第 5 章

信息系统的物理安全和可靠性

计算机硬件及其运行环境是计算机信息系统运行的基础，它们的安全直接影响着整个信息系统的安全。由于自然灾害、设备自身的缺陷、设备的自然损坏和受到环境干扰等自然因素，以及人为的窃取和破坏等原因，计算机设备和其中信息的安全面临很大的问题。本章主要讨论从物理层面增强信息系统安全的方法。

5.1 节给出了物理安全的定义，指出了狭义和广义物理安全包含范畴的不同，明确本章讲述的物理安全包括环境安全、设备安全、媒体(介质)安全、系统安全；5.2 节～5.4 节分别介绍了环境安全、设备安全和媒体(介质)安全；5.5 节介绍了系统安全，可靠性是评价系统安全的重要指标，指出提高系统可靠性一般采取避错、容错和容灾备份技术；5.6 节介绍了隔离网络安全防护技术；5.7 节、5.8 节分别介绍了容错和灾难恢复技术。

视频讲解

5.1 物理安全概述

根据国家标准 GB/T 21052—2007《信息安全技术 信息系统物理安全技术要求》，物理安全是指为了保证信息系统安全可靠运行，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、空调等)、环境人员、系统等采取适当的安全措施。

物理安全是计算机网络信息系统运行的基础，直接影响着计算机信息系统的安全。以下是计算机系统物理安全遭到破坏的一个典型的例子。

2006 年 12 月 26 日晚 8 时 26 分至 40 分，我国台湾屏东外海发生地震。大陆出口光缆、中美海缆、亚太 1 号等至少 6 条海底通信光缆发生中断，造成我国大陆至台湾地区、美国、欧洲的通信线路大量中断，互联网大面积瘫痪，除我国外，日本、韩国、新加坡网民均受到影响。

传统意义的物理安全包括设备安全、环境安全以及介质安全，涉及的安全技术解决了由于设备/设施/介质的硬件条件所引发的信息系统物理安全威胁问题，从系统的角度看，这一层面的物理安全是狭义的物理安全，是物理安全的最基本内容。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。

本章讨论的物理安全包括环境安全、设备安全、介质安全、系统安全四方面。

1. 环境安全

环境安全是指为保证信息系统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。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。

2. 设备安全

设备安全是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,其技术要素包括设备的防盗、防电磁泄露、电源保护以及设备振动、碰撞、冲击适应性等方面。

3. 介质安全

介质安全是指存储信息的介质的安全,能够安全保管、防盗、防损坏和防霉。

4. 系统安全

系统安全是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,如通过边界保护、配置管理、设备管理等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。

5.2 环境安全

5.2.1 环境安全面临的威胁

计算机的运行环境对计算机的影响非常大,影响计算机运行的环境因素主要有温度、湿度、灰尘、腐蚀、电磁干扰等,这些因素从不同侧面影响计算机的可靠工作。

1. 温度

无论是台式计算机还是笔记本,计算机元器件如CPU、主板、显卡、声卡、网卡都是封闭在机箱内的,计算机在工作的时候,机箱内部温度很高,所以计算机都配备有风扇和散热设备,但是如果计算机持续工作或外部环境过高,计算机元器件的温度会过高,即使有散热设备也无法保证计算机处于正常工作的温度范围。计算机正常工作的温度范围是0～45℃。当环境温度超过60℃时,计算机系统就不能正常工作,温度每升高10℃,电子元器件的可靠性就会降低25%。元器件可靠性降低会直接影响计算机的正确运算,从而影响计算结果的正确性。

另外,温度对磁介质的磁导率影响很大,磁盘表面的磁介质具有热胀冷缩的特性,如果温度过高或过低,磁盘表面会发生变形,从而造成数据的读写错误;温度过高还会使插头、插座、计算机主板、各种信号线腐蚀速度加快,容易造成接触不良;温度过高也对显示器造成不良的影响,会使显示器各线圈骨架尺寸发生变化,使图像质量下降。

总之,环境温度过高或过低都容易引起硬件损坏,计算机工作的环境温度一般应控制在20℃左右。

2. 湿度

如果环境相对湿度低于40%,环境比较干燥;如果高于60%,则比较潮湿。湿度过高或过低对计算机的可靠运行都有影响。

湿度过大会使元器件的表面附着一层很薄的水膜，造成元器件各引脚之间的漏电。当水膜中含有杂质时，它们会附着在元器件引脚、导线、接头表面，造成这些表面发霉和触点腐蚀。磁性介质是多孔材料，在相对湿度高的情况下，它就会吸收空气中的水分变潮，使其磁导率发生明显变化，造成磁介质上的信息读写错误。

湿度过低则意味着环境比较干燥，过于干燥就很容易产生静电。在环境非常干燥的情况下去触摸元器件，会造成元器件的损害。除此之外，过于干燥的空气还可能会造成磁介质上的信息被破坏、纸张变脆、印制电路板变形等危害。

计算机正常的工作湿度应该控制在40%～60%。

3．灰尘

空气中的灰尘对计算机中的精密机械装置，如磁盘、光盘驱动器影响很大。磁盘机、光盘机的读头与盘片之间的距离很小，不到1μm，在高速旋转过程中，各种灰尘包括纤维性灰尘会附着在盘片表面，当读头靠近盘片表面读信号的时候，就可能擦伤盘片表面或者磨损读头，造成数据读写错误或数据丢失。灰尘中还可能有导电性和腐蚀性尘埃，附着在元器件与电子线路的表面，在湿度很大的情况下，会造成短路或腐蚀裸露的金属表面。因此需要对进入机房的空气进行过滤，并采取严格的机房卫生制度，降低机房灰尘的含量。

4．电气和电磁干扰

电气和电磁干扰是指电网电压和计算机内外的电磁场引起的干扰。常见的电气干扰是指电压瞬间较大幅度的变化、突发的尖脉冲或电压不足甚至掉电。例如，机房内使用较大功率的吸尘器、电钻，机房外使用电锯、电焊机等大用电量设备，这些情况都容易在附近的计算机电源中产生电气噪声信号干扰。这些干扰一般容易破坏信息的完整性，有时还会损坏计算机设备。

对计算机正常运行影响较大的电磁干扰是静电干扰和周边环境的强电磁干扰。计算机中的芯片大部分是MOS器件，静电电压过高会破坏这些MOS器件，据统计，50%以上的计算机设备的损害直接或间接与静电有关。防静电的主要方法有：机房应该按防静电要求装修(如使用防静电地板)，整个机房应该有一个独立且良好的接地系统，机房中各种电器和用电设备都接在统一的地线上。周边环境的强电磁干扰主要是指无线电发射装置、微波线路、高压线路、电气化铁路、大型电机、高频设备等产生的强电磁干扰。这些强电磁干扰轻则会使计算机工作不稳定，重则会对计算机造成损坏。

5．停电

电子设备是计算机信息系统的物理载体，停电会使得电子设备停止工作，从而破坏信息系统的可用性，因此供电事故已经成为当前信息系统安全的一大威胁。

例如2015年，雷击造成比利时电网停电，谷歌设在当地的数据中心也暂时断电，尽管大部分服务器都利用备用电池和冗余电量维系短期用电，但还是造成了几十GB的数据丢失。还有黑客攻击电力基础设施的事件，例如，在2015年年底和2016年年初，乌克兰境内的多处变电站遭受黑客恶意软件攻击，直接导致乌克兰国内大范围停电，约140万家庭无电可用。

5.2.2 环境安全防护

为规范电子信息系统机房设计,确保电子信息系统设备安全、稳定、可靠地运行,GB 50174—2008《电子信息系统机房设计规范》(以下简称《规范》)对机房分级与性能要求、机房位置与设备布置、环境要求、建筑与结构、空气调节、电气、电磁屏蔽、机房布线、机房监控与安全防范、给水排水、消防等方面提出了具体要求。

1. 机房安全等级

计算机系统中的各种数据依据其重要性和保密性,可以划分为不同等级,需要提供不同级别的保护。对于高等级数据采取低水平的保护会造成不应有的损失,对不重要的信息提供多余的保护,又会造成不应有的浪费。因此,应对计算机机房规定不同的安全等级。《规范》将电子信息系统机房划分为A、B、C三级,设计时应根据机房的使用性质、管理要求及其在经济和社会中的重要性确定所属级别。

符合下列情况之一的电子信息系统机房应为A级。

(1) 电子信息系统运行中断将造成重大的经济损失。

(2) 电子信息系统运行中断将造成公共场所秩序严重混乱。

例如,国家气象台、国家级信息中心、重要的军事指挥部门、大中城市的机场、广播电台、电视台等的电子信息系统机房和重要的控制室应为A级。

符合下列情况之一的电子信息系统机房应为B级。

(1) 电子信息系统运行中断将造成较大的经济损失。

(2) 电子信息系统运行中断将造成公共场所秩序混乱。

例如,科研院所、高等院校、三级医院、大中城市的气象台、省部级以上政府办公楼、大型工矿企业等的电子信息系统机房和重要的控制室应为B级。

不属于A级或B级的电子信息系统机房为C级。

A级电子信息系统机房内的场地设施应按容错系统配置,在电子信息系统运行期间,场地设施不应因操作失误、设备故障、外电源中断、维护和检修而导致电子信息系统运行中断。容错系统是具有两套或两套以上相同配置的系统,在同一时刻,至少有两套系统在工作。按容错系统配置的场地设备,至少能经受住一次严重的突发设备故障或人为操作失误事件而不影响系统的运行。

B级电子信息系统机房内的场地设施应按冗余要求配置,在系统运行期间,场地设施在冗余能力范围内,不应因设备故障而导致电子信息系统运行中断。冗余系统是重复配置系统的一些部件或全部部件,当系统发生故障时,冗余配置的部件介入并承担故障部件的工作,由此减少系统的故障时间。

C级电子信息系统机房内的场地设施应按基本需求配置,在场地设施正常运行情况下,应保证电子信息系统运行不中断。

2. 机房位置及设备布置要求

1) 机房位置选择

电子信息系统机房位置选择应符合下列要求。

(1) 电力供给应稳定可靠,交通、通信应便捷,自然环境应清洁。

(2) 应远离产生粉尘、油烟、有害气体以及生产或储存具有腐蚀性、易燃、易爆物品的场所。

（3）远离水灾、火灾隐患区域。

（4）远离强振源和强噪声源。

（5）避开强电磁场干扰。

对于多层或高层建筑物内的电子信息系统机房，在确定主机房的位置时，应对设备运输、管线敷设、雷电感应和结构荷载等问题进行综合考虑和经济比较；采用机房专用空调的主机房，应具备安装室外机的建筑条件。

2）机房组成

电子信息系统机房的组成应根据系统运行特点及设备具体要求确定，一般宜由主机房、辅助区、支持区和行政管理区等功能区组成。

主机房的使用面积应根据电子信息设备的数量、外形尺寸和布置方式确定，并预留今后业务发展需要的使用面积。辅助区的面积宜为主机房面积的0.2～1倍。用户工作室可按每人3.5～4m^2计算。硬件及软件人员办公室等有人长期工作的房间，可按每人5～7m^2计算。

3）设备布置

电子信息系统机房的设备布置应满足机房管理、人员操作和安全、设备和物料运输、设备散热、安装和维护的要求。

产生尘埃及废物的设备应远离对尘埃敏感的设备，并宜布置在有隔断的单独区域内。

当机柜或机架上的设备为前进风/后出风方式冷却时，机柜和机架的布置宜采用面对面和背对背的方式。

主机房内和设备间的距离应符合下列规定。

（1）用于搬运设备的通道净宽不应小于1.5m。

（2）面对面布置的机柜或机架正面之间的距离不应小于1.2m。

（3）背对背布置的机柜或机架背面之间的距离不应小于1m。

（4）当需要在机柜侧面维修测试时，机柜与机柜、机柜与墙之间的距离不应小于1.2m。

（5）成行排列的机柜，其长度超过6m时，两端应设有出口通道；当两个出口通道之间的距离超过15m时，在两个出口通道之间还应增加出口通道；出口通道的宽度不应小于1m，局部可为0.8m。

3. 机房的环境条件

1）温度、湿度及空气含尘浓度

主机房和辅助区内的温度、相对湿度应满足电子信息设备的使用要求；无特殊要求时，应根据电子信息系统机房的等级，按照如表5.1所示要求执行。

表5.1　机房温度、相对湿度要求

项　　目	技术要求			备注
	A级	B级	C级	
主机房温度（开机时）	23℃±1℃		18～28℃	不得结露
主机房相对湿度（开机时）	40%～55%		35%～75%	
主机房温度（停机时）	5～35℃			

续表

项　　目	技术要求			备注
	A级	B级	C级	
主机房相对湿度(停机时)	40%～70%		20%～80%	不得结露
主机房和辅助区温度变化率(开、停机时)	＜5℃/h		＜10℃/h	
辅助区温度、相对湿度(开机时)	18～28℃、35%～75%			
辅助区温度、相对湿度温度(停机时)	5～35℃、20%～80%			
不间断电源系统电池室温度	15～25℃			

A级和B级主机房的含尘浓度,在静态条件下测试,每升空气中大于或等于0.5μm的尘粒数应少于18 000粒。

对于重要的系统机房,应安装吹尘、吸尘设备,排除进入人员所带的灰尘。空调系统进风口应安装空气滤清器,并应定期清洁和更换过滤材料,以防灰尘进入,同时进风压力要大,房间要密封,使室内空气压力高于室外,防止室外灰尘进入室内。

2) 噪声、电磁干扰、振动及静电

有人值守的主机房和辅助区,在电子信息设备停机时,在主操作员位置测量的噪声值应小于65dB(A)。

主机房内无线电干扰场强,在频率为0.15～1000MHz时,主机房和辅助区内的无线电干扰场强不应大于126dB。

主机房和辅助区内磁场干扰环境场强不应大于800A/m。

在电子信息设备停机条件下,主机房地板表面垂直及水平向的振动加速度值,不应大于500mm/s^2。

主机房和辅助区的绝缘体的静电电位不应大于1kV。

机房场地环境要求更详细的内容,可以参阅GB 50174—2008《电子信息系统机房设计规范》。

视频讲解

5.3 设备安全

5.3.1 设备安全面临的威胁

1. 计算机硬件容易被盗

纵观PC的发展历史,微型化、移动化是其发展趋势。人们最早使用的是CRT显示器和较大的机箱,设备非常笨重,目前CRT显示器已经被液晶显示器取代;便携式计算机、以iPad为代表的智能移动终端的出现给人们的工作和娱乐带来了方便。PC朝着体积越来越小,越来越便携的方向发展,给人们带来便利的同时也带来了容易被盗窃的风险。目前,PC的机箱一般都设计成便于用户打开的,有的甚至连螺钉旋具也不需要,而便携式计算机、智能移动终端整个机器都能够很容易被搬走,其中数据的安全就更谈不上了。

2. 电磁泄露

电磁泄露是指电子设备的杂散(寄生)电磁能量通过导线或空间向外扩散,使用专门的接收设备将这些电磁辐射接收下来,经过处理,就可以恢复还原出原信息,如图 5.1 所示。任何处于工作状态的电磁信息设备如主机、磁盘、显示器、打印机等工作时都会产生不同程度的电磁泄露,尤其是显示器,由于显示的信息是给人阅读的,不加任何保密措施,因此其产生的辐射是最容易造成泄密的。随着信息技术设备处理速度的不断提高,电磁发射的强度也不断增强,对信息设备安全的威胁也就越大。

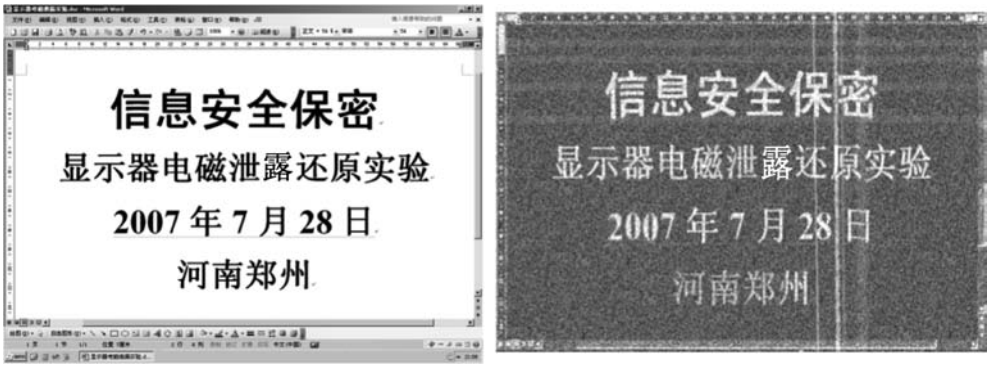

图 5.1　电磁泄露的还原效果

计算机及其外部设备的信息可以通过两种方式泄露出去。一种是以电磁波的形式辐射出去,称为辐射泄露。经实际仪器测试,在距离计算机几百米以外的距离可以根据接收到的电磁波复现显示器上显示的信息,计算机屏幕上的信息在其所有者毫不知晓的情况下泄露出去。1985 年,在法国召开的“计算机与通信”国际会议上,荷兰的一位工程师 Winvan Eck 公开了他窃取微机信息的技术。他用价值仅几百美元的器件对普通电视机进行改造,然后装在汽车里,从楼下的街道接收到了放置在 8 层楼上的计算机电磁泄露的信息,并显示出计算机屏幕上显示的图像。另一种是通过各种线路和金属管传导出去的,称为传导泄露。例如,计算机的电源线、机房内的电话线、上(下)水管道和暖气管道、地线等都可能作为传导介质。这些金属导体有时也起着天线作用,将传导的信号辐射出去。在这些泄露源中,最大量和最基本的辐射源是载流导线。美国曾于 20 世纪 70 年代在苏联领海纵深内部的鄂霍次克海 120m 深的海底军事通信电缆上安装了 6m 长的窃听设备,记录了所有经过电缆的通信信号,由于没有采取任何加密措施,大量的军事情报便轻而易举地落在了美国人的手里。

理论分析和实际测量表明,影响计算机电磁辐射强度的因素如下。

(1) 功率和频率。设备的功率越大,则辐射强度越大。信号频率越高,则辐射强度越大。

(2) 距离因素。在其他条件相同的情况下,离辐射源越近,则辐射强度就越大;离辐射源越远,则辐射强度越小。也就是说,辐射强度与距离成反比。

(3) 屏蔽状况。辐射源是否屏蔽,屏蔽情况的好坏,对辐射强度的影响都很大。

3. 电气与电磁干扰

电气干扰是指电网电压引起的干扰,常见的电气干扰是指电压瞬间较大幅度的变化、突发的尖脉冲或电压不足甚至掉电。例如,机房内使用较大功率的吸尘器、电钻,机房外使用电锯、电焊机等大用电量设备,这些情况都容易在附近的计算机电源中产生电气噪声信号干扰。这些干扰一般容易破坏信息的完整性,有时还会损坏计算机设备。防止电气干扰的办法是采用稳压电源或不间断电源,为了防止突发的电源尖脉冲,对电源还要增加滤波和隔离措施。

电磁干扰是指经辐射或传导的电磁能量对设备或信号传输造成的不良影响。过去人们往往认为计算机是具有逻辑特征的数字系统,受电磁干扰的影响不大,但随着微电子技术的发展,计算机已朝高速度、高灵敏度、高集成度的方向发展,使得系统的抗电磁干扰度降低。比较常见的一种现象就是,站在电视机前或计算机前使用手机时,计算机中会出现波形,这就是电磁干扰。

一方面,计算机本身会产生电磁干扰。计算机中的元器件长期使用后其性能会衰减,它们的性能参数往往会偏离理论值,加之工作环境温度不稳定,引起电子线路、设备或系统内部元器件参数改变,从而使元器件存在不同程度的噪声干扰;每个元器件和每根导线上均流过一定大小的电流,因此其周围都会形成一定大小的磁场。当计算机电路中的元器件或线路布局不合理,电路间耦合不良时,就会在导线间产生分布电容或电感,寄生耦合便通过它们耦合进计算机,使信号畸变出错;如果信号线阻抗与负载阻抗不完全匹配,脉冲信号就会在传输线中产生反射现象,使信号波形产生瞬时冲击,造成电路逻辑故障。计算机插件印制板金属化孔通导不良,印制线粗细不均匀,都会产生信号反射干扰;计算机中的高频电路不仅会产生时序信号,还会产生辐射干扰。计算机内部产生的电磁干扰不但会造成计算机本身的工作异常,而且还可能造成计算机数据信息的失密和失窃。

另一方面,计算机外部的设备也会产生电磁干扰。计算机工作在一段很宽的工作频率范围内,它基本上与工业、科技、医学高频设备、广播、电视、通信、雷达等射频设备的工作频段相同,致使计算机工作在一个相当复杂的电磁环境中,容易受这些设备干扰。如果计算机房内使用较大功率的吸尘器、电钻,机房外使用电锯、电焊机等大用电量设备,这些设备的使用会对计算机信号造成干扰,甚至会造成传输信息的丢失,计算机设备的破坏。来自大自然的雷电、大气放电、地球热辐射的干扰会产生随机电流,轻则增加电噪声干扰,使计算机信息出错,重则使计算机元器件击穿,使计算机设备损坏;静电危害是计算机、半导体器件的“大敌”,是造成微机半导体损坏的基本原因。有研究指出,当穿塑料鞋走动,穿尼龙或丝绸工作服在工作台前长期工作时都可能产生很高的静电电压,不仅会使磁记录破坏,还会使计算机设备外壳产生静电感应。

因此,外部电磁环境的干扰和系统内部的互相干扰,严重威胁着计算机系统工作的稳定性和可靠性。

5.3.2 设备安全防护

设备安全防护包括设备的防盗、防止电磁泄露、抗电磁干扰、电源保护等。

1. 设备防盗

设备防盗就是利用一定的防盗手段保护计算机信息系统的设备和部件，以提高计算机信息系统设备和部件的安全性。早期的防盗主要采取增加质量或胶黏的方法，使设备长久固定或黏接在一个固定点。虽然增加了安全性，但对于移动和调整位置十分不便。之后，又出现了将设备和固定盘用锁连接，打开锁才能搬运设备的方法。常见的锁有机箱锁扣、Kensington 锁孔、机箱电磁锁等。

机箱锁扣实现方式非常简单。在机箱上固定一个带孔的金属片，然后在机箱侧板上打一个孔，当侧板安装在机箱上时，金属片刚好穿过锁孔，此时用户在锁孔上加装一把锁就实现了防护功能。这种锁实现起来比较简单，造价低，但防护强度有限，安全系数低。

Kensington 锁孔是由美国的 Kensington 公司发明，因此而得名。Kensington 锁孔需要配合 Kensington 线缆锁来实现防护功能。使用时将钢缆的一头固定在桌子或其他固定装置上，另一头将锁头固定在机箱上的 Kensington 锁孔内，就实现了防护功能。其特点是固定方式灵活，对于一些开在机箱侧板上的 Kensington 锁孔，不仅可以锁定机箱侧板，而且钢缆还能防止机箱被人挪动或搬走。

机箱电磁锁主要应用于高端商用 PC 产品上，实现方式是将电磁锁安装在机箱内，嵌入在 BIOS 中的子系统通过密码实现电磁锁的开关管理。这种防护方式更加安全和美观，也是一种人性化的安全防护方式，如图 5.2 所示。

图 5.2　机箱电磁锁

另外还有一种使用光纤电缆保护设备的方法，这种方法是将光纤电缆连接到每台重要的设备上，光束沿光纤传输，如果通道受阻，则报警。这种保护装置比较简单，一套装置可以保护机房内所有的重要设备，并且设备还可以随意移动、搬运。

一种更方便的方法是使用智能网络传感设备。将传感设备安放在机箱边缘，当机箱盖被打开时，传感开关自动复位，此时传感开关通过控制芯片和相关程序，将此次开箱事件自动记录到 BIOS 中或通过网络及时传给网络设备管理中心，实现集中管理。智能网络传感设备是一种创新的防护方式，但对电源和网络的依赖性大。如果在关掉电源和切断网络的情况下打开机箱，则传感器是无法捕获到的。

另外，安装视频监视系统也是必不可少的，视频监视系统是一种更为可靠的防护设备，能对系统运行的外围环境、操作环境实施监控。对重要的机房，还应采取特别的防盗措施，如值班守卫，出入口安装金属防护装置保护安全门、窗户。

2. 防电磁泄露

计算机是一种非常复杂的机电一体化设备，工作在高速脉冲状态的计算机就像是一

台很好的小型无线电发射机和接收机,不但产生电磁辐射泄露保密信息,而且还可以引入电磁干扰影响系统正常工作。尤其是在微电子技术和卫星通信技术飞速发展的今天,计算机电磁辐射泄密的危险越来越大。国际上把信息辐射泄露技术简称为 TEMPEST (Transient ElectroMagnetic Pulse Emanations Standard Technology,瞬时电磁脉冲发射标准技术),这种技术主要研究与解决计算机和外部设备工作时因电磁辐射和传导产生的信息外漏问题,具体研究内容包括:电子设备辐射的途径与方式、对电子信息设备辐射泄露如何防护、如何从辐射信息中提取有用信息、信息辐射的测试技术与测试标准。

计算机设备的防泄露措施主要有屏蔽技术、使用干扰器、滤波技术、采用低辐射设备、隔离和合理布局等。

1) 屏蔽技术

屏蔽是 TEMPEST 技术中的一项基础措施。屏蔽最典型的例子就是电梯,电梯提供了一个屏蔽的环境,屏蔽的效果是在电梯中手机接收不到信号了。根据不同的需要屏蔽方法包括整体屏蔽、设备屏蔽和元器件屏蔽。整体屏蔽的方法是采用金属网把需要保护的房间屏蔽起来,为了保证良好的屏蔽效果,金属网接地要良好,并且要经过严格的测试验收。整体屏蔽技术适用于需要处理高度保密信息的场合,如军、政首脑机关的信息中心和驻外使馆等地方,应该将信息中心的机房整个屏蔽起来。整体屏蔽的费用比较高,出于对成本的控制和保密性要求的降低,也可以将设备屏蔽,把需要屏蔽的计算机和外部设备放在体积较小的屏蔽箱内,该屏蔽箱要很好地接地,对于从屏蔽箱内引出的导线也要套上金属屏蔽网。对于电子线路中的局部元器件如 CPU、内存条等强辐射部件可采用屏蔽盒进行屏蔽。

2) 使用干扰器

干扰器是一种能辐射电磁噪声的电子仪器,它通过增加电磁噪声降低辐射泄露信息的总体信噪比,从而增大辐射信息被截获后破解还原的难度,达到“掩盖”真实信息的目的。具体的方法是将一台能产生噪声的干扰器放置在计算机设备的旁边,干扰器产生的噪声与计算机设备产生的信息辐射一起向外泄露。

干扰技术可分为白噪声干扰技术和相关干扰技术两种。白噪声干扰技术的原理是使用白噪声干扰器发出强于计算机电磁辐射信号的白噪声,起到阻碍和干扰接收的作用。这种方法有一定的作用,但由于要靠掩盖的方式进行干扰,发射的功率又必须足够强,所以会造成控件的电磁污染,而白噪声干扰也容易被接收方使用较为简单的方法进行滤除或抑制解调接收。相关干扰技术的原理是使用相关干扰器发出能自动跟踪计算机电磁辐射信号的相关干扰信号,使电磁辐射信号被扰乱,起到乱数加密的效果,使接收方即使接收到电磁辐射信号也无法调节出信号锁携带的真实信息,如图 5.3 所示。相对于白噪声干扰技术,相关干扰技术对环境的电磁污染较小,且使用简单,效果显著,比较适合于单独工作的个人计算机上。

3) 滤波技术

滤波能非常有效地减少和抑制电磁泄露,是抑制传导泄露的主要方法之一。主要方法是在信号传输线、公共接地线及电源线上加装滤波器。

图 5.3　相关干扰器

4）采用低辐射设备

低辐射设备是指在设计和生产计算机设备时，就对可能产生电磁辐射的元器件、集成电路、连接线、显示器等采取了防辐射措施，把电磁辐射抑制到最低限度。由于制造低辐射设备所使用的材料成本较高，它的造价也比较昂贵。使用低辐射计算机设备是防止计算机电磁辐射泄露的较为根本的防护措施。

5）隔离和合理布局

隔离是将信息系统中需要重点防护的设备从系统中分离出来，加以特别防护，并切断其与系统中其他设备间的电磁泄露通路。合理布局是指合理放置信息系统中的关键设备，并尽量拉大涉密设备与非安全区域的距离。让计算机房远离可能被侦测的地点，这是因为计算机辐射的距离有一定限制，超过 300m，即使攻击者接收到辐射信号也很难还原。对于一个单位而言，计算机房尽量建在单位辖区的中央地区而不是边缘地区。若一个单位辖区的半径小于 300m，距离防护的效果就有限。

对计算机与外部设备究竟要采取哪些防泄露措施，要根据计算机中的信息的重要程度而定。对于企业而言，需要考虑这些信息的经济效益，在选择保密措施时，不应该花费 100 万元去保护价值 10 万元的信息，对于军队则需要考虑这些信息的保密级别。

3. 防电磁干扰

防制计算机受到电磁干扰的主要手段有接地、屏蔽、滤波。

1）接地

良好的接地系统，一是可以消除各电路之间流经公共阻抗时所产生的公共抗阻干扰和雷击，避免计算机电路受磁场和电位差的影响，二是可保证设备及人身安全。理想的接地面为零电位，各接地点之间无电位差。在接地设计时，应注意交流地、直流地、防雷地和安全地的接地线要分开，不要互连，复杂电路要采用多点接地和公共地等。

2）屏蔽

电磁屏蔽是对两个空间区域之间进行金属的隔离，以控制电场、磁场和电磁波由一个区域到另一个区域的感应和辐射。具体地讲，就是用屏蔽体将元部件、电路、电缆或整个系统的干扰源包围起来，防止干扰电磁场向外扩散；用屏蔽体将接收电路、设备或系统包围起来，防止它们受到外界电磁场的影响。在计算机工程中，凡是受到电磁场干扰的地方都可以用屏蔽的方法来削弱干扰，以确保计算机正常运行。

屏蔽材料通常采用高导电性的材料,如铜板、铜箔、铝板、铝箔、钢板或金属镀层、导电涂层。由于电磁干扰无孔不入,因此屏蔽体上应尽量少留开口,还可以根据需要采取不同的金属材料组成的多层屏蔽体。

3) 滤波

滤波是抑制和防止干扰的一项重要措施。在一定的频带内,滤波器衰减很小,电能很容易通过,而在此频带外衰减则很大,能有效抑制传输。应在计算机的线路板上采取适当的滤波措施,防止外部的电磁干扰,同时又能使脉冲信号的高频成分大大减少,从而使线路板的辐射得到改善。

视频讲解

5.4 媒体(介质)安全

5.4.1 媒体安全面临的威胁

常见的信息存储媒体有磁盘、光盘、U盘、移动硬盘、打印纸等,这些媒体上存储了大量有用信息甚至机密信息,是各类黑客或攻击者进行盗窃、破坏和篡改的目标。光盘、U盘、移动硬盘、打印纸等体积小、易携带,成为最容易造成信息泄露的设备,下面首先讨论硬盘面临的安全威胁。

硬盘面临的安全威胁如下。

(1) 目前PC的硬盘是很容易安装和拆卸的,导致硬盘容易被盗。

(2) 硬盘上的文件几乎没有任何保密措施,如果硬盘被盗了,那么硬盘上的文件、信息、办公秘密、商业机密也就暴露无遗。目前比较常用的办公软件Word可以通过设置保护密码和限制访问进行文件保护,但为了办公方便,使用得极少,而且在强大的破译软件面前,这种密码保护根本不堪一击。

(3) 文件删除操作留下的隐患。文件的删除操作是人们经常执行的操作,系统在执行删除操作时,数据是否在磁盘上不存在了呢? 实际上,文件删除操作仅在文件目录中做了一个标记,并没有删除文件本身数据存储区,数据仍然残留在磁盘上,直到新的数据覆盖,如图5.4所示。这段时间内信息泄露的可能性比较大。

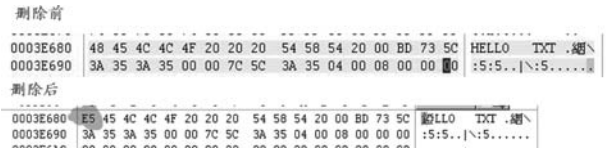

图5.4 文件删除前后磁盘存储区的变化

(4) 硬盘本身的脆弱性。磁盘本身很容易被划坏或被各种硬物碰伤或受潮霉变,硬盘上的数据也随之而变得无法读取。

媒体面临的安全威胁还来自管理方面的缺陷,在媒体的使用和管理上存在如下4方面的缺陷。

(1) 缺乏对媒体的管理和维护能力,一旦存储有重要、敏感信息的媒体发生故障,只

能销毁或冒着泄密的重大危险到固定维修点甚至国外去维修。

(2) 对存储有敏感信息的媒体没有专门的存放场所,而是和一般办公文件一起存放,造成一旦办公场所发生火灾等突发危险时,媒体随之而遭殃。

(3) 缺乏对媒体的分类和拷贝限制。没有根据媒体的重要程度进行分类存放,且对媒体中信息的拷贝流程没有严加管理,信息拷贝几乎人手一份,所以媒体中的信息也毫无秘密可言。

(4) 缺乏媒体的管理办法。没有形成对媒体分类存放和拷贝管理方法,以及相应的复制登记制度、媒体处理和销毁制度。

5.4.2　媒体安全防护

媒体的安全防护应从加强磁盘安全保密控制和加强媒体安全管理两方面入手。

1. 加强磁盘安全保密控制

可以通过磁盘加密技术和磁盘信息清除技术加强对磁盘及其存储信息的安全保护。

磁盘加密技术是指使用加密工具对存储在磁盘上的信息进行加密,即使存储信息被第三方窃取或复制,也很难读懂,从而保证信息不被泄露。具体的磁盘信息加密技术还可细分为文件加密、目录加密、数据库加密和整盘数据加密。具体应用可视磁盘信息的保密强度要求而定。

磁盘清除技术可以分为直流消磁法和交流消磁法两种。直流消磁法是使用直流磁头将磁盘上原先记录信息的剩余磁通全部以一种形式的恒定值来代替。通常,完全格式化方式格式化磁盘就是这种方法。交流消磁法是使用交流磁头将磁盘上原先所记录信息的剩余磁通变得极小,这种方法的消磁效果比直流消磁法的效果要好,消磁后磁盘上的残留信息强度可比消磁前下降 90dB。

2. 加强媒体安全管理

(1) 设置管理人员对媒体进行专门管理。一方面所有对存储媒体的访问应当由管理员统一进行管理,另一方面管理员要负责所有媒体的接收和发出,并做好相应的核准和记录工作。

(2) 做好媒体的归档工作。任何媒体都要有完整的归档记录,归档文件要清楚、齐全,一旦投入使用,任何人未经批准不得增、删、改。

(3) 加强敏感媒体的管理。所有媒体应采用物理方法标识出密级;造册登记,编制目录,集中管理;复制、传递、使用、发放都要有审批签字手续,归还时要严格复核手续等;凡属规定密级的各种记录媒体,禁止使用中途转借给他人;保密的存储介质或文件在不使用时应存放在安全的地点并锁在安全器内;销毁必须登记,并由承办人填写销毁记录。

(4) 当存储媒体不使用时,在转交给他人使用之前,不能只做简单的删除操作,而必须把存储在上面的保密数据彻底格式化。

(5) 如果要对关键敏感性的媒体进行销毁,可以采取物理粉碎、强磁场消磁和高温焚烧等方法进行销毁,同时也要注意销毁的登记。

5.5 系统安全和可靠性技术

1. 系统安全和可靠性的定义

系统安全是指为保证信息系统安全可靠运行而采取的安全措施,可用性和可靠性是衡量系统安全的主要指标。

可用性是指系统在规定条件下,完成规定功能的能力。系统可用性用可用度来衡量。系统在 t 时刻处于正确状态的概率称为可用度,用 $A(t)$来表示。

$A(t)$=平均无故障时间/(平均无故障时间+平均修复时间)

平均无故障时间(Mean Time Between Failures,MTBF)是指两次故障之间能正常工作的平均时间。故障是指由于部件的物理失效、环境应力的作用、操作错误或不正确的设计,引起系统的硬件或软件的错误状态。故障既可能是元器件故障、软件故障,也可能是人为攻击造成的系统故障。

平均修复时间(Mean Time Repair a Failure,MTRF)是指从故障发生到系统恢复所需要的平均时间。

可用性还表现在以下3方面。

1) 可靠性

如果系统从来没有故障,那么可用性就是100%,但这基本上是不可能的,所以引进一个辅助参数——可靠性,即在一定的条件下,在指定的时期内系统无故障地执行指定任务的可能性。系统可靠性采用可靠度来衡量。可靠度是指在 t_0 时刻系统正常运行的条件下,在给定的时间间隔内,系统仍然能执行其功能的概率。

2) 可维修性

可维修性是指系统发生故障时容易进行修复以及平时易于维护的程度。可维修性可表现为平均修复时间,在指定时间内恢复服务的可能性。

3) 维修保障

维修保障即系统发生故障时,后勤支援的能力。

因计算机系统硬、软件故障降低信息系统的可靠性,提高信息系统可靠性一般采取避错和容错技术,为抵御灾难造成的信息系统不可用,可采用容灾备份技术实现对灾难的容忍。

2. 提高信息系统可靠性的措施

提高信息系统的可靠性一般采取避错、容错和容灾备份技术。

1) 避错

避错即通过提高信息系统软硬件的质量以抵御故障的发生,要求组成系统的各个部件、器件、软件具有高可靠性,不允许出错或出错率极低。通过精选元器件、严格的工艺、精心的设计来提高可靠性。在现有条件下,避错设计是提高系统可靠性的有效办法。受人们认知的局限性和技术水平的限制,避错不能完全消除错误的发生。

2) 容错

一个系统无论采用多少避错方法,对于可靠性的提高都是有限的,因为不可能保证永

远不出错。因此，还要发挥容错技术，使得在故障发生时，系统仍能继续运行，提供服务与资源。容错设计是在承认故障的情况下进行的，是指在计算机内部出现故障的情况下，计算机仍能正确地运行程序并给出正确结果的设计。

3）容灾备份

容灾备份是信息系统安全的基础设施，对重要信息系统建立容灾备份系统，可以防范和抵御灾难发生给信息系统造成的毁灭性打击。

5.6　隔离网络安全防护

5.6.1　隔离网络定义

隔离网络一般是指不连接互联网的计算机和网络设备组成的封闭的、独立的安全网络。政府机构、金融机构、军事机构和能源、交通、电力等基础行业都会构建隔离网络以保护重要数字资产。针对这类隔离网络，传统的黑客渗透攻击手段都会失效。但隔离网络并不代表着绝对安全，它只能隔离计算机数字资产的网络访问，无法阻断利用物理介质传输数据，如U盘、光盘等数据存储介质，键盘、鼠标等硬件设备。非安全的硬件设备和数据存储介质进入隔离网络，极有可能成为黑客渗透入侵隔离网络的桥梁。

维基解密于2017年6月22日解密了美国中央情报局（CIA）穹顶7（Vault7）网络武器库中的第十二批档案，分别是“野蛮袋鼠”（Brutal Kangaroo）和“激情猿猴”（Emotional Simian）项目。被披露的档案中详细描述了美国情报机构如何远程隐蔽地入侵封闭的计算机网络或独立的安全隔离网络。

5.6.2　隔离网络典型攻击手段和案例

1. “震网三代”病毒攻击原理和流程

2010年6月，“震网”病毒首次被发现，它被称为有史以来最复杂的网络武器，使用了4个Windows 0day漏洞用于攻击伊朗的封闭网络中的核设施工控设备，称为“震网一代”。时隔两年，2012年5月，“火焰”病毒利用了“震网一代”相同的Windows漏洞作为网络武器攻击了多个国家，在一代的基础上新增了更多的高级威胁攻击技术和0day漏洞，定义它为“震网二代”。维基解密公开的CIA穹顶7网络武器库资料表明，其攻击封闭网络的方式和前两代“震网”病毒的攻击方式相似，并使用了新的未知攻击技术，一般定义它为“震网三代”，其主要针对微软Windows操作系统进行攻击，通过USB存储介质对安全隔离网络进行渗透攻击和窃取数据，其对安全隔离网络的攻击原理和流程如图5.5所示。

（1）配置。在攻击者计算机（图5.5中的基础端）上进行恶意代码开发和攻击软件生成。

（2）传输。将生成的攻击软件通过网络传输或存储介质拷贝等方式传输到可能发起攻击的连接互联网的计算机（图5.5中主要计算机），在计算机中植入恶意程序。

（3）感染。凡是接入被感染计算机（图5.5中主要计算机）的USB存储设备（如U盘或移动硬盘），都会被植入恶意程序，整个USB存储设备将会变成一个数据中转站，成为

新的感染源。

(4) 执行。如果这个被感染的 USB 存储设备插入到隔离网络的计算机(图 5.5 中的目标机)中,恶意程序就会在隔离网络计算机后台偷偷运行,等待窃取各类信息。

(5) 部署。隔离网络中被感染计算机中运行的恶意程序还会通过修改注册表,修改系统核心文件,实现隐藏自身、开机自动运行等功能。

(6) 收集。恶意程序在后台运行,按照需要收集各类 Word、PPT、Excel、PDF 等文件数据,被复制到被感染移动存储介质的隐藏目录中。

(7) 卸载。用户隔离网络计算机(图 5.5 中目标机)中卸载移动存储介质。

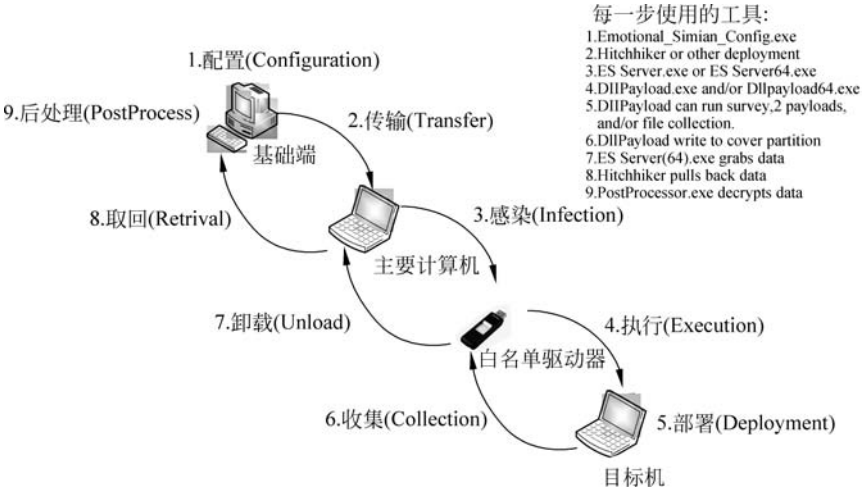

图 5.5 文件删除前后磁盘存储区的变化

(8) 取回。当保存有窃取信息的移动存储介质插回连接互联网的被攻击计算机(图 5.5 中主要计算机),被攻击计算机中后台运行的恶意程序就会读取移动存储介质中存放的被窃取数据,并秘密发送给攻击者计算机(图 5.5 中基础端)。

(9) 后处理。攻击者计算机收到被窃取的信息后按需进行处理。

更可怕的是,多台封闭网络中被感染的计算机彼此间会形成一个隐蔽的网络,用于数据交换和任务协作,并在封闭网络中持续潜伏攻击。

2. "冲击钻"攻击原理和流程

维基解密的创始人阿桑奇于 2017 年 3 月 9 日左右发布一段 2min 的视频专门解释了一个入侵安全隔离网的网络武器"冲击钻"(Hammer Drill),并在同年 3 月 19 日在维基解密网站公布了该项目详细开发文档。

"冲击钻"是通过劫持 Windows 系统上的光盘刻录软件,感染光盘这类数据传输介质的方式,以达到入侵隔离网络的目的。在该项目的开发文档中详细介绍了感染光盘的步骤,下面进行简要分析。

(1) 冲击钻会启动一个线程通过 Windows 操作系统的 WMI 接口来监控系统进程。

(2) 如果在进程列表中发现 NERO EXPRESS. EXE 和 NERO STARTSMART. EXE 等光盘刻录软件进程名,就会往进程中注入一个恶意的 DLL 文件,并劫持进程的读

文件操作。

(3) 如果发现光盘刻录软件读入了 PE 可执行文件,就篡改文件,注入 shellcode 恶意代码。

最终,光盘刻录软件读取编辑的 PE 可执行文件都会被感染,这个光盘将成为一个恶意感染源,如果光盘被接入隔离网络使用,计算机操作人员不慎运行或安装了其中的软件,黑客也就成功渗透了隔离网络。由于资料只披露了 HammerDrill 2.0 的开发笔记,没有利用高级的安全漏洞技术,但在技术上推测实际上可以作为"震网三代"的一个辅助攻击组件,配合震网三代感染光盘等软数据存储介质。

3. "BadUSB"攻击流程和原理

在维基解密披露的 CIA 知识库文档中还介绍了"BadUSB"技术,实际上这是近年计算机安全领域最热门的攻击技术之一,黑客已经广泛利用了该技术,其攻击原理和流程如图 5.6 所示。"BadUSB"主要是利用恶意的 HID(Human Interface Device,即计算机直接与人交互的设备,例如键盘、鼠标等)设备和无线网卡设备进行攻击,而与正常的普通的 HID 不同,这类设备被黑客定制小型化,外形和一个 U 盘没有任何差别。

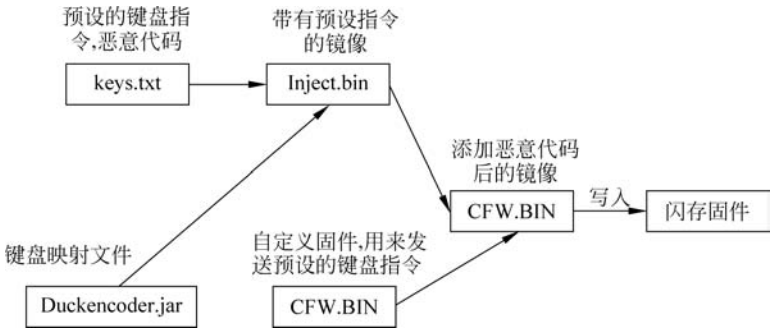

图 5.6　BadUSB 攻击原理和流程图

类似的 HID 设备一旦插入计算机就会被模拟成键盘自动输入恶意代码运行,而 NSA(美国国家安全局)的另外一个强大的无线间谍工具水蟒蛇一号(COTTONMOUTH-I),也是看起来像一个普通 U 盘,但实际上是一个恶意的小型计算机,在被披露的文档中介绍了它可以创建一个无线桥接网络接入到目标网络中,然后通过这个无线网络控制目标计算机。

5.6.3　隔离网络安全防护技术

封闭的隔离网络并不意味着绝对安全。隔离网络除了要修复系统和软件的安全漏洞,还要加强管理严格控制数据的进出,包括外部数据存储介质和硬件设备的接入。

(1) 物理隔离计算机、电视机、打印机、扫描仪等设备,一定要把出厂携带的无线网卡和蓝牙等设备进行拆除或禁用,防止出现利用无线网络的注入攻击或信息泄露。

(2) 对隔离网络使用的信息设备的供应链进行严格管理,防止供应商通过供应链对设备芯片和物理配件进行更替。

(3) 对隔离网络信息处理设备使用进行严格控制,禁止隔离网络设备有意或无意连

接国际互联网。

(4) 对隔离网络移动存储介质和光盘等使用进行严格管理,禁止个人移动存储设备和光盘插入隔离网络计算机中使用。

5.7 容错技术

容错是一种可靠性保障技术,利用冗余的资源使计算机具有容忍故障的能力,即在发生故障的情况下,计算机仍有能力完成指定的任务或继续向外提供正确的服务。

人们对容错技术的研究开始得很早,1952 年,冯·诺依曼就在美国加利福尼亚理工学院做过 5 个关于容错理论研究的报告,他的精辟论述成为以后容错研究的基础。容错技术最早在硬件上研究和实现,在 1950—1970 年得到了重大的发展,并成为一种成熟的技术应用于实际系统中,如双 CPU、双电源。到 20 世纪 60 年代末,出现了以自检、自修计算机 STAR 为代表的容错计算机。20 世纪 70 年代容错技术的应用和研究范围迅速扩大至交通管制、工厂自动化、电话开关等领域,并且出现了用软件实现容错的 SIFT 计算机。20 世纪 80 年代,容错技术的研究随着计算机的普及深入到各个行业,许多公司生产的容错计算机如 Stratus 容错计算机系列,IBM System 88 等已商品化并推入市场。

容错技术主要是通过冗余设计来实现。冗余就是超过系统实现正常功能的额外资源。它以增加资源的办法来换取可靠性。根据增加资源的不同,容错技术可以分为硬件容错、软件容错、信息容错和时间容错。

1. 硬件容错

硬件容错用以避免由于硬件造成的系统失效,通过硬件的物理备份来获得容错能力,如冗余处理器、冗余内存、冗余电源等。广泛应用的硬件冗余之一是硬件堆积冗余,在物理级通过原件的重复获得。硬件容错还可以通过待命储备冗余实现,系统中设置 $m+1$ 个模块,只有一个处于工作状态,其余 m 块都处于待命接替状态,一旦工作模块出了故障,立刻切换到一个待命储备模块,当换上的储备模块发生故障,又切换到另一储备模块,直至资源枯竭。目前,硬件容错广泛应用于信息关键系统中,例如,民航飞机中总有几套计算机系统同时运行,磁盘冗余阵列是硬件容错的典型。

2. 软件容错

软件容错用以避免由于软件引起的系统失效。软件容错的基本思想是用多个不同的软件执行同一功能,利用软件设计差异来实现容错。通过提供足够的冗余信息与算法程序,使系统在实际运行中能够及时发现程序错误,采取补救措施,保证整个计算的正确运行。执行同一任务采用的不同软件程序组成一个有机整体,完成错误检测、程序系统重组及系统恢复等多项功能,达到利用设计差异实现容错的目的。

3. 数据容错

数据容错是指增加额外的数据位以检测或纠正数据在运算、存储及传输中的错误。编码技术是一种数据容错技术,它通过在数据中附加冗余的信息以达到故障检测和故障掩蔽或容错的目的,包括检错编码与纠错编码技术。检错编码可以自动发现错误,而纠错编码具有自动发现错误和纠正错误的能力。编码技术常用在信息的存储、传输和处理中。

在计算机系统中，常用的编码技术有奇偶校验码、循环冗余校验码和扩展海明码等。

4. 时间容错

时间容错是通过消耗时间资源来实现容错，其基本思想是重复执行指令或程序来消除故障带来的影响。按照重复运算在指令级还是程序级可以分为指令复执和程序卷回。指令复执就是当机器检测到错误后，让当前指令重复执行若干次，如果错误是瞬时的，在指令复执期间，有可能不再出现，程序就可继续向前运行；如果在指令复执期间不能纠正错误，则需要通过人工干预或调用诊断程序来消除错误。程序卷回是重复执行一小段程序，常用回滚技术实现。例如，将机器运行的某一时刻作为检查点，此时检查系统运行的状态是否正确，无论正确与否，都将这一状态存储起来，一旦出现运行故障，就返回到最近一次正确的检查点重新运行。

这四种容错技术中最重要也是应用最多的是硬件容错和软件容错，也是本节学习的重点。

5.7.1　硬件容错

硬件容错是通过硬件冗余实现的，硬件冗余通过在一个硬件部件中提供两个或多个物理实体实现冗余，是在给定器件可靠性的前提下提高系统组成部件可靠性的有效方法。硬件冗余有以下三种基本形式。

1. 被动冗余

在无须其他操作的情况下，通过屏蔽故障实现容错。三模冗余（Triple Modular Redundancy，TMR）是被动冗余的典型代表。TMR 首先利用三份硬件同时进行相同功能的计算，再通过投票器从三份计算结果中选择正确的计算结果。如果三份硬件中有一个发生故障，产生错误计算结果，则投票器将剩余两个硬件产生的相同计算结果作为最终计算结果。根据应用的不同，三模冗余的硬件可以是处理器、存储器、电源等。值得注意的是，由于投票器使用少数服从多数的算法，因此 TMR 仅能够屏蔽一个故障部件，为了屏蔽更多的故障部件，则需要使用 5MR、7MR 等更高模的冗余。

2. 主动冗余

在容错之前首先进行故障检测，在故障检测后再进行故障定位和故障恢复工作，从而移除系统中的故障部件。备用备件是一种主动冗余方法，在一个 n 模冗余的备用备件方法中，n 个模块中只有一个是活跃的，而其他 $n-1$ 个模块都作为备份使用。每个模块都有一个故障检测器，并将所有模块连接在一个选择器上。当活跃模块的故障检测器发现故障后，选择器将从备份模块中选择一个模块作为新的活跃模块。

3. 混合冗余

结合了被动冗余和主动冗余的方法，利用主动冗余防止大量错误的产生；利用被动容错实现故障部件的更换。例如，可以在使用 TMR 的基础上，将投票器选择的正确结果反馈给所有冗余模块，各个模块通过将自己的计算结果与反馈结果进行比较，从而判断该模块是否为故障模块，并决定是否将自己移除。

5.7.2　软件容错

随着软件功能和性能的飞速提升，软件变得越来越复杂，软件由于设计缺陷或误操作

而引发系统错误的概率也不断提高。统计数据表明,当前计算机系统中60%～90%的故障是由软件故障引起的。由于软件不像硬件那样存在制造缺陷,也不会产生磨损,所以软件故障大多是由设计故障引起的。

软件容错用于提高软件系统的可靠性,通过提供足够的冗余信息和算法程序,使系统在实际运行时能够及时发现程序设计错误,采取补救措施,以提高软件可靠性。软件容错使软件在出错时仍能向外提供正常或降级服务,避免出现重大人身或财产损失。软件容错技术的方法主要有N版本程序设计和恢复块方法。

1. 恢复块方法

1975年,B. Randell提供了一种动态故障屏蔽技术——恢复块方法,如图5.7所示,这也是最早的一种软件容错技术。恢复块通常与判决器一起使用。在使用恢复块的系统中,系统被划分成一个个故障恢复块,整个系统由这些故障恢复块组成。每个块包含一个主块和一些用来替换的后备模块。主块在第一时间运行,其输出要通过判决器来检查可接受性。这是整个设计中的瓶颈,因为判决器不知道正确的输出是什么。判决器执行检查,检查输出是否在某个可接受的范围内,或输出有没有超出允许的最大变化率。例如,如果任务是计算一艘船的位置,如果前后几微秒之间的距离差有1000km,这样的结果显然是不正确的。

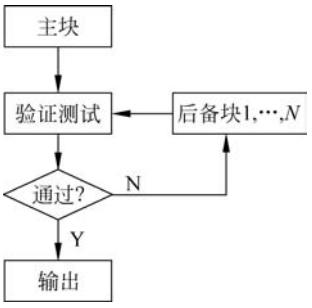

图5.7 恢复块方法

主块得到输出后,立即进行接受测试,当接受测试判断输出不可接受时,系统将回滚并恢复到主块运行之前的状态,然后调用第二个模块,运行获得结果并进行接受测试。如果调用也失败的话,则继续调用另外的替换模块,系统重复这样的操作,直到用完所有模块,或超出规定的时间限制。

使用恢复块方法会引起时间开销,当首要执行模块失败时就发生了时间开销,包括保存全局状态和启动一个或多个替换的模块。这使得恢复块系统很复杂,因为在重试下一个之前,需要系统状态具有回滚的能力。当然也可以通过其他方法完成回滚,例如,使用硬件支持该操作。

设置接受测试时,设计人员常常面临一些难题,如果允许的范围太严格,那么接受测试将产生大量的错误警报。如果设置太宽松的话,把错误的输出当作正确结果接受的可能性会大大增大。因此设置接受测试时必须从实际出发,根据需求进行相应的设置工作。

2. N版本技术(NVP)

N版本技术是一种静态的故障屏蔽技术,其设计思想是N个独立生成的功能相同的程序同时执行,使用表决器比较各个版本产生的结果,并将其中一个作为正确的结果给出。这种容错方法依赖于不同版本程序之间的独立性。该技术已经运用到很多实际系统中,例如,铁路交通控制系统、飞行控制系统。

在N版本软件系统中,有N个不同的模块同时独立地执行。每个模块以不同的方式完成相同的任务,各自向表决器提交它们的结果,由表决器确定正确的结果,并作为模块的结果返回。利用设计多样性得到的N版本软件系统能克服大多数软件中出现的设计故障。N版本软件的一个重要特性就是系统包含多个版本软件和多种类型的硬件。

目的是通过增加差异以避开共有的故障。开发N版本软件过程中，对于每个不同版本，尽可能以不同的方式实现。包括不同的工具(例如静态和动态的分析器，辅助调试的专家系统等工具)、不同的编程语言以及不同的环境。每个开发小组在编程期间也要尽可能地减少交流。只有满足设计的多样性，N版本软件才能真正做到容错。

恢复块和N版本软件之间的不同之处并不多，但却非常突出。传统的恢复块方法中，用来替换的块逐个执行，直到判决器找到可接受的结果；N版本软件方法通常在N份冗余的硬件上同时执行这些不同版本的软件。在逐个重试的过程中，尝试多个替换版本的时间开销可能很大，这种方法尤其不适用于实时系统：相反地，同时运行的N版本软件系统需要N份冗余硬件和通信网络连接它们。这两种方法的另一个重要不同在于判决器和表决器。恢复块方法需要为每个模块建立一个特定的判决器，而N版本软件方法中，只需要使用一个简单的表决器即可。在实际开发中，设计人员要全面衡量它们的优缺点，并结合应用的实际需求，进行折中考虑，尤其是性能和资金的开销方面，从而确定哪种方案更适合工程。

为了体现对设计的冗余，NVP系统的N份程序必须采取不同的方法或由不同的人独立设计。NVP系统的结构如图5.8所示。

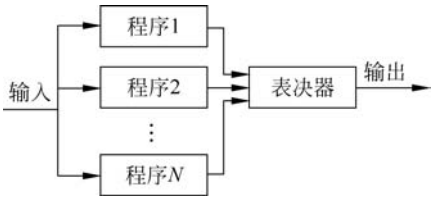

图5.8　NVP系统结构

5.8　信息系统灾难恢复技术

视频讲解

随着信息化的发展，越来越多关键数据和业务集中到信息系统中，社会对信息系统的依赖性越来越强，而信息系统易受到地震、火灾、人为误操作、硬件故障等诸多侵扰，一方面，数据丢失和损坏将造成难以估量的损失；另一方面，即使短时间的系统停机也将造成业务停顿和经济损失，因此灾难备份和恢复成为迫切需要解决的问题，重要信息系统必须建立容灾备份系统，以防范和抵御灾难带来的打击。美国国防部提出的信息保障模型PDRR中就包含恢复环节，灾难恢复是信息系统安全的重要组成部分。

5.8.1　概述

传统的数据备份技术和服务器集群技术足以避免由于各种软硬件故障、人为操作失误和病毒侵袭所造成的破坏，保障数据安全，但是当面临大范围灾害性突发事件，如地震、火灾、恐怖袭击时，上述技术就无能为力了。此时若想迅速恢复应用系统的数据，保持企业的正常运行，就必须建立异地的灾难备份系统(容灾系统)。美国Minnesota大学的研究表明，遭遇灾难的同时又没有灾难恢复计划的企业，超过60%在2～3年后将退出市场。在美国“9·11”事件中，很多公司多年积累的经营数据毁于一旦，公司处于崩溃的边缘，而一些建立了容灾系统的公司，如总部设在世贸中心的摩根-斯坦利公司，却在第二天就恢复了正常运转。这一事例再次唤起人们对容灾技术的重视。

业务连续性和灾难恢复起步于20世纪70年代中期的美国，历史性标志是1979年在美国宾夕法尼亚州的费城建立了专业商业化的容灾备份中心并对外提供服务。20世纪

90年代后期,千年虫问题促进了业务连续性和灾难恢复管理的进一步深入和发展。2001年轰动一时的"9·11"恐怖袭击事件不仅造成了重大的人员伤亡和财产损失,一批设在世贸中心的公司因为重要数据的毁灭而再也无法正常营业。"9·11"给大家带来的深刻的启示就是容灾备份是信息系统安全的重要设施,重要信息系统必须构建容灾备份系统,以防范和抵御灾难带来的毁灭性打击。

我国业务连续性和灾难恢复工作起步于20世纪90年代末,这时一些单位在信息化建设的同时,开始关注数据安全的保护,开展了数据备份工作。随后,千年虫问题和"9·11"事件也极大触动了我国灾难恢复管理的发展和成熟。

2003年,中共中央办公厅、国务院办公厅下发了《国家信息化领导小组关于加强信息安全保障工作的意见》,在文件中要求要高度重视灾难备份工作。为贯彻落实中央指示,国务院信息化工作办公室于2004年9月下发了《关于做好重要信息系统灾难备份工作的通知》,文件强调了"统筹规划、资源共享、平战结合"的灾难恢复工作原则。为进一步推动八个重点行业(银行、证券、保险、电力、民航、铁路、海关、税务)加快实施灾难恢复工作,国务院信息化工作办公室于2005年4月下发了《重要信息系统灾难恢复指南》,文件指明了灾难恢复的流程,容灾备份中心的等级划分及灾难恢复预案的制定,使得灾难恢复建设迈上了一个新的台阶。2007年,在《重要信息系统灾难恢复指南》基础上,编制并正式发布了国家标准GB/T 20988—2007《信息安全技术 信息系统灾难恢复规范》来指导信息技术容灾备份系统的建设。

5.8.2 灾难恢复的级别和指标

1. 灾难恢复的定义

在《重要信息系统灾难恢复规划指南》中对于灾难有明确定义:灾难是由于人或自然原因造成的信息系统运行严重故障或瘫痪,使信息系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件,通常导致信息系统需要切换到备用场地运行。灾难主要包括地震、火灾、水灾、战争、恐怖袭击、设备系统故障、人为破坏等无法预料的突发事件。

灾难恢复是指利用技术、管理手段及相关资源确保关键数据、关键数据处理信息系统、关键业务在灾难发生后可以恢复和重续运营的过程。灾难恢复的最高目标是实现数据零丢失和业务连续性。

2. 容灾备份系统的种类

按照建立容灾系统目标的不同,容灾备份系统可以分为两种,即数据容灾、应用容灾。

数据容灾是最常见的容灾备份方式,是指建立一个异地的备份数据系统,该系统是对本地系统关键应用数据的实时复制,也可比本地数据略微滞后。数据容灾的主要目的是保证企业关键数据的完整性和可用性。在数据容灾这个级别,发生灾难时应用会中断,服务器必须暂停业务来进行异地恢复,这种方式的优点是成本低,构建简单。但是对需要保持7×24h连续服务的企业来说,数据级容灾方式显然是不够的。

应用级容灾是在数据容灾的基础上,同时将应用程序的处理状态进行备份,其实现方式是在异地建立一套完整的、与本地数据系统相当的备份应用系统(可以同本地应用系统

互为备份，也可与本地应用系统共同工作）。当灾难发生时，异地的应用容灾中心可以接替原来的系统继续工作，保持业务的连续性。应用容灾是更高层次的容灾系统。

3. 灾难备份系统的级别

设计一个容灾备份系统需要考虑多方面的因素，包括备份/恢复的数据量大小、应用数据中心和备援数据中心之间的距离和连接方法、灾难发生时所要求的恢复速度、备援中心的管理和经营方法，以及可投入的资金多少等。根据这些因素，可将容灾备份系统划分为不同的级别，分别适用于不同的规模和应用场合。

1）国际上的灾难恢复等级划分

灾难恢复的国际标准是1992年Anaheim提出的SHARE 78，将灾难恢复由高到低划分为以下7级。

（1）第0级：没有异地数据。

第0级没有任何异地备份或应急计划，数据仅在本地进行备份恢复，没有送往异地。事实上，这一层并不具备真正灾难恢复的能力。

（2）第1级：卡车运送访问方式（Pickup Truck Access Method，PTAM）。

第1级要求必须设计一个灾难恢复应急方案，能够备份所需要的信息并将它保存在异地，灾难恢复时将根据需要，有选择地搭建备援的硬件平台并在其上恢复数据。PTAM指将本地备份的数据用交通工具送到远方。这种方案相对来说成本较低，但难于管理。

PTAM是一种广泛使用的容灾系统，备份数据被送往远离本地的异地保存，可抵御大规模的灾难事件。灾难发生后，需要按预定的数据恢复方案购置和安装备援硬件平台，恢复系统和企业数据，并重新与网络连接。这种容灾方案成本低（仅需要传输工具和存储设备的消耗），且易于配置。但当数据容量增大时，备份数据难以管理，用户难以及时知道所需的数据存储在什么地方。

当备援系统开始工作后，首先应及时恢复关键应用，非关键应用可根据需要慢慢恢复，因为PTAM的备份地点事先往往只有很少的硬件设备，因此将其称为冷备份站点，它的恢复时间往往较长，如一星期甚至更久。

（3）第2级：PTAM＋热备份中心。

第2级在第1级的基础上再加上热备份中心以进一步灾难恢复。热备份中心拥有足够的硬件和网络设备，当主数据中心破坏时可切换用于支持关键应用的备援站点。对于十分关键的应用，必须由热备份站点在异地提供支持。这样当灾难发生时才能及时恢复。在第2级容灾系统中，平时备份数据用PTAM的方法存入备份数据仓库，当灾难发生的时候，备份数据再被运送到一个热备份站点。虽然移动数据到一个热备份站点增加了成本，但却缩减了灾难恢复的时间，一般在一天左右。

（4）第3级：电子链接。

第3级是在第2级的基础上用电子链路取代卡车进行备份数据传送的容灾系统，热备份站点和主数据中心在地理上必须远离，备份数据通过网络传输。由于热备份站点要持续运行，因此系统成本高于第2级，但进一步提高了灾难恢复的速度，典型的恢复时间在一天以内。

(5) 第4级：活动状态的备份中心。

第4级要求地理上分开的两个站点同时处于工作状态并相互管理彼此的备份数据，另一项重大的改进就是两个站点之间可以相互分担工作负载，站点一可以成为站点二的备份；反之亦然，备援行动可以在任何一个方向发生。关键的在线数据不停地在两个站点之间复制和传送着，灾难发生时，另一站点可通过网络迅速切换用于支持关键应用。但是该系统自最近一次数据复制以来的业务数据将会丢失，其他非关键应用也将需要手工恢复。第4级容灾系统把关键应用的灾难恢复时间降低到了小时级或分钟级。

(6) 第5级：两个活动的数据中心，两步提交。

第5级与第4级的结构类似，在满足第4级所有功能要求的基础上，进一步提供了两个站点间的数据互作镜像(数据库的一次提交过程会同时更新本地和远程数据库中的数据)。数据库的两步提交方法保证了任何一项事务在被接受以前，两个站点间的数据都必须同时被更新。在备援站点中需要配备一些专用硬件设备，以保证在两个站点之间自动分担工作负载和两步提交的正确执行，因为采用了两步提交来同步数据，在两个站点间互作镜像，所以当灾难发生时，只有传送中尚未完成提交的数据被丢失，恢复的时间被降低到了分钟级。

(7) 第6级：0数据丢失。

第6级是灾难恢复的最高级别，可以实现零数据丢失。只要用户按下Enter键向系统提交了数据，那么不管发生了什么灾难性事件，系统都能保证该数据的安全。所有的数据都将在本地和远程数据库之间同步更新，当发生灾难事件时，备援站点能通过网络侦测故障并立即自动切换，负担起关键应用。第6级是容灾系统中最昂贵的方式，但也是速度最快的恢复方式。

第4级、第5级和第6级容灾系统具有类似的系统框架结构，区别在于数据备份管理软件的差异和备援站点内硬件配置的不同，进而导致了系统成本和性能的差异。第4级的容灾系统只需要配置远程系统备份软件即可工作；第5级容灾系统依赖于数据库系统的两步提交来保持数据的同步；第6级容灾系统则需要配置复杂的数据管理软件和专用的硬件设备，以保证灾难发生时的零数据丢失和备援站点的即时切换。

2) 我国灾难恢复等级划分

在GB/T 20988—2007《信息安全技术 信息系统灾难恢复规范》中，根据支持灾难恢复各个等级所需要的资源，即数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、技术支持能力、运行维护管理能力和灾难恢复预案这7个要素划分了6个灾难恢复等级。

第一级：基本支持。

第二级：备用场地支持。

第三级：电子传输和部分设备支持。

第四级：电子传输和完整设备支持。

第五级：实时数据传输及完整设备支持。

第六级：数据零丢失和远程集群支持。

（1）第一级：基本支持。

在第一级中，每周至少做一次完全数据备份，并且备份介质场外存放，同时还需要有符合介质存放的场地；单位要制定介质存放、验证和转储的管理制度，并按介质特征对备份数据进行定期的有效性验证；单位需要指定经过完整测试和演练的灾难恢复预案，具体技术和管理支持如表5.2所示。

表5.2　灾难恢复第一级要求

	要　素	要　求
A.1.1	数据备份系统	① 完全数据备份至少每周一次； ② 备份介质场外存放
A.1.2	备用数据处理系统	—
A.1.3	备用网络系统	—
A.1.4	备用基础设施	有符合介质存放条件的场地
A.1.5	技术支持	—
A.1.6	运行维护支持	① 有介质存取、验证和转储管理制度； ② 按介质特征对备份数据进行定期的有效性验证
A.1.7	灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案

（2）第二级：备用场地支持。

第二级相当于在第一级的基础上，增加了在预定时间内能调配所需使用的数据处理设备、通信线路和网络设备到场要求；并且需要有备用的场地，它能满足信息系统和关键功能恢复运行的要求；对于单位的运维能力，也增加了具有备份场地管理制度和签署符合灾难恢复时间要求的紧急供货协议，具体技术和管理支持如表5.3所示。

表5.3　灾难恢复第二级要求

	要　素	要　求
A.2.1	数据备份系统	① 完全数据备份至少每周一次； ② 备份介质场外存放
A.2.2	备用数据处理系统	灾难发生时能在预定时间内调配所需的数据处理设备
A.2.3	备用网络系统	灾难发生时能在预定时间内调配所需的通信线路和网络设备
A.2.4	备用基础设施	① 有符合介质存放条件的场地； ② 有满足信息系统和关键业务恢复运作要求的备用场地
A.2.5	技术支持	—
A.2.6	运行维护支持	① 有介质存取、验证和转储管理制度； ② 按介质特征对备份数据进行定期的有效性验证； ③ 具有备份场地管理制度； ④ 与相关厂商签署符合灾难恢复时间要求的紧急供货协议； ⑤ 与相关厂商签署符合灾难恢复时间要求的备用通信线路协议
A.2.7	灾难恢复预案	有相应的经过完整性测试和演练的灾难恢复预案

(3) 第三级：电子传输和部分设备支持。

第三级要求配置部分数据处理设备、部分通信线路和网络设备；要求每天实现多次的数据电子传输，并在备用场地配置专职的运行管理人员；对于运行维护支持而言，要求具备备用计算机处理设备维护管理制度和电子传输备份系统运行管理制度，具体技术和管理支持如表5.4所示。

表5.4 灾难恢复第三级要求

	要 素	要 求
A.3.1	数据备份系统	① 完全数据备份至少每天一次； ② 备份介质场外存放； ③ 每天多次利用通信网络将关键数据定时批量传送至备用场地
A.3.2	备用数据处理系统	配置灾难恢复所需的部分数据处理设备
A.3.3	备用网络系统	配备部分通信线路和网络设备
A.3.4	备用基础设施	① 有符合介质存放条件的场地； ② 有满足信息系统和关键业务恢复运作要求的备用场地
A.3.5	技术支持	在备用场地有专职的计算机机房运行管理人员
A.3.6	运行维护支持	① 按介质特征对备份数据进行定期的有效性验证； ② 有介质存取、验证和转储管理制度； ③ 有备用计算机机房管理制度； ④ 有备用数据处理设备硬件维护管理制度； ⑤ 有电子传输数据备份系统运行管理制度
A.3.7	灾难恢复预案	有相应的经过完整性测试和演练的灾难恢复预案

(4) 第四级：电子传输和完整设备支持。

第四级相对于第三级中的部分数据处理设备和网络设备而言，须配置灾难恢复所需的全部数据处理设备、通信线路和网络设备，并处于就绪状态；备用场地也提出了7×24h运行的要求，同时，对技术支持人员和运维管理要求也有相应的提高，具体如表5.5所示。

表5.5 灾难恢复第四级要求

	要 素	要 求
A.4.1	数据备份系统	① 完全数据备份至少每天一次； ② 备份介质场外存放； ③ 每天多次利用通信网络将关键数据定时批量传送至备用场地
A.4.2	备用数据处理系统	配置灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态
A.4.3	备用网络系统	配备灾难恢复所需的通信线路和网络设备，并处于就绪状态
A.4.4	备用基础设施	① 有符合介质存放条件的备用场地； ② 有符合备用数据处理系统和备用网络设备运行要求的场地； ③ 有满足关键业务功能恢复运作要求的场地； ④ 以上场地应保持7×24h运作

续表

	要　素	要　求
A.4.5	技术支持	在备用场地有： ① 7×24h 专职计算机机房管理人员； ② 专职数据备份技术支持人员； ③ 专职硬件、网络技术支持人员
A.4.6	运行维护支持	① 按介质特征对备份数据进行定期的有效性验证； ② 有介质存取、验证和转储管理制度； ③ 有备用计算机机房运行管理制度； ④ 有硬件和网络运行管理制度； ⑤ 有电子传输数据备份系统运行管理制度
A.4.7	灾难恢复预案	有相应的经过完整性测试和演练的灾难恢复预案

（5）第五级：实时数据传输和完整设备支持。

第五级相对于第四级的数据电子传输而言，要求采用远程数据复制技术，利用网络将关键数据实时复制到备用场地；备用网络应具备自动或集中切换能力；备用场地有 7×24h 专职数据备份、硬件、网络技术支持人员，具备较严格的运行管理制度，具体如表 5.6 所示。

表 5.6　灾难恢复第五级要求

	要　素	要　求
A.5.1	数据备份系统	① 完全数据备份至少每天一次； ② 备份介质场外存放； ③ 用远程数据复制技术，并利用通信网络将关键数据实时复制到备份场地
A.5.2	备用数据处理系统	配置灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态
A.5.3	备用网络系统	① 配备灾难恢复所需的通信线路和网络设备，并处于就绪状态； ② 具备通信网络自动或集中切换能力
A.5.4	备用基础设施	① 有符合介质存放条件的备用场地； ② 有符合备用数据处理系统和备用网络设备运行要求的场地； ③ 有满足关键业务功能恢复运作要求的场地； ④ 以上场地应保持 7×24h 运作
A.5.5	技术支持	在备用场地有： ① 7×24h 专职计算机机房管理人员； ② 专职数据备份技术支持人员； ③ 专职硬件、网络技术支持人员
A.5.6	运行维护支持	① 按介质特征对备份数据进行定期的有效性验证； ② 有介质存取、验证和转储管理制度； ③ 有备用计算机机房运行管理制度； ④ 有硬件和网络运行管理制度； ⑤ 有实时数据备份系统运行管理制度
A.5.7	灾难恢复预案	有相应的经过完整性测试和演练的灾难恢复预案

(6) 第六级：数据零丢失和远程集群支持。

第六级相对于第五级的实时数据复制而言，要求实现远程数据实时备份，实现零丢失；备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容，应用软件是集群的，可以实现无缝切换，并具备远程集群系统的实时监控和自动切换能力；对于备用网络系统的要求也加强，要求最终用户可通过网络同时接入主、备中心；备用场地还有7×24h专职操作系统、数据库和应用软件的技术支持人员，具备完善、严格的运行管理制度。具体技术和管理支持如表5.7所示。

表5.7 灾难恢复第六级要求

	要 素	要 求
A.6.1	数据备份系统	① 完全数据备份至少每天一次； ② 备份介质场外存放； ③ 远程实时备份，实现数据零丢失
A.6.2	备用数据处理系统	① 备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容； ② 应用软件是集群的，可以实现无缝切换； ③ 具备远程集群系统的实时监控和自动切换能力
A.6.3	备用网络系统	① 配备与生产系统相同等级的通信线路和网络设备； ② 备用网络处于运行状态； ③ 最终用户可通过网络同时接入主、备中心
A.6.4	备用基础设施	① 有符合介质存放条件的备用场地； ② 有符合备用数据处理系统和备用网络设备运行要求的场地； ③ 有满足关键业务功能恢复运作要求的场地； ④ 以上场地应保持7×24h运作
A.6.5	技术支持	在备用场地有： ① 7×24h专职计算机机房管理人员； ② 7×24h专职数据备份技术支持人员； ③ 7×24h专职硬件、网络技术支持人员； ④ 7×24h专职操作系统、数据库和应用软件技术支持人员
A.6.6	运行维护支持	① 按介质特征对备份数据进行定期的有效性验证； ② 有介质存取、验证和转储管理制度； ③ 有备用计算机机房运行管理制度； ④ 有硬件和网络运行管理制度； ⑤ 有实时数据备份系统运行管理制度； ⑥ 有操作系统、数据库和应用软件运行管理制度
A.6.7	灾难恢复预案	有相应的经过完整性测试和演练的灾难恢复预案

通过分析以上灾难恢复的级别，一个完整的容灾系统应该具有以下几个组成部分。

(1) 本地的高可用系统：确保本地发生局部故障或单点故障时的系统安全。

(2) 数据备份系统：用于抗御用户误操作、病毒入侵、黑客攻击等的威胁。

(3) 数据远程复制系统：保证本地数据中心和远程备援中心的数据一致。

(4) 远程的高可用管理系统：实现远程广域范围的数据管理，它基于本地的高可用

系统之上，在远程实现故障的诊断、分类并及时采取相应的故障管理措施。

4. 容灾系统的系统结构

容灾系统的系统框架如图 5.9 所示。

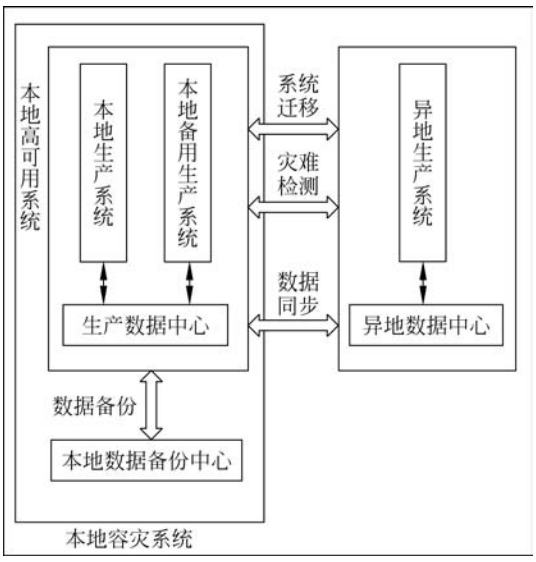

图 5.9　容灾系统的系统框架

容灾系统的主要作用是保证数据完整性和业务连续性，数据完整性是业务连续性的基础。一个完整的容灾系统，应该由本地生产系统、本地备用生产系统、生产数据中心、本地备份数据中心、异地应用系统、异地数据中心六部分组成。本地生产系统、本地备用生产系统和生产数据中心组成了高可用系统，根据需求，可以使用其中的某几部分组成不同级别的容灾系统。

使用本地高可靠系统和本地数据备份中心可建立本地容灾中心，能够容忍硬件毁坏等灾难造成的单点失效，而对于火灾、大楼倒塌等大规模灾难却无能为力。使用本地高可用系统、本地备用数据中心和异地数据中心，可以建立异地数据容灾系统。使用本地高可靠系统、本地备用数据中心、异地应用系统和异地数据中心，可以建立异地应用容灾系统。而根据异地备份中心与本地系统距离的远近，系统所能容忍的灾难也不相同，如果异地数据备份中心与本地系统在 100km 之内，可以容忍火灾、停电、建筑物倒塌等灾难；如果达到了几百千米，可以容忍地震、水灾等大规模、大范围的灾难。

本地系统与异地系统的数据同步方式也有很多种选择，例如，对于异地数据容灾系统，数据同步方式可以选择用运输工具运输到异地数据中心，也可以选择同步或者异步的方式直接由生产数据中心复制到异地数据中心；而对于异地应用容灾系统，就只能选择同步或者异步的方式直接由生产数据中心直接复制到异地数据中心。在这个容灾系统结构中，本地数据中心需要及时地将数据复制到异地数据中心，并要保证数据的完整性和可用性；而为使异地系统能够及时地发现本地系统的灾难，就需要进行灾难检测，保证异地系统能够及时发现灾难，并能及时地替换本地系统，也就是将本地系统的业务迁移到异地

系统,从而保证业务的连续性。

5. 灾难恢复的指标

在灾难恢复领域,除了等级划分,还提供了用于量化描述灾难恢复目标的最常用的恢复目标指标:RTO(恢复时间目标)和RPO(恢复点目标)。

恢复点目标(Recovery Point Objective,RPO):灾难发生后,系统和数据必须恢复到的时间点要求。它代表了灾难发生时允许丢失多长时间的数据量。例如,1h的RPO指灾难发生后容灾系统能够对灾难发生1h前的所有数据进行恢复,但这1h的数据可能会丢失。

恢复时间目标(Recovery Time Objective,RTO):灾难发生后,信息系统或业务功能从停顿到必须恢复的时间要求,它代表了系统恢复的时间。

PRO描述的是数据丢失指标,而RTO描述的是服务丢失指标,二者没有必然的关联性。实际中可根据RPO和RTO的要求规划建设容灾备份系统。

5.8.3 容灾系统关键技术

容灾系统所包含的关键技术包括数据存储技术、远程镜像技术、灾难检测、系统迁移等。

1. 数据存储技术

容灾系统需要存储的数据量庞大,为了提高备份的效率,出现了很多新的备份技术,在很大程度上提高了备份速度,目前采用的备份技术主要有以下几种。

1) 直接附加存储

传统的直接附加存储(Direct Access Storage,DAS)结构中,将存储设备(如磁盘、阵列)通过SCSI接口附加在服务器上,由服务器提供存储设备的管理和对外服务。这种存储结构价格比较便宜,但是支持的存储容量有限制,每条并行的SCSI总线最多只能支持15个磁盘阵列,当业务量非常大,需要存储的数据非常多时,这种存储结构就不大适用了。并且客户每次访问存储设备中的数据时,数据需要在存储设备和服务器之间多次转发,尽管服务器并不关心数据内容,通常也不对数据本身进行处理,但数据请求和传送都需要服务器的介入,存储容量扩大后,对同一台服务器进行访问,容易形成访问瓶颈。

2) 网络附加存储

网络附加存储(Network Attached Storage,NAS)是一种以数据为中心的存储结构,存储子系统不再附属于某个服务器,而是通过专门系统的定制,将通用服务器上的无关功能去掉,只保留存储相关功能,可以看成是一台专门负责存储的"瘦"服务器,具有比DAS更高的读写性能。NAS将存储设备通过网络协议控制器直接连接在局域网上,通过NAS内部的文件管理系统对外提供服务。

将NAS设备连接到网络上非常方便。NAS设备提供RJ-45这样的网络物理接口和单独的IP地址,可以将其直接挂接在主干网的交换机或其他局域网的Hub上,通过简单的设置(如设置机器的IP地址等)就可以在网络中即插即用地使用,而且进行网络数据在线扩容时也无须停顿,从而保证数据流畅存储。与传统的服务器或DAS存储设备相比,NAS可以拥有更大的存储空间和相对低廉的价格。

由于普通的 LAN 不是针对存储应用设计的专用网络，而且目前大部分 LAN 还是使用 10Mb/s 或 100Mb/s 的传输速率连接，加上 LAN 上又有大量计算机，因此网络有限的带宽要面对大量的传输需求，NAS 存储设备所能分到的带宽必然有限。这就造成 NAS 的最大缺点，传输速率慢且不稳定，这在进行备份或者大文件存取时将花费大量的时间。

3）存储区域网络

存储区域网络（Storage Area Network，SAN）的设计思想实际上很简单，就是建立一个单独的网络系统，采用适合数据传输和管理特点的物理、链路、网络传输等各层协议，专门用于存储的管理和数据交换。目前该网络使用 FC（Fiber Channel）协议。该网络只用于存储，不会有其他服务的数据流在上面传输，可以做到独享带宽；而且因为光纤通道本身具有的高传输速率，使得 SAN 的传输速率可以达到 200Mb/s 或者更高，同时还可以保证数据传输速率的稳定性。但也正是由于受到 SAN 使用专用网络拓扑结构和不同于一般网络传输协议的限制，SAN 的设备仅能做到与连接在 SAN 上的服务器间的直接访问，而在 LAN 上的客户端是无法直接访问 SAN 的设备的，必须通过服务器间接访问。由于 SAN 的硬件设备价格昂贵，而且，SAN 作为一种专用的存储网络，需要培训专门的人员来管理，这使得 SAN 的总体拥有成本居高不下，使得很多希望使用 SAN 的企业望而却步，转而使用性能较差的 NAS，因而 SAN 的普及和使用受到较大影响。

4）基于 IP 的存储网络和 iSCSI

为了解决前面提到的 SAN 应用带来的问题，又出现了基于 IP 的存储网络，IP 存储网络可以说是结合了 NAS 和 SAN 两者的优点：一方面，它采用 TCP/IP 作为网络协议，使得它具有 NAS 易于访问的特点；另一方面，它又有独立专用的存储网络结构。因此，基于 IP 的存储网络可以使用目前应用广泛的以太网（Ethernet）技术和设备来构建专用的存储网络，通过使用 Ethernet 的设备，其成本与 FC SAN 相比大为降低，而且还保持有 SAN 的传输速率高且稳定的优点。以上两点可以说是基于 IP 的存储网络技术的两个最大的优势。

IP-SAN 最大的问题是它的性能能否达到 FC-SAN 的标准。Ethernet 虽然已经出现了很长时间，但由于 Ethernet 已拥有的大量用户和巨大市场，各个厂家不会放弃它，Ethernet 仍然具有很大的发展潜力。虽然 FC 协议也在持续不断地发展，但是 FC-SAN 的用户数量和市场范围都远无法和 Ethernet 相比，其发展动力也就不如 Ethernet 大。Ethernet 速度目前已经有了数量级的提高，千兆级 Ethernet 也已经投入使用，但目前主要用于服务器端或构建主干网。千兆级 Ethernet 在速度上已经可以和 FC 相比了，其传输介质可以使用光纤、无屏蔽双绞线等多种传输介质，其价格却不像 FC 那么昂贵。下一步 Ethernet 的速度会达到 10Gb/s，而 FC 的下一个目标只是制造和推广 2Gb/s 的产品。

目前基于 IP 的存储网络的核心技术是 iSCSI，这是一种开放协议，其基本架构是在 SCSI 的数据包上加上 TCP/IP，由于加入了 TCP/IP，iSCSI 协议可以使 SCSI 数据包在普通的 IP 网络上传输。iSCSI 协议与 FC 协议没有任何联系，该协议的最终目的是取代 FC 协议在 SAN 中的位置。

2. 远程镜像技术

数据备份技术通常是在本地节点进行的备份操作，备份间隔的单位通常为天或月，生

成静态的文件,可以经过压缩等处理,静态保存,在灾难发生时能够从备份中将数据恢复出来。例如,保存于光盘、磁带、硬盘等数据备份介质上的数据,需要经过恢复技术配合合适的系统硬件环境才能恢复出来供业务系统使用。

而在容灾系统中的远程镜像则是将数据实时或准实时复制到异地节点,这是一个动态的过程,数据是在不断更新的,复制的数据在异地节点上保持原来的数据形态,与本地节点的数据保持基本一致性,可以不经过恢复技术就直接使用。

镜像是在两个或多个磁盘或存储系统上产生同一个数据镜像视图的一个信息存储过程,一个叫主镜像系统,另外一个叫从镜像系统。按主、从镜像存储系统所处的位置可分为本地镜像和远程镜像,远程镜像是容灾备份的核心技术。按请求镜像的主机是否需要远程镜像站点的确认信息,又可分为同步远程镜像和异步远程镜像。

同步远程镜像中每一步本地I/O事务均需等待远程复制的完成方予释放,这种方式的远端数据与本地数据完全同步,但由于数据复制过程中存在时延,本地I/O访问效率下降,所以只限于在相对较近的距离上应用(一般专线连接在60km以内,常见于同城系统),同时,这种复制技术还受到带宽因素的制约,若远程的I/O带宽较窄时,会显著拖慢主数据中心的I/O,影响系统性能。但同步镜像使远程拷贝总能与本地机要求复制的内容相匹配,当主站点出现故障时,用户和应用程序换到一个代替站点后,远程的副本可以继续执行操作。

异步远程镜像保证在更新远程存储视图前完成向本地存储系统的基本输入/输出操作,而由本地存储系统提供请求镜像服务器的操作完成确认信息,不需要等待远程存储系统提供操作完成确认信息,这使得本地系统性能受到很小的影响。但是,许多远程的从属存储子系统的写操作没有得到确认,当某种因素造成数据传输失败时,可能出现数据一致性问题。为了解决数据一致性问题,目前大多采用延迟复制的技术,它可以在确保本地数据完好无损后进行远程数据更新。

3. 快照

远程镜像技术往往同快照技术结合起来实现数据信息的远程备份,即通过镜像把数据备份在远程存储系统中,再借助快照技术把远程存储系统中的信息备份到远程的磁带库、光盘库中。快照是通过软件对要备份的磁盘子系统的数据快速扫描,在正常应用进行的同时实现对数据的一个完全的备份。它可使用户在正常应用不受影响的情况下实时提取当前在线数据,其备份窗口接近于零,可大大增加系统应用的连续性,为实现系统真正的不间断运转提供了保证。

4. 灾难检测

对于火灾、地震等大规模灾难,当然可以依靠人为确定,但是对于停电、硬件毁坏等很难觉察到的灾难就不能仅依靠人去发现。现在对灾难的发现方法一般是通过心跳技术和检查点技术,这种技术在高可靠性集群中应用很广泛。对于异地容灾,备份生产中心和主生产中心可能相隔千里,这时候因为网络延迟较大或者其他原因,可能会影响心跳检测的效果,因此如何对现有的检测技术进行改进,以适应广域网的要求,将是实现高效的远程容灾系统的基础。

心跳技术,就是每隔一段时间都要向外广播自身的状态(通常为"存活"状态),在进行

心跳检测时，心跳检测的时间和时间间隔是关键问题，如果心跳检测得太频繁，将会影响系统的正常运行，占用系统资源；如果间隔时间太长，则检测就比较迟钝，影响检测的及时性。检查点技术又称为主动检测，就是每隔一段时间周期，就会对被检测对象进行一次检测，如果在给定的时间内，被检测对象没有响应，则认为检测对象失效。与心跳技术相同，检测点技术也受到检测周期的影响，如果检测周期太短，虽然能够及时发现故障，但是给系统造成很大的开销；如果检测周期太长，则无法及时发现故障。

为了能够实现异地容灾系统，就必须建立广域网上的分布式可靠性系统，这就需要有高效的故障检测系统，能够及时地发现故障，及时切换。而对于广域网来说属于异步的系统，没有同步的时钟，没有可靠的传输通道，如何在异步的分布式模型中实现可靠高效的故障检测将是建立异地容灾系统的基础。

5. 系统迁移

在发生灾难时，为了能够保证业务的连续性，必须能够实现系统透明迁移，也就是能够利用备用系统透明地代替生产系统。对于实时性要求不高的容灾系统，通过 DNS 或者 IP 地址的改变来实现系统迁移便可以了，但是对于可靠性、实时性要求较高的系统，就需要使用进程迁移算法，进程迁移算法的好坏对于系统迁移的速度有很大影响，现在该算法在分布式系统和集群中得到了广泛的运用，并发挥着重大作用，也有很多研究对该算法的性能进行了改进。

进程迁移算法在目前主要有贪婪拷贝算法、惰性拷贝算法和预拷贝算法。贪婪拷贝算法简单、易于实现，但是延时较长，并且冗余数据造成较大的网络延迟；惰性拷贝的延迟小，网络负担小，但是对原主机具有依赖性，可靠性差；预拷贝算法将信息分为两次拷贝，使得传输时间反而增长。现在的进程迁移算法都是应用于本地集群的，要想在远距离容灾系统中实现高效的进程迁移，就必须对进程迁移算法进行改进，使它能够适应广域网复杂的环境。

习　　题

一、填空题

1. 物理安全是对_____、_____、_____、系统等采取的安全措施。

2. _____简称为 TEMPEST(Transient Electro Magnetic Pulse Emanations Standard Technology)技术。

3. 提高系统可靠性的方法有_____、_____和_____。

4. 物理安全包括_____、_____、_____和_____。

5. 环境安全面临的安全威胁有_____、_____和_____等。

6. 容错技术包括_____、_____、_____和_____。

7. 按照建立容灾系统目标的不同，容灾备份系统可以分为两种：_____和_____。

8. 用于量化描述灾难恢复目标的最常用的恢复目标指标是_____和_____。

9. 硬件冗余的三种基本形式是_____、_____和_____。

10. 软件容错技术的方法主要有_____和_____。

二、简答题

1. 环境可能对计算机安全造成哪些威胁？如何防护？

2. 计算机哪些部件容易产生辐射？如何防护？

3. TEMPEST 技术的主要研究内容是什么？

4. 计算机设备防泄露的主要措施有哪些？它们各自的主要内容是什么？

5. 为了保证计算机安全稳定地运行，对计算机机房有哪些主要要求？机房的安全等级有哪些？根据什么因素划分？

6. 灾难恢复的指标是什么？分别代表什么含义？

7. 国际上如何划分灾难恢复的等级？

8. 按照建立容灾系统目标的不同，容灾备份系统可以分为几种？分别适用于什么场合？