速缓存：高速存取指令和数据存取速度快，但存储容量小。

主存储器：内存存放计算机运行期间的程序和数据，其存取速度快，存储容量不大。

外存储器：外存存放系统程序和大型数据文件及数据库，存储容量大，成本低。

按照与 CPU 的接近程度，存储器分为内存储器与外存储器，简称内存与外存。内存储器又常称为主存储器（简称主存），属于主机的组成部分；外存储器又常称为辅助存储器（简称辅存），属于外部设备。CPU 不能像访问内存那样直接访问外存，外存要与 CPU 或 I/O 设备进行数据传输，必须通过内存进行。在 80386 以上的高档微机中，还配置了高速缓冲存储器（Cache），这时内存包括主存与高速缓存两部分。对于低档微机，主存即为内存。

4. 常用存储器

（1）硬盘，是计算机主要的存储介质之一，由一个或者多个铝制或者玻璃制的碟片组成。这些碟片外覆盖有铁磁性材料。绝大多数硬盘都是固定硬盘，被永久性地密封固定在硬盘驱动器中。其物理结构为：磁头是读写合一的电磁感应式磁头；磁道是当磁盘旋转时，磁头若保持在一个位置上，则每个磁头都会在磁盘表面划出一个圆形轨迹；扇区是磁盘上的每个磁道被等分为若干个弧段，每个扇区可以存放 512B 的信息，磁盘驱动器在向磁盘读取和写入数据时以扇区为单位；每个盘面都被划分为数目相等的磁道，并从外缘的“0”开始编号，具有相同编号的磁道形成一个圆柱，即磁盘柱面。

（2）光盘，以光信息作为存储物的载体，用来存储数据，采用聚焦的氢离子激光束处理记录介质的方法存储和再生信息。激光光盘分不可擦写光盘（如 CD-ROM、DVD-ROM 等）和可擦写光盘（如 CD-RW、DVD-RAM 等）。高密度光盘（Compact Disc）是近代发展起来不同于磁性载体的光学存储介质。常见的 CD 光盘非常薄，只有 1.2mm 厚，分为 5 层，包括基板、记录层、反射层、保护层、印刷层等。

（3）U 盘，全称“USB 闪存盘”，英文名“USB flash disk”。它是一个 USB 接口的无需物理驱动器的微型高容量移动存储产品，可以通过 USB 接口与计算机连接，实现即插即用。使用 USB 接口连到计算机的主机后，U 盘的资料可与计算机交换。U 盘最大的优点就是小巧便于携带、存储容量大、价格便宜、性能可靠。U 盘容量有 1GB、2GB、4GB、8GB、16GB、32GB、64GB 等。

（4）ROM，是只读内存（Read-Only Memory）的简称，是一种只能读出事先所存数据的固态半导体存储器。其特性是一旦储存资料就无法再将之改变或删除。通常用在不需经常变更资料的电子或计算机系统中，资料不会因为电源关闭而消失。

（5）RAM（随机存取存储器，Random Access Memory），其存储单元的内容可按需随意取出或存入，且存取的速度与存储单元的位置无关的存储器。这种存储器在断电时将丢失

其存储内容，故主要用于存储短时间使用的程序。按照存储信息的不同，随机存储器又分为静态随机存储器（Static RAM，SRAM）和动态随机存储器（Dynamic RAM，DRAM）。

3.2.4　输入输出系统

1. 输入输出系统控制方式

1）程序查询方式

这种方式是在程序控制下由 CPU 与外设之间交换数据。CPU 通过 I/O 指令询问指定外设当前的状态，如果外设准备就绪，则进行数据的输入或输出；否则 CPU 等待，循环查询。

程序查询方式是一种程序直接控制方式，这是主机与外设间进行信息交换的最简单方式，输入和输出完全是通过 CPU 执行程序来完成的。一旦某一外设被选中并启动后，主机将查询这个外设的某些状态位，看其是否准备就绪？若外设未准备就绪，主机将再次查询；若外设已准备就绪，则执行一次 I/O 操作。

这种方式控制简单，但外设和主机不能同时工作，各外设之间也不能同时工作，系统效率很低。因此，仅适用于外设的数目不多，对 I/O 处理的实时要求不高，CPU 的操作任务比较单一且并不很忙的情况。

这种方式的优点是结构简单，只需要少量的硬件电路即可；缺点是由于 CPU 的速度远远高于外设，因此通常处于等待状态，工作效率很低。

2）中断方式

中断是主机在执行程序过程中，遇到突发事件而中断程序的正常执行，转去对突发事情的处理，待处理完成后返回源程序继续执行。中断过程如下：中断请求、中断响应、中断处理和中断返回。

计算机中有多个中断源，有可能在同一时刻有多个中断源向 CPU 发出中断请求，这种情况下 CPU 按中断源的中断优先级顺序进行中断响应。

中断处理方式的优点是显而易见的，它不但为 CPU 省去了查询外设状态和等待外设就绪所花费的时间，提高了 CPU 的工作效率，还满足了外设的实时性要求。缺点是对系统的性能要求较高。

3）直接存储器访问方式（DMA）

DMA 方式指高速外设与内存之间直接进行数据交换，不通过 CPU 并且 CPU 不参加数据交换的控制。工作过程如下：外设发出 DMA 请求，CPU 响应 DMA 请求，把总线让给 DMA 控制器，在 DMA 控制器的控制下通过总线实现外设与内存之间的数据交换，见图 3-8。DMA 最明显的一个特点是它不是用软件而是采用一个专门的控制器来控制内存与外设之间的数据交流，无须 CPU 介入，大大提高了 CPU 的工作效率。

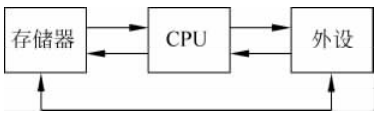

图 3-8　直接存储器访问方式

2. 输入输出设备

1）输入设备

常用的输入设备有键盘、鼠标、扫描仪等。

（1）键盘的分类。按键盘的键数分，键盘可分为 83 键、101 键盘、104 键盘、107 键盘等；

按键盘的形式分，键盘可分为有线键盘、无线键盘、带托键盘和 USB 键盘等。

（2）鼠标的分类。按照工作原理，鼠标可分为机械式鼠标、光电式鼠标两类。按鼠标的形式分，鼠标可分为有线鼠标和无线鼠标。

（3）扫描仪的分类。扫描仪通过光源照射到被扫描的材料上来获得材料的图像。扫描仪常用的有台式、手持式和滚筒式 3 种。分辨率是扫描仪很重要的特征，常见扫描仪的分辨率有 300×600、600×1200 等。

2）输出设备

常用的输出设备有显示器、打印机等。

（1）显示器。按使用的器件分类可分为阴极射线管显示器（CRT）、液晶显示器（LCD）和等离子显示器；按显示颜色可分为彩色显示器和单色显示器。显示器的主要性能指标有像素、分辨率、屏幕尺寸、点间距、灰度级、对比度、帧频、行频和扫描方式。

（2）打印机。打印机分为针式打印机、喷墨打印机、激光打印机、热敏打印机 4 种。

3）其他输入输出设备

包括数码相机 DC、数码摄像机 DV、手写笔、投影机、扫描仪、绘图仪等。

3. I/O 接口

1）接口的功能

使主机和外设能够按照各自的形式传输信息，见图 3-9。

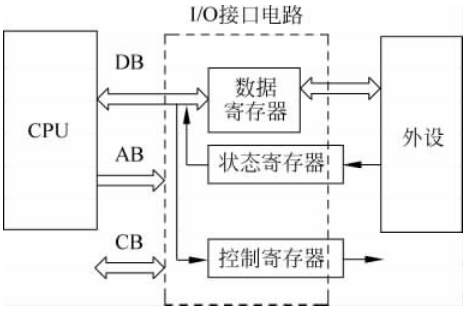

图 3-9 I/O 接口

2）几种接口

（1）显示卡：主机与显示器之间的接口。

（2）硬盘接口：IDE 接口、EIDE 接口、ULTRA 接口和 SCSI 接口等。

（3）串行接口：COM 端口，也称为串行通信接口。

（4）并行接口：是一种打印机并行接口标准。

3.3 物理与设备安全

3.3.1 物理安全概述

1. 物理安全的概念

物理安全是为保证信息系统的安全可靠运行，降低或阻止人为或自然因素从物理层面对信息系统保密性、完整性、可用性带来的安全威胁，从系统的角度采取的适当安全措施。

物理安全也称为实体安全，是系统安全的前提。硬件设备的安全性能直接决定了信息系统的保密性、完整性、可用性，信息系统所处物理环境的优劣直接影响信息系统的可靠性，系统自身的物理安全问题也会对信息系统的保密性、完整性、可用性带来安全威胁。

物理安全是以一定的方式运行在一些物理设备之上的，是保障物理设备安全的第一道防线。因为物理安全会导致系统存在风险。比如：环境事故造成的整个系统毁灭；电源故障造成的设备断电以至操作系统引导失败或数据库信息丢失；设备被盗、被毁造成数据丢失或信息泄露；电磁辐射可能造成数据信息被窃取或偷阅；报警系统的设计不足或失灵可能造成的事故等。

设备安全技术主要指保障构成信息网络的各种设备、网络线路、供电连接、各种媒体数据本身及其存储介质等安全的技术，主要包括设备的防盗、防电磁泄露、防电磁干扰等，是对可用性的要求。

物理环境安全是物理安全的最基本保障，是整个安全系统不可缺少和忽视的组成部分。环境安全技术主要是指保障信息网络所处环境安全的技术，主要技术规范是对场地和机房的约束，强调对于地震、水灾、火灾等自然灾害的预防措施，包括场地安全、防火、防水、防静电、防雷击、电磁防护、线路安全等。

2. 概念的理解

(1) 狭义物理安全。传统意义的物理安全包括设备安全、环境安全/设施安全以及介质安全。设备安全的技术要素包括设备的标志和标记、防止电磁信息泄露、抗电磁干扰、电源保护以及设备振动、碰撞、冲击适应性等方面。环境安全的技术要素包括机房场地选择、机房屏蔽、防火、防水、防雷、防鼠、防盗防毁、供配电系统、空调系统、综合布线、区域防护等方面。介质安全的安全技术要素包括介质自身安全以及介质数据安全。以上是狭义物理安全观，也是物理安全的最基本内容。

(2) 广义物理安全。广义的物理安全还应包括由软件、硬件、操作人员组成的整体信息系统的物理安全，即包括系统物理安全。信息系统安全体现在信息系统的保密性、完整性、可用性 3 个方面，从物理层面出发，系统物理安全技术应确保信息系统的保密性、可用性、完整性，如通过边界保护、配置管理、设备管理等等级保护措施保护信息系统的保密性，通过容错、故障恢复、系统灾难备份等措施确保信息系统可用性，通过设备访问控制、边界保护、设备及网络资源管理等措施确保信息系统的完整性。

3. 物理安全分类

(1) 信息系统物理安全。为了保证信息系统安全可靠地运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施(包括机房建筑、供电、空调)、环境人员、系统等采取适当的安全措施。

(2) 设备物理安全。为保证信息系统的安全可靠运行，降低或阻止人为或自然因素对硬件设备安全可靠运行带来的安全风险，对硬件设备及部件所采取的适当安全措施。

(3) 环境物理安全。为保证信息系统的安全可靠运行所提供的安全运行环境，使信息系统得到物理上的严密保护，从而降低或避免各种安全风险。

(4) 介质物理安全。为保证信息系统的安全可靠运行所提供的安全存储的介质，使信

息系统的数据得到物理上的保护,从而降低或避免数据存储的安全风险。

3.3.2 物理安全威胁与防范

物理安全威胁指物理设备及配套部件的安全威胁,而不是软件逻辑上的威胁。物理设备运行在某一个物理环境中。环境不好,对物理设备有威胁,自然会影响其运行效果。物理环境安全是物理安全的最基本保障,是整个安全系统不可缺少和忽视的组成部分。环境安全技术主要是保障物联网系统安全的相关技术。其技术规范是物联网系统运行环境内外(场地和机房)的约束。其环境分为自然环境威胁和人为干扰。自然环境威胁包括地震、水灾、火灾等自然灾害。人为干扰包括静电、雷击、电磁、线路破坏和盗窃等。

1) 自然环境威胁

(1) 地震。地震灾害具有突发性和不可预测性,并产生严重次生灾害,对机器设备会产生很大影响。但是,破坏性地震发生之前,人们对地震有没有防御,防御工作做得好坏将会大大影响到经济损失的大小和人员伤亡的多少。防御工作做得好,就可以有效地减轻地震的灾害损失。

(2) 水灾。水灾指洪水、暴雨、建筑物积水和漏雨等对设备造成的灾害。水灾不仅威胁人民生命安全,也会造成设备的巨大财产损失,并对物联网系统运行产生不良影响。对付水灾,可采取工程和非工程措施以减少或避免其危害和损失。

(3) 雷击。雷电会对人和建筑造成危害,而电磁脉冲主要影响电子设备,主要是受感应作用所致。雷击防范的主要措施是,根据电器、微电子设备的不同功能及不同受保护程序和所属保护层确定防护要点作分类保护;根据雷电和操作瞬间过电压危害的可能通道从电源线到数据通信线路都应做多层保护。

(4) 火灾。火灾是指在时间和空间上失去控制的燃烧所造成的灾害。在各种灾害中,火灾是最经常、最普遍地威胁公众安全和社会发展的主要灾害之一。机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。

2) 人为干扰威胁

(1) 盗窃。盗窃指以非法占有为目的,秘密窃取他人占有的数额较大的公私财物或者多次窃取公私财物的行为。物联网的很多设备和部件都价值不菲,这也是偷窃者的目标。因为偷窃行为所造成的损失可能远远超过其本身的价值,因此必须采取严格的防范措施,以确保计算机设备不会丢失。

(2) 人为损坏。人为损坏包括故意的和无意的设备损坏。无意的设备损坏多半是操作不当造成的;而有意破坏则是有预谋的破坏。这两种情况都存在。预防的方法是,对于重要的设备,要加强外部的物理保护,如专用间、围栏、保护外壳等。

(3) 静电。静电是由物体间的相互摩擦、接触而产生的。静电产生后,由于未能释放而保留在物体内,会有很高的电位(能量不大),从而产生静电放电火花,造成火灾。还可能使大规模集成电路损坏,这种损坏可能是不知不觉造成的。

(4) 电磁泄漏。电子设备工作时要产生电磁发射。电磁发射包括辐射发射和传导发射。这两种电磁发射可被高灵敏度的接收设备接收并进行分析、还原,造成计算机的信息泄露。屏蔽是防电磁泄漏的有效措施,屏蔽主要有电屏蔽、磁屏蔽和电磁屏蔽 3 种类型。

3.3.3　设备环境安全与防范

1. 机房环境安全

机房是各类信息设备的中枢，机房工程必须保证网络和计算机等高级设备能长期而可靠地运行。其质量的优劣直接关系到机房内整个信息系统是否能稳定、可靠地运行，是否能保证各类信息通信畅通无阻。机房的环境必须满足计算机等各种微机电子设备和工作人员对温度、湿度、洁净度、电磁场强度、噪声干扰、安全保安、防漏、电源质量、振动、防雷和接地等的要求。机房的物理环境受到了严格控制，主要包括温度、电源、地板、监控等几个方面。

(1) 温度。“数据处理环境热准则”建议温度为 20～25℃(68～75℉)，湿度为 40%～55%，适宜数据中心环境的最大露点温度是 17℃。在数据中心电源会加热空气，除非热量被排除出去；否则环境温度就会上升，导致电子设备失灵。通过控制空气温度，服务器组件能够保持制造商规定的温度/湿度范围内。空调系统通过冷却室内空气下降到露点帮助控制湿度，湿度太大，水可能在内部部件上开始凝结。如果在干燥的环境中，辅助加湿系统可以添加水蒸气，因为如果湿度太低，可能导致静电放电，会损坏元器件。

(2) 电源。机房电源由一个或多个不间断电源(UPS)和/或柴油发电机组成备用电源。对关键服务器来说，最好同时连接到两个电源，以实现 $N+1$ 冗余系统的可靠性。静态开关有时用来确保在发生电力故障时瞬间从一个电源切换到另一个电源。为了保证设备用电质量和用电安全，电源应至少有两路供电，并应有自动转换开关。当一路供电有问题时，可迅速切换到备用线路供电。应安装备用电源，如 UPS，停电后可供电 8h 或更长时间。关键设备应有备用发电机组和应急电源。同时为防止、限制瞬态过压和引导浪涌电流，应配备电涌保护器(过压保护器)。为防止保护器的老化、寿命终止或雷击时造成的短路，在电涌保护器的前端应有诸如熔断器等过电流保护装置。

(3) 地板。机房的地板相对瓷砖地板要提升 60cm，这个高度现在变得更高了，是 80～100cm，以提供更好的气流均匀分布。这样空调系统可以把冷空气也灌到地板下，同时也为地下电力线布线提供更充足的空间，现代数据中心的数据电缆通常是经由高架电缆盘铺设的，但仍然有些人建议出于安全考虑还是应将数据线铺设到地板下，并考虑增加冷却系统。小型数据中心里没有提升的地板可以不用防静电地板。计算机机柜往往被安装到一个热通道中，以便使空气流通效率最好。

(4) 监控报警。按照国家有关标准设计实施，机房应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警，以保护系统免受水、火、有害气体、地震、静电的危害。针对重要的机房或设备应采取防盗措施，如应用视频监视系统能对系统运行的外围环境、操作环境实施监控。电源管理排查干扰，包括排除电源线的中断、异常、电压瞬变、冲击、噪声、突然失效事件。

2. 机房安全设计

如果机房的防静电、防火防水、接地防雷、室内温湿度有保障，可有效提高机房的物理安全性。机房应该符合国家标准和国家有关规定。其中，D 级信息系统机房应符合《计算机场地安全要求》(GB 9361—88)的 B 类机房要求；B 级和 C 级信息系统机房应符合《计算机场

地安全要求》(GB 9361—88)的 A 类机房要求。机房建设最好进行以下设计：①机房装饰，包括抗静电地板铺设、棚顶墙体装修、天棚及地面防尘处理、门窗等；②供配电系统，包括供电系统、配电系统、照明、应急照明、UPS 电源；③空调新风系统，包括机房精密空调、新风换气系统；④消防报警系统，包括消防报警、手提式灭火器；⑤防盗报警系统，如红外报警系统；⑥防雷接地系统，包括电源防雷击抗浪涌保护、等电位连接、静电泄放等、接地系统；⑦安防系统，包括门禁、视频等；⑧机房动力环境监控系统。

3. 设备安全与策略

设备安全技术指保障构成信息网络的各种设备、网络线路、供电连接、各种媒体数据本身及其存储介质等安全的技术，主要包括设备的防盗、防电磁泄漏、防电磁干扰等，是对可用性的要求。

1) 设备安全问题

这里的设备指系统中的物理设备或一个子系统，不是指小的元器件。它指由集成电路、晶体管、电子管等电子元器件组成，应用电子技术(包括)软件发挥作用的设备等。设备安全主要是指设备被盗、设备被干扰、设备不能工作、人为损坏、设备过时等问题。

2) 设备安全策略

(1) 设备改造。它是对由于新技术出现，在经济上不宜继续使用的设备进行局部的更新，即对设备的第二种无形磨损的局部补偿。

(2) 设备更换。它是设备更新的重要形式，分为原型更新和技术更新。原型更新即简单更新，用结构相同的新设备更换因为严重有形磨损而在技术上不宜继续使用的旧设备。这种更换主要解决设备的损坏问题，不具有技术进步的性质。

(3) 技术更新。用技术上更先进的设备去更换技术陈旧的设备。它不仅能恢复原有设备的性能，而且使设备具有更先进的技术水平，具有技术进步的性质。

(4) 备份机制。即两台设备一起工作。也称双工，指两台或多台服务器均为活动，同时运行相同的应用，保证整体的性能，也实现了负载均衡和互为备份。双机双工模式是目前群集的一种形式。

(5) 监控报警。监控报警是安全报警与设备监控的有效融合。监控报警系统包括安全报警和设备监控两个部分。当设备出现问题时，监控报警系统可以迅速发现问题，并及时通知责任人进行故障处理。

4. 通信线路安全

1) 线路安全威胁

线路物理安全指为保证信息系统的安全可靠运行，降低或阻止人为或自然因素对通信线路的安全可靠运行带来的安全风险，对线路所采取的适当安全措施。线路的物理安全按不同的方法分类。比如，可以分为自然安全威胁和人为安全威胁，也可以分为线路端和线路间的安全威胁，还可以分为被破坏程度的安全威胁。线路的物理安全风险主要有：地震、水灾、火灾等自然环境事故带来的威胁；线路被盗、被毁、电磁干扰、线路信息被截获、电源故障等人为操作失误或错误。

2) 线路安全对策

通信线路的物理安全是网络系统安全的前提。由于通信线路属于弱电，耐压值很低。

因此，在其设计和施工中必须优先考虑保护线路和端口设备不受水灾、火灾、强电流、雷击的侵害。必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷。在布线时要考虑可能的火灾隐患，线路要铺设到一般人触摸不到的高度，而且要加装外保护盒或线槽，避免线路信息被窃听。要与照明电线、动力电线、暖气管道及冷热空气管道之间保持一定距离，避免被伤害或被电磁干扰。充分考虑线路的绝缘、线路的接地与焊接的安全。线路端的接口部分要加强外部保护，避免信息泄露或线路损坏。

思　考　题

3-1　简述图灵模型。

3-2　简述冯·诺依曼模型。

3-3　简述计算机系统组成。

3-4　简述微型计算机的结构。

3-5　有几种系统总线？它们的功能分别是什么？

3-6　CPU 由几个部分组成？

3-7　存储器怎么分类？

3-8　什么是物理安全？

3-9　物理安全有哪几方面的威胁？怎样防范？

3-10　设备环境安全有哪几方面的威胁？怎样防范？