第3章 物理安全威胁与防范

本章将介绍物理安全的基本概念、环境安全威胁与防范、设备安全问题与策略、数据存储介质的安全和物理安全标准。要求学生了解物理安全威胁，并掌握防范方法。

3.1 物理安全概述

本节将介绍物理安全的基本概念，威胁和防范策略。其中包括机房安全，设备安全和存储安全。

3.1.1 物理安全概念

1. 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了信息系统的可靠性，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，保障物理设备安全的第一道防线。物理安全会导致系统存在风险。例如，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致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。

设备安全技术主要是指保障构成信息网络的各种设备、网络线路、供电连接、各种媒体数据本身以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。所有的物理设备都是运行在一定的物理环境之中的。

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、电磁防护和线路安全等。

2. 分类

(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的安全。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、可用性三方面,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。

3.1.2　物理安全的定义

1. 信息系统物理安全

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)、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。

3.2　环境安全威胁与防范

环境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。这部分的防范主要是要采取的方法和策略。

3.2.1 物理安全威胁与防范

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和人为干扰。自然环境包括地震、水灾和火灾等自然灾害。人为环境包括静电、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，防御工作做得好与否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。雷电是一种伴有闪电和雷鸣的放电现象。产生雷电的条件是雷雨云中有积累并形成极性。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。人类能够对火进行利用和控制是文明进步的一个重要标志。但是，失去控制的火就会给人类造成灾难。机房发生火灾一般是由于电器原因、人为事故或外部火灾蔓延引起的。电器设备和线路因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎，吸烟、乱扔烟头等，使存在易燃物质(如纸片、磁带和胶片等)的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。火灾防范的关键是提高人们的安全意识。

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，加强外部的物理保护，如专用间、围栏和保护外壳等。

(3) 静电。静电是由物体间的相互摩擦、接触而产生的，物联网设备也会产生很强的静

电。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器损坏，这种损坏可能是不知不觉造成的。

（4）电磁泄漏。电子设备在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、磁屏蔽和电磁屏蔽三种类型。

3.2.2　外界干扰与抗干扰

物联网系统的外部干扰主要集中在数据采集这个阶段，也就是感知器件的外部干扰。因此，物联网数据采集器部分抗干扰将是讨论的重点。

1. 数据采集的外界干扰

1）干扰的定义

干扰是指对系统的正常工作产生不良影响的内部或外部因素。从广义上讲，机电一体化系统的干扰因素包括电磁干扰、温度干扰、湿度干扰、声波干扰和振动干扰等。在众多干扰中，电磁干扰最为普遍，且对控制系统影响最大，而其他干扰因素往往可以通过一些物理的方法较容易地解决。

电磁干扰是指在工作过程中受环境因素的影响，出现的一些与有用信号无关的，并且对系统性能或信号传输有害的电气变化现象。这些有害的电气变化现象使得信号的数据发生瞬态变化，增大误差，出现假象，甚至使整个系统出现异常信号而引起故障。例如传感器的导线受空中磁场影响产生的感应电势会大于测量的传感器输出信号，使系统判断失灵。

2）形成干扰的三个要素

干扰的形成包括三个要素：干扰源、传播途径和接受载体。三个要素缺少任何一项干扰都不会产生。

（1）干扰源。产生干扰信号的设备被称作干扰源，如变压器、继电器、微波设备、电机、无绳电话和高压电线等都可以产生空中电磁信号。当然，雷电、太阳和宇宙射线属于干扰源。

（2）传播途径。是指干扰信号的传播路径。电磁信号在空中直线传播，并具有穿透性的传播叫做辐射方式传播，电磁信号借助导线传入设备的传播被称为传导方式传播。传播途径是干扰扩散和无所不在的主要原因。

（3）接受载体。是指受影响设备的某个环节吸收了干扰信号，转化为对系统造成影响的电器参数。接受载体不能感应干扰信号或弱化干扰信号，使其不被干扰影响就提高了抗干扰的能力。接受载体的接受过程又称为耦合，耦合分为传导耦合和辐射耦合两类。传导耦合是指电磁能量以电压或电流的形式通过金属导线或集总元件（如电容器、变压器等）耦合至接受载体。辐射耦合指电磁干扰能量通过空间以电磁场形式耦合至接受载体。

根据干扰的定义可以看出，信号之所以是干扰因为它对系统造成了不良影响，反之则不能称其为干扰。从形成干扰的要素可知，消除三个要素中的任何一个都会避免干扰。抗干扰技术就是针对三个要素的研究和处理。

3）电磁干扰的种类

物联网系统工作时产生的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

成系统信息泄露。外界的电磁干扰也能使物联网系统工作不正常，甚至瘫痪。必须通过屏蔽、隔离、滤波、吸波和接地等措施提高计算机网络系统的抗干扰能力，使之能抵抗强电磁干扰；同时将物联网的电磁泄漏发射降到最低。物联网系统和其他电子设备一样，工作时要产生电磁发射，电磁发射可被高灵敏度的接收设备接收并进行分析、还原，造成系统信息泄露。另一方面，物联网系统又处在复杂的电磁干扰的环境中，这种电磁干扰有时很强，使物联网系统不能正常工作，甚至被摧毁。电磁防护的措施有两类：一类是对传导发射的防护，主要采取对电源线和信号加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；另一类是对辐射的防护，这类防护措施又可以分为以下两种：一种是采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；另一种是干扰的保护措施，即在计算机系统工作的同时，利用干扰装置产生一种与物联网系统辐射相关的伪噪声向空气辐射来掩盖物联网系统的工作频率和信息特征。

按干扰的耦合模式分类，电磁干扰包括下列类型：

(1) 静电干扰。大量物体表面都有静电电荷存在，特别是含电气控制的设备，静电电荷会在系统中形成静电电场。静电电场会引起电路的电位发生变化，通过电容耦合产生干扰。静电干扰还包括电路周围物件上积聚的电荷对电路的泄放，大载流导体(输电线路)产生的电场通过寄生电容对机电一体化装置传输的耦合干扰等。

(2) 磁场耦合干扰。大电流周围磁场对机电一体化设备回路耦合形成的干扰。动力线、电动机、发电机、电源变压器和继电器等都会产生这种磁场。产生磁场干扰的设备往往同时伴随着电场的干扰，因此又统一称为电磁干扰。

(3) 漏电耦合干扰。绝缘电阻降低而由漏电流引起的干扰。多发生于工作条件比较恶劣的环境或器件性能退化、器件本身老化的情况下。

(4) 共阻抗干扰。共阻抗干扰是指电路各部分公共导线阻抗、地阻抗和电源内阻压降相互耦合形成的干扰。这是机电一体化系统普遍存在的一种干扰。

(5) 电磁辐射干扰。由各种大功率高频、中频发生装置、各种电火花以及电台电视台等产生高频电磁波向周围空间辐射，形成电磁辐射干扰。雷电和宇宙空间也会有电磁波干扰信号。

4) 干扰存在的形式

在电路中，干扰信号通常以串模干扰和共模干扰形式与有用信号一同传输。

(1) 串模干扰是叠加在被测信号上的干扰信号，也称为横向干扰。产生串模干扰的原因有分布电容的静电耦合，长线传输的互感，空间电磁场引起的磁场耦合，以及 50Hz 的同频干扰等。

(2) 共模干扰往往是指同时加载在各个输入信号接口端的共有信号干扰。

2. 数据采集外界抗干扰措施

为了提高电子设备的抗干扰能力，除了在芯片、部件上提高抗干扰能力外，主要的措施有屏蔽、隔离、滤波、吸波和接地等，其中屏蔽是应用最多的方法。

提高抗干扰的措施最理想的方法是抑制干扰源，使其不向外产生干扰或将其干扰影响限制在允许的范围之内。由于车间现场干扰源的复杂性，要想对所有的干扰源都做到使其不向外产生干扰几乎是不可能的，也是不现实的。另外，来自于电网和外界环境的干扰，机

电一体化产品用户环境的干扰也是无法避免的。因此，在产品开发和应用中，除了对一些重要的干扰源，主要是对被直接控制的对象上的一些干扰源进行抑制外，更多的则是在产品内设法抑制外来干扰的影响，以保证系统可靠地工作。抑制干扰的措施很多，主要包括屏蔽、隔离、滤波、接地和软件处理等方法。

1）屏蔽

屏蔽是利用导电或导磁材料制成的盒状或壳状屏蔽体，将干扰源或干扰对象包围起来从而割断或削弱干扰场的空间耦合通道，阻止其电磁能量的传输。屏蔽可以有效地抑制电磁信息向外泄露，衰减外界电磁干扰，保护内部的设备、器件或电路，使其能在恶劣的电磁环境下正常工作。按需屏蔽的干扰场性质不同，可分为电场屏蔽、磁场屏蔽和电磁场屏蔽。平时所说的屏蔽一般指电磁屏蔽。还有几种特殊的屏蔽措施，如金属板屏蔽、金属栅网屏蔽、多层屏蔽、薄膜屏蔽也能达到预期效果。

（1）电场屏蔽。为了消除或抑制由于电场耦合引起的干扰。通常用铜和铝等导电性能良好的金属材料作屏蔽体，屏蔽体结构应尽量完整严密并保持良好的接地。

（2）磁场屏蔽。为了消除或抑制由于磁场耦合引起的干扰。对静磁场及低频交变磁场，可用高磁导率的材料作屏蔽体来保证磁路畅通。对高频交变磁场，主要靠屏蔽体壳体上感生的涡流所产生的反磁场起排斥原磁场的作用。选用材料也是良导体，如铜、铝等。

2）隔离

隔离是指把干扰源与接收系统隔离开来，使有用信号正常传输，而干扰耦合通道被切断，达到抑制干扰的目的。常见的隔离方法有光电隔离、变压器隔离和继电器隔离。

（1）光电隔离。光电隔离是以光作为媒介在隔离的两端进行信号传输，所用的器件是光电耦合器。由于光电耦合器在传输信息时不是将其输入和输出的电信号进行直接耦合，而是借助于光作为媒介物进行耦合，因而具有较强的隔离和抗干扰能力。

（2）变压器隔离。对于交流信号的传输一般使用变压器隔离干扰信号的办法。隔离变压器也是常用的隔离部件，用来阻断交流信号中的直流干扰，抑制低频干扰信号的强度，并把各种模拟负载和数字信号源隔离开来。传输信号通过变压器获得通路，而共模干扰由于不能形成回路而被抑制。

（3）继电器隔离。继电器线圈和触点仅在机械上形成联系，而没有直接的联系，因此可利用继电器线圈接收电信号，利用其触点控制和传输电信号，从而实现强电和弱电的隔离。同时，继电器触点较多，其触点能承受较大的负载电流，因此应用非常广泛。

3）滤波

滤波是抑制干扰传导的一种重要方法。由于干扰源发出电磁干扰频谱往往比要接收的信号的频谱宽得多，因此当接收器接收有用信号时，也会接收到那些不希望有的干扰。这时可以采用滤波的方法，只让所需要的频率成分通过，而将干扰频率成分加以抑制。

常用滤波器根据其频率特性又可分为低通、高通、带通和带阻等。低通滤波器只让低频成分通过，而高于截止频率的成分则受抑制、衰减，不让通过。高通滤波器只通过高频成分，而低于截止频率的成分则受抑制、衰减，不让通过。带通滤波器只让某一频带范围内的频率成分通过，而低于下截止和高于上截止频率的成分均受抑制，不让通过。带阻滤波器只抑制某一频率范围内的频率成分，不让其通过，而低于下截止和高于上截止频率的频率成分则可通过。

4）接地

将电路、设备机壳等与作为零电位的一个公共参考点（大地）实现低阻抗的连接，称之为接地。接地的目的有两个：一是为了安全，例如把电子设备的机壳、机座等与大地相接，当设备中存在漏电时，不致影响人身安全，称为安全接地；二是为了给系统提供一个基准电位，例如脉冲数字电路的零电位点等，或为了抑制干扰，如屏蔽接地等。

5）软件抗干扰设计

（1）软件滤波。用软件来识别有用信号和干扰信号，并滤除干扰信号的方法称为软件滤波。识别信号的原则有三种：

① 时间原则。如果掌握了有用信号和干扰信号在时间上出现的规律性，在程序设计上就可以在接收有用信号的时区打开输入口，而在可能出现干扰信号的时区封闭输入口，从而滤掉干扰信号。

② 空间原则。在程序设计上为保证接收到的信号正确无误，可将从不同位置、用不同检测方法、经不同路线或不同输入口接收到的同一信号进行比较，根据既定逻辑关系来判断真伪，从而滤掉干扰信号。

③ 属性原则。有用信号往往是在一定幅值或频率范围的信号，当接收的信号远离该信号区时，软件可通过识别予以剔除。

（2）软件“陷阱”。从软件的运行来看，瞬时电磁干扰可能会使 CPU 偏离预定的程序指针，进入未使用的 RAM 区和 ROM 区，引起一些莫名其妙的现象，其中死循环和程序“飞掉”是常见的。为了有效地排除这种干扰故障，常用软件“陷阱法”。这种方法的基本指导思想是把系统存储器（RAM 和 ROM）中没有使用的单元用某一种重新启动的代码指令填满，作为软件“陷阱”，以捕获“飞掉”的程序。一般当 CPU 执行该条指令时，程序就自动转到某一起始地址，而从这一起始地址开始存放一段使程序重新恢复运行的热启动程序，该热启动程序扫描现场的各种状态，并根据这些状态判断程序应该转到系统程序的哪个入口，使系统重新投入正常运行。

（3）软件“看门狗”。“看门狗（WATCHDOG）”就是用硬件（或软件）的办法要求使用监控定时器定时检查某段程序或接口，当超过一定时间系统没有检查这段程序或接口时，可以认定系统运行出错（干扰发生），可通过软件进行系统复位或按事先预定方式运行。“看门狗”是工业控制机普遍采用的一种软件抗干扰措施。当侵入的尖锋电磁干扰使计算机“飞程序”时，WATCHDOG 能够帮助系统自动恢复正常运行。

3.2.3 机房安全

1. 机房安全要求

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、噪音干扰、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，主要分为温度、电源、地板、监控等方面。

（1）温度。说到温度，一般用的都是空调了。空调用来控制数据中心的温度和湿度，制

冷与空调工程协会的“数据处理环境热准则”建议温度范围为 20℃～25℃(68℉～75℉),湿度范围为 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在制造商规定的温度/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,可能导致静电放电问题,可能会损坏元器件。

(2) 电源。机房的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。为了避免出现单点故障,所有电力系统,包括备用电源都是全冗余的。对于关键服务器来说,要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 8 小时或更长时间。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(2 英尺),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。计算机机柜往往被组织到一个热通道中,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,例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,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 GB 9361—88 的 B 类机房要求;B 级和 C 级信息系统机房应符合 GB 9361—88 的 A 类机房要求。

在设计时应对供配电方式、空气净化、安全防范措施以及防静电、防电磁辐射和抗电磁干扰、防水防潮、防雷击、防火防尘等诸多方面给予高度的重视。要符合安全可靠、应用灵活、管理科学等几个方面的基本要求,在方案设计论证时应严格按照国家相关标准执行,在机房设计中首先要依据相关标准确定机房的建设等级、安全等级、风险等级,然后根据各个等级所需要达到的设计要求进行各子系统的专业设计。机房建设主要涉及:

(1) 机房装饰。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。供电系统、配电系统、照明、应急照明、UPS 电源。

(3) 空调新风系统。机房精密空调、新风换气系统。

(4) 消防报警系统。消防报警、手提式灭火器。

(5) 防盗报警系统。红外报警系统。

(6) 防雷接地系统。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：门禁、视频。

(8) 机房动力环境监控系统：机房环境监控系统。

3.3 设备安全问题与策略

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、各种媒体数据本身以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。

3.3.1 设备安全问题与防范

1. 设备安全问题

这里的设备指物联网系统中的物理设备或一个子系统，不是指小的元器件。它是指由集成电路、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。

物联网设备的安全主要是设备被盗、设备被干扰、设备不能工作、人为损坏、设备过时等问题。

(1) 设备被盗。很多电子设备价值不菲，这会导致一些不法分子有盗窃的动机。

(2) 设备被干扰。外界对设备的干扰很多，前面已经介绍。

(3) 设备不能工作。任何设备都有坏的时候，设备不能工作也很正常。

(4) 人为损坏。这种情况有两种可能：一是有意破坏，起因是有人蓄意破坏设备，致使设备不能工作；二是工作人员因为操作失误，无意识地导致设备的损坏。

(5) 设备过时。电子设备升级很快，尽管设备依然可以使用，但是因为设备已经过时，已经无法胜任新的工作。

2. 设备安全策略

前面已经介绍了防盗和设备抗干扰问题。设备不能工作、人为损坏、设备过时等问题可采用以下方法：

(1) 设备改造。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。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。也称为双工，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。

3.3.2　通信线路安全

1. 线路安全威胁

线路物理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。例如，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. 线路安全的对策

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，或线路被损坏。

3.4　数据存储介质的安全

本节将介绍数据安全的威胁和数据安全的核心技术。

3.4.1　数据安全的威胁

1. 数据安全威胁

硬件故障占所有数据意外故障一半以上，常有雷击、高压、高温等造成的电路故障，高温、振动碰撞等造成的机械故障，高温、振动碰撞、存储介质老化造成的物理坏磁道扇区故障，当然还有意外丢失损坏的固件 BIOS 信息等。威胁数据安全的因素有很多，主要有以下几个：

（1）硬盘驱动器损坏。一个硬盘驱动器的物理损坏意味着数据丢失。设备的运行损耗、存储介质失效、运行环境以及人为的破坏等都能给硬盘驱动器设备造成影响。

（2）光盘损坏。因为光盘表面介质的质量问题，或人为划伤光盘表面，或光盘被压破裂

等都会使光盘损坏数据不能读出。这种损坏几乎不可修复。

(3) U 盘损坏。物理损坏指的是 U 盘受到外界破坏。例如外壳破损,芯片外表损坏。如是外壳损坏,芯片没事的话,这个是没有问题的。插入计算机还是会显示的。如是芯片损坏的,从外表上是看不出的。那就不是物理损坏,而是彻底损坏。

(4) 信息窃取。从电子设备上非法复制信息。

(5) 自然灾害。包括地震、水灾、火灾等自然灾难。

(6) 电源故障。电源供给系统故障,一个瞬间过载电功率会损坏在硬盘或存储设备上的数据。

(7) 磁干扰。磁干扰是指重要的数据接触到有磁性的物质会造成数据丢失。

2. 数据安全保护

数据安全的定义是为数据处理系统建立和采用的技术和管理的安全保护,保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。确保网络数据的可用性、完整性和保密性。

信息存储操作在生活和工作中越来越多,也越来越重要。为防止电子设备中的数据意外丢失,一般都采用许多重要的安全防护技术来确保数据的安全。下面是常用的数据安全防护技术:

(1) 磁盘阵列。磁盘阵列是指把多个类型、容量、接口甚至品牌一致的专用磁盘或普通硬盘连成一个阵列,使其以更快的速度、准确、安全的方式读写磁盘数据,从而达到数据读取速度和安全性的一种手段。

(2) 数据备份。备份管理包括备份的可计划性,自动化操作,历史记录的保存或日志记录。

(3) 双机容错。双机容错的目的在于保证系统数据和服务的在线性,即当某一系统发生故障时,仍然能够正常地向网络系统提供数据和服务,使得系统不至于停顿,双机容错的目的在于保证数据不丢失和系统不停机。

(4) 网络存储技术 NAS。NAS 解决方案通常配置为作为文件服务的设备,由工作站或服务器通过网络协议和应用程序进行文件访问,大多数 NAS 链接在工作站客户端和 NAS 文件共享设备之间进行。

(5) 数据迁移。由在线存储设备和离线存储设备共同构成一个协调工作的存储系统,该系统在在线存储和离线存储设备间动态地管理数据,使得访问频率高的数据存放于性能较高的在线存储设备中,而访问频率低的数据存放于较为廉价的离线存储设备中。

(6) 异地容灾。以异地实时备份为基础的高效、可靠的远程数据存储,在各单位的 IT 系统中必然有核心部分,通常称为生产中心,往往给生产中心配备一个备份中心,该备份中心是远程的,并且在生产中心的内部已经实施了各种各样的数据保护。不管怎么保护,当火灾、地震这种灾难发生时,一旦生产中心瘫痪了,备份中心会接管生产,继续提供服务。

(7) 存储区域网络 SAN。它是一个集中式管理的高速存储网络,由多个供应商存储系统、存储管理软件、应用程序服务器和网络硬件组成 SAN。SAN 允许服务器在共享存储装置的同时仍能高速传送数据。这一方案具有带宽高、可用性高、容错能力强的优点,而且它可以轻松升级,容易管理,有助于改善整个系统的总体成本状况。

3.4.2 数据安全的核心技术

数据存储安全是数据安全的一部分，其目的是防止其他系统未经授权访问数据，或破坏数据。存储设备有能力防止未被授权的设置改动，对所有的更改都要做审计跟踪。数据存储的安全目标是保护机密的数据，确保数据的完整性，防止数据被破坏或丢失。未来存储安全的核心是以数据恢复为主，兼顾数据备份、数据擦除。

1. 数据恢复

数据恢复只是一种技术手段，将保存在计算机、笔记本、服务器、存储磁带库、移动硬盘、U 盘、数码存储卡和 MP3 等设备上丢失的数据进行抢救和恢复的技术。具体方法有：

(1) 硬件故障的数据恢复。首先是诊断，找到问题点，修复相应的硬件故障，然后进行数据恢复。

(2) 磁盘阵列(RAID)数据恢复。首先是排除硬件故障，然后分析阵列顺序、块大小等参数，用阵列卡或阵列软件重组，按常规方法恢复数据。

(3) U 盘数据恢复。U 盘、优盘、XD 卡、SD 卡、CF 卡、MEMORY STICK、SM 卡、MMC 卡、MP3、MP4、记忆棒、数码相机、DV、微硬盘、光盘和软盘等各类存储设备数据介质损坏或出现电路板故障、磁头偏移、盘片划伤等情况下，采用开体更换、加载和定位等方法进行数据修复。

灾难恢复则是一套完整的数据恢复的系统方案。其先决条件是要做好备份策略及恢复计划。日常备份制度描述了每天的备份以什么方式、使用什么备份介质进行，是系统备份方案的具体实施细则，在制定完毕后，应严格按照制度进行日常备份，否则将无法达到备份方案的目标。数据备份有多种方式，以磁带机为例，有全备份、增量备份和差分备份等。

2. 数据备份

1) 数据丢失的问题

2001 年 9 月 11 日，当世界贸易中心大楼倒塌而灰飞烟灭时，整个大楼计算机系统里存储的大量信息也随之丢失，众多公司因此而无法开展自己业务。2004 年 12 月 27 日，因为强烈地震，东南亚出现了海啸，受灾严重地区的金融、保险、能源、交通、电信等关乎国计民生的行业的信息系统几乎陷入瘫痪，大量信息系统的数据丢失。数据安全已经成为现实而又严峻的问题。当今的信息化社会，计算机和通信技术在信息的收集、处理、存储、传输和分发中扮演着极其重要的角色，与此同时，如何有效保护信息系统里存储的信息是必须面对的一个新问题。

2) 数据备份的概念

在这种情况下，数据备份就成为保证信息系统安全的基础设施。所谓数据备份就是将数据以某种方式加以保留，以便在系统遭受破坏或其他特定情况下重新加以利用的一个过程。不仅在于保证数据的一致性和完整性防范意外事件的破坏消除系统使用者和操作者的后顾之忧，而且还是历史数据保存归档的最佳方式，换言之，即便系统正常工作而没有任何数据丢失或破坏发生，备份工作仍然具有非常大的意义。

3）数据存储管理

网络数据存储管理系统是指在分布式网络环境下，通过专业的数据存储管理软件，结合相应的硬件和存储设备，对全网络的数据备份进行集中管理，从而实现自动化的备份、文件归档、数据分级存储以及灾难恢复等。

为在整个网络系统内实现全自动的数据存储管理，备份服务器、备份管理软件与智能存储设备的有机结合是这一目标实现的基础。网络数据存储管理系统的工作原理是在网络上选择一台应用服务器作为网络数据存储管理服务器，安装网络数据存储管理服务器端软件，作为整个网络的备份服务器。在备份服务器上连接一台大容量存储设备（磁带机或磁带库）。在网络中其他需要进行数据备份管理的服务器上安装备份客户端软件，通过局域网将数据集中备份管理到与备份服务器连接的存储设备上。网络数据存储管理系统的核心是备份管理软件，通过备份软件的计划功能，可为整个部门建立一个完善的备份计划及策略，并可借助备份时的呼叫功能，让所有的服务器备份都能在同一时间进行。备份软件也提供完善的灾难恢复手段，能够将备份硬件的优良特性完全发挥出来，使备份和灾难恢复时间大大缩短，实现网络数据备份的全自动智能化管理。

4）数据备份方案

⑴全备份。所谓全备份就是用一盘磁带对整个系统进行完全备份，包括系统和数据。这种备份方式的好处就是很直观，容易被人理解。而且当发生数据丢失的灾难时，只要用一盘磁带（即灾难发生之前一天的备份磁带）就可以恢复丢失的数据。然而它也有不足之处：首先由于每天都对系统进行完全备份，因此在备份数据中有大量是重复的，例如操作系统与应用程序。这些重复的数据占用了大量的磁带空间，这对用户来说就意味着增加成本；其次，由于需要备份的数据量相当大，因此备份所需时间较长。对于那些业务繁忙，备份窗口时间有限的单位来说，选择这种备份策略无疑是不明智的。

⑵增通备份。就是每次备份的数据只是相当于上一次备份后增加的和修改过的数据。这种备份的优点很明显：投有重复的备份数据，既节省磁带空间，又缩短了备份时间。但它的缺点在于当发生灾难时，恢复数据比较麻烦。举例来说，如果系统在星期四的早晨发生故障，丢失大批数据，那么现在就需要将系统恢复到星期三晚上的状态。这时管理员需要首先找出星期一的那盘完全备份磁带进行系统恢复，然后再找出星期二的磁带来恢复星期二的数据，最后再找出星期三的磁带来恢复星期三的数据。很明显这比第一种策略要麻烦得多。另外，这种备份可靠性也差。在这种备份下，各磁带间的关系就像链子一样，一环套一环，其中任何一盘磁带出了问题都会导致整条链子脱节。

⑶差分备份。就是每次备份的数据是相对于上一次全备份之后新增加的和修改过的数据。管理员先在星期一进行一次系统完全备份；然后在接下来的几天里，管理员再将当天所有与星期一不同的数据（新的或经改动的）备份到磁带上。举例来说，星期一，网络管理员按惯例进行系统完全备份；星期二，假设系统内只多了一个资产清单，于是管理员只需将这份资产清单一并备份下来即可；星期三，系统内又多了一份产品目录，于是管理员不仅要将这份目录，还要连同星期二的那份资产清单一并备份下来。

由此可以看出，全备份所需时间最长，但恢复时间最短，操作最方便，当系统中数据量不大时，采用全备份最可靠；差分备份在避免了另外两种策略缺陷的同时，又具有了它们的所有优点。首先，它无须每天都做系统完全备份，因此备份所需时间短，并节省磁带空间；其

次，它的灾难恢复也很方便，系统管理员只需两盘磁带，即星期一的磁带与发生前一天的磁带就可以将系统完全恢复。在备份时要根据它们各自的特点灵活使用。

3．数据擦除

近年来，企事业单位在享受数据中心带来巨大生产力的同时，其内在的数据中心安全漏洞也让人担忧，越来越多的企事业单位投入大量资金着手数据中心安全建设。数据泄密事件的频繁发生更让企业数据中心安全笼罩在阴影中，而对涉密数据进行硬盘数据擦除，以达到硬盘数据销毁，成为当下保障数据中心安全的有效方式之一。

硬盘数据擦除技术旨在通过相关的硬盘数据擦除技术及硬盘数据擦除工具将硬盘上的数据彻底删除，无法恢复。

另外，目前市面上已经出现了很多复制擦除检测一体机品牌产品，它们可以快速擦除硬盘上的数据。硬盘数据销毁速度达7G/分钟，符合7次安全硬盘数据擦除国际标准。硬盘被执行全盘写零擦除后，目前全球无任何专业数据恢复公司有能力再恢复出数据，有效确保企业数据中心安全。

习题3

1．名词解释

(1)物理安全；(2)设备安全技术；(3)数据安全；(4)硬盘数据擦除技术。

2．判断题

(1) 物理安全是以一定的方式运行在一些软件之上的，保障物理设备安全的第一道防线。(　　)

(2) 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。(　　)

3．填空题

(1) 干扰的形成包括三个要素：_____、_____和_____。

(2) 机房的物理环境受到了严格的控制，主要分为_____、_____、_____、_____。

(3) 威胁数据安全的主要因素有很多，主要包括_____、_____、_____、_____。

4．简答题

(1) 数据采集外界抗干扰措施有哪些？

(2) 设备安全策略有哪些？

(3) 常用的数据安全防护技术有哪些？

(4) 简单介绍数据恢复的方法。

5．论述题

国内外物理安全技术相关标准有哪些？