第3章 物理环境与设备安全

随着信息技术的不断发展，物联网、智能家居、无人驾驶等一些“高大上”的词汇愈加频繁地出现在人们的视野当中，而这些新兴的技术，无一不与物理硬件安全密切相关。本章就物理环境和设备安全展开，介绍了当前一些安全研究重点，如工控安全、芯片安全和可信计算。

3.1 物理安全和物理安全管理

本节分为两个主要部分，分别是物理安全和物理安全管理。第一部分介绍了我们所面临的物理威胁，并且提出了相应的解决方案；第二部分给出了两种物理安全管理方法，设备访问控制以及物理访问控制。

3.1.1 物理安全

1. 定义

物理安全又称实体安全，其确保了计算机网络设备、设施和其他媒体的安全和可靠运行，免遭火灾、地震、有害气体等其他环境事故、人为操作失误以及各类计算机网络犯罪行为所造成的破坏的措施和过程，是计算机网络信息系统安全的重要组成部分，是整个系统安全的前提。

2. 物理威胁及其防护

目前，物理安全受到各种各样的威胁，主要威胁包括：日常使用中的设备可能会遇到损毁和破坏，以及面临因电磁泄漏造成的威胁，并且在生活中可能还会遇到相关的电子干扰，更重要的是在外部环境安全中所遭受的危险。

为了有效合理地对物理安全进行保护，需要做出以下的保护措施。

（1）防损毁保护。防损毁的具体措施包括：

- 严格按照规范操作。
- 设备定期检测、维护、保养。
- 制定或者设计病毒防范程序保障计算机系统安全。
- 要求特别保护的设备应与其他设备进行隔离。

（2）防电磁信息泄露。有两种技术方法可以抑制计算机系统中的信息泄露：电子混淆和物理抑制。前者主要是利用干扰、调频等技术掩护计算机的工作状态，保护信息，防止信

息泄露；后者是压制所有有用信息，防止信息泄露。

（3）防电子干扰。对于电子通信设备，若出现电子干扰现象，将严重影响电子通信设备的运行稳定性，降低其运行效率。对应的电子干扰对策包括“同频干扰”和“蓝牙无线电干扰”等。

（4）环境安全防护。环境安全防护要做到防患于未然，首先要注意的是防火，在潮湿天气，还要注意防潮和防雷，针对一些特殊装置，还要防震动和噪声。当然，必要情况下还要考虑防止一些极端自然灾害，例如防地震、水灾等。

3. 安全设备

常见的网络安全设备主要有网络物理安全隔离卡、物理安全隔离网闸、物理安全隔离器等。

本节将主要介绍 PC 网络物理安全隔离卡，它是一种典型的安全设备。它的工作原理是通过单个硬盘上磁道的读写控制技术，将两个工作空间分隔成无法访问的空间。它将一台普通计算机虚拟成两台或三台计算机，实现工作站的双重状态，即安全状态和公共状态，而且这两种状态是绝对隔离的，这样一台工作站就可以在完全安全的状态下连接内部和外部网络。安全隔离卡是在 PC 的物理层面上设置的。内部和外部网络必须通过网络安全隔离卡连接，数据在任何时候都只能通向一个分区。其工作方式如图 3.1 所示。

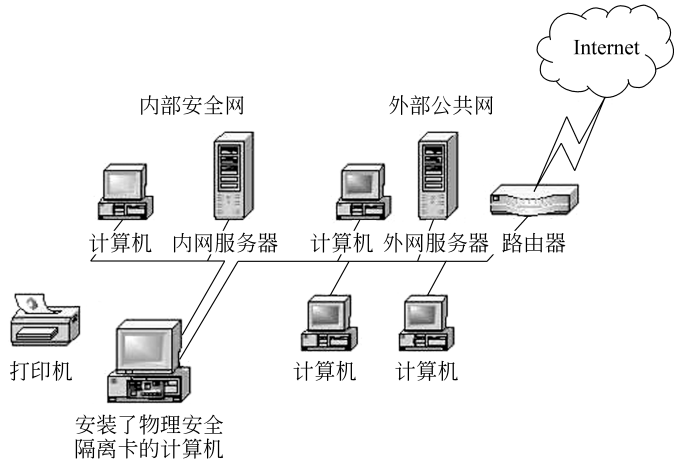

图 3.1　物理安全隔离卡的解决方案

当工作站处于安全状态时，主机只能使用硬盘的安全区域连接到内部网络。此时，外部连接（如 Internet）被断开，硬盘公共区域的通道被关闭；当主机处于公共状态时，主机只能使用硬盘公共区域连接到外部网络。此时，内部网络连接被断开，且硬盘安全区也是被封闭的。

出于安全考虑，两个分区不允许直接交换数据，但硬盘的物理隔离图可以通过独特的设计巧妙地实现数据交换。这意味着在这两个分区旁边的硬盘上设置了另一个功能区。当计算机处于不同的状态时，它的功能区会被转换，这些状态被表示为硬盘的 D 盘。每个分区都可以通过这个功能区实现数据交换。当然，如果有必要，也可以创建一个单向的安全通道，即数据只能从公共区域传输到安全区域，但不能反向传输。

3.1.2 物理安全管理

我们知道，物理安全面临着大量不同的威胁、弱点以及风险，如物理损毁、电磁信息泄露等，这就要求我们有一个高效、便捷的物理安全管理方法。物理安全管理包括设备的安全管理、安全区域的管理等。本节简单介绍一下物理安全管理中最主要的两种方法：设备访问控制和物理访问控制。

设备访问控制是指所有硬件、软件、组织管理策略或程序，它们对访问进行授权或限制，监控和记录访问的企图、标识用户的访问企图，并且确定访问是否经过了授权。

物理访问控制(Physical Access Control)主要是指对进出数据中心、服务器机房、实验室等关键资产运营相关场所的人员进行严格的访问控制。物理访问控制的方法主要有：在机房和数据中心加固更多的围墙和门来抵御威胁；还可以采用专业摄像器材来监控相关设备所在场所；也可以在专门的场所设置警报装置和警报系统来防范威胁；最重要的是，对相关人员要加强安全管理，设置专门的 ID 卡或其他辨明身份的证件。

物理访问控制除了要防范各种威胁，还必须对各种设备增加设备锁来减少损失。例如，对机箱设备、键盘鼠标、计算机桌抽屉等要上锁，以确保即便他人进入房间也无法使用计算机设备；机房钥匙应妥善保管，防止丢失。

3.2 工业控制设备安全

工业控制设备安全，又称 ICS(Industrial Control System)安全。本节主要介绍工业控制设备，分析近些年来工控安全态势、存在的安全威胁及其来源，最后分析安全防护手段等内容。

3.2.1 工控设备简介

工控是指工业自动化控制，主要利用电气手段、电子技术、计算机技术等多项技术和手段共同进行工业制造和生产过程控制的自动化检测、调控、优化和管理，具有精确性、效率性和自动化的特点。工控技术的发展为工业带来第三次革命，极大提高了工业化生产的效率。

目前，工控系统已广泛应用于电站电网、水利工程、石油化工、工业制造和先进制造等各个领域。随着工业技术的发展，工控系统呈现出层次化、网络化的特点。一个完整的工业自动化系统如图 3.2 所示。

“控制设备”是整个工业控制系统的核心组件，负责工业生产运行的实时本地控制。典型控制设备如下。

1. 分布式控制系统(DCS)

又称分散控制系统或集散控制系统，是基于集中控制系统产生的，是一种建立于网络之上，但又不同于集中式控制系统的新型控制系统，具有高内聚和高透明的特点。

2. 可编程控制器(PLC)

一种电子系统，可以执行数字运算操作，被广泛使用于钢铁建材、石油化工、机械制造等

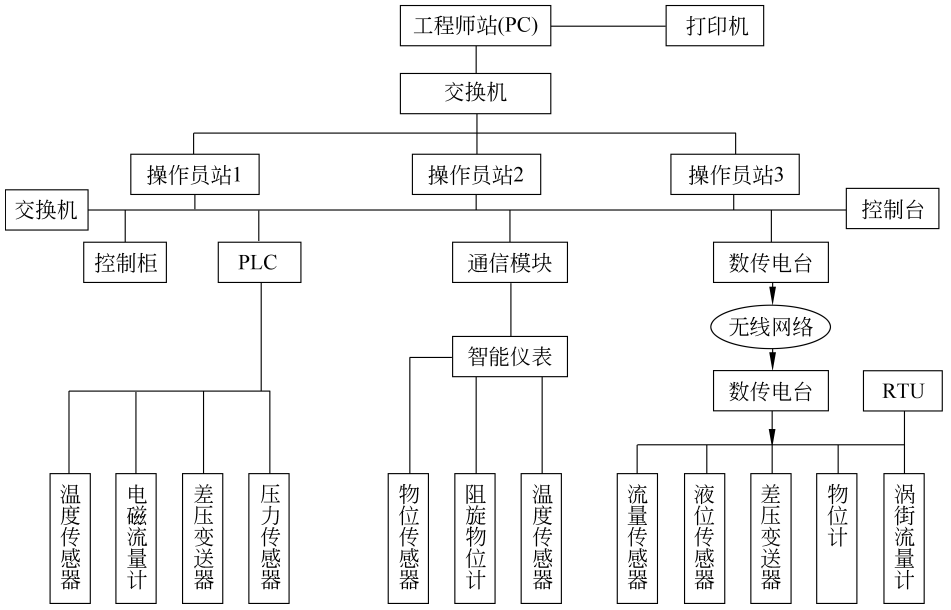

图 3.2　一个完整的工业自动化系统

工业领域。它由微处理器、数据存储器、指令存储器、输入/输出和数字模拟等单元模块化而成，可以通过存储器对指令进行控制、执行运算，通过输入/输出单元的数字模拟接口，控制或监督各种类型的电气系统或生产过程。具有编程方便、维修方便、可靠性高和体积小等特点。

3. 紧急停车系统(ESD)

独立于 DCS，比 DCS 具有更高的响应速度，可以有效避免更多的危险，降低事故造成的损失，保护人员的安全，具有更高的安全性和灵活性。

4. 总线控制系统(FCS)

DCS 的更新换代产品。采用全数字式的信号传输方式，可以对多个过程变量进行传送，提高了检测精度，减少了 I/O 装置，降低了成本。此外，FCS 具有比 DCS 更高的开放性，更彻底的功能分散性以及可互操作性，克服了 DCS 存在的缺点。

5. 智能电子设备(IED)

IEC 61850 标准将 IED 定义为："由一个或多个处理器组成，具有从外部源接收和传送数据或控制外部源的任何设备，即电子多功能仪表、微机保护、控制器，在特定的环境下在接口所限定范围内能够执行一个或多个逻辑接点任务的实体。"

6. 远程终端单元(RTU)

如图 3.2 所示，工业控制设备就是远程终端单元(RTU)。用于远程检测和控制，克服通信距离长和生产环境恶劣的条件限制，采用低功耗设计，集远程数据收集、监控和控制于一体。一般采用工业级设计，具有多功能性、接口多样性、高安全性、高稳定性、易维护性和易用性等特点。

3.2.2 工控安全态势

工控系统安全与国家战略安全密不可分。图 3.3 和图 3.4 展示了 1982—2014 年发生的工控安全事件数量与事件对应的工业行业各自所占的比例，这些安全事件都造成了巨额的经济损失。

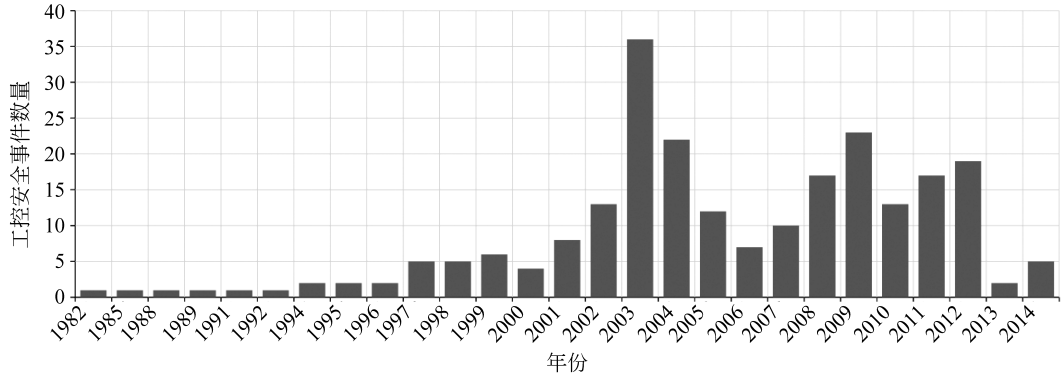

图 3.3 工控安全事件年份统计

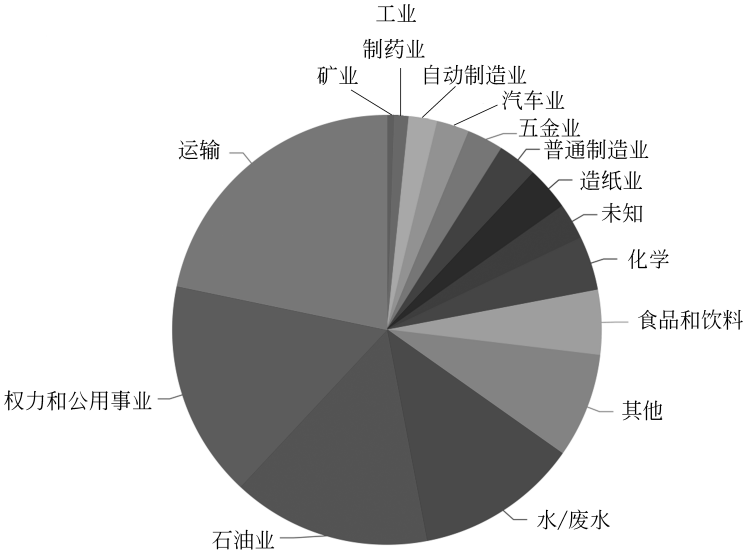

图 3.4 工控安全事件涉及的工业行业统计情况

以伊朗的震网病毒(Stuxnet)为例，2010 年该网络超级病毒肆虐全球工业界，诸多国家基础能源设施均没有躲开病毒的魔爪，即便是科学技术发达的美国也未能幸免，其中伊朗遭受到的病毒攻击最为严重。短时间内威胁到了全球诸多企业的正常运作，部分国家核电站的运作受到了极大威胁，甚至威胁到了国家安全。

工控安全方面的研究，我国呈现出“点状发展，底子薄弱”的特点。过去，点状发展表现为：研究工控安全方面的机构企业较为分散，大多都是单枪匹马，缺少统一的集中指挥与合作。底子薄弱表现为：工控安全方面的研究相对滞后，工控所需的核心设备只能依托进口

而无法掌握在自己手中，多项工控安全研究需要参考国外标准。近年来，随着我国工业技术的飞速发展，国内工控安全方面政策环境持续向好，相关研究初见成效，且处于持续增强的态势，产业规模迅速扩张，工业技术体系日趋完善。

3.2.3 工控安全问题

目前，工业控制设备存在的安全问题主要包括如下。

(1) 身份认证和安全鉴别方面的功能不足或缺失。在开放的工控网络环境中，易遭受伪装攻击，导致工控系统被非授权访问。

(2) 数据保密性和完整性保护功能缺失。攻击者易通过数据截获来获取明文信息。

(3) 访问控制能力不够。

(4) 审计功能缺少安全完备性。

(5) 具有高危安全漏洞且难以在短时间内修补。

(6) 易遭受拒绝服务攻击，严重影响系统实时性。

(7) 存在较多非必要的端口和服务，徒增引发安全问题的可能性和被入侵的攻击面。

除此之外，工业控制设备方面还存在其他的安全问题。

3.2.4 工控安全来源

对于工业控制安全问题的产生，究其根源主要在于以下几方面。

(1) 缺乏工控安全意识。这是导致现有工控系统安全功能缺失或不完善的主要原因，使其在面对攻击时显现出脆弱性。工业控制自动化领域存在重视功能安全而相对忽略信息安全的普遍现象，即“重 Safety 轻 Security”。

工控的 Safety 和 Security 的区别在于：Safety 更加着重于因为硬件故障而引发的一系列安全问题，它面对的主要是突发性硬件或系统故障等。而 Security 还需进一步考虑人为因素所导致的工控安全威胁，如黑客攻击、病毒威胁等。

(2) 工业控制技术正在发展得更加标准通用的同时，也为工控漏洞发现与深入挖掘带来了更多的便利性，这使得攻击者有机可乘，工控的脆弱性也随之显现。

(3) 工控系统网络与企业网乃至是互联网的连接，无疑扩宽了可能遭受网络攻击的攻击面，使得工控设备就犹如待宰的羔羊一般直接需要面临无数可能的各种网络攻击。

(4) 智能化技术的飞速发展在提高工业自动化程度、促进传统工控设备的升级的同时，也带来了额外风险。

(5) 工业环境的独特性使得工控设备的更新或升级相对要慢上一拍，在面对新的安全风险时无法保障系统设备安全。

3.2.5 工控安全防护

对于目前存在的工控安全问题，主要有以下几个防范措施。

(1) 建立更加全面立体的工控安全防御体系，全方位提高工控系统安全性。

(2) 重点加强核心部件的安全管理，对访问控制要进行严格把关。

(3) 针对工控网络的脆弱性加强防护，对 NCU 服务严格控制，设计相应的安全软件。

(4) 加强对工业控制系统的安全运维管理。

(5) 从工控设备的全生命周期不留死角地关注其信息安全,并定期进行风险监测和风险评估,防患于未然。

(6) 建立有效的安全评测机制和安全应急体系。

(7) 增强工控安全意识,既要重视功能安全,同时也不能忽略信息安全的重要性。

2016 年 10 月,工业和信息化部印发《工业控制系统信息安全防护指南》,对各工业企业开展针对工业控制系统的安全防护工作进行了全面的指导。

3.3 芯片安全

集成电路(Integrated Circuit,IC),或称为芯片(Chip),是一种在一个或多个半导体基质上,运用光刻、氧化、外延等特殊工艺将一个具有特定功能的电路所需的电感、电阻、电容和晶体管等元件以及布线互连在一起,而后封装于管壳内的微型电子部件或器件,常常是计算机或其他电子设备的核心部分。

芯片是信息产业的基石,是现代计算机系统硬件和其他电子设备的核心部件,在从个人计算机到大型工控系统的调控和运行过程中,发挥着至关重要的作用,同时也是程序和数据载体,若芯片安全无法得到保障,那么其所承载的程序和数据就会面临安全威胁。当前,芯片不仅广泛应用于生活生产和工业生产各个方面,同时也应用于国防军事、能源、金融经济等领域,一旦受到恶意攻击,可能会对金融安全和国防安全造成严重的损失。

目前,集成电路的主要安全威胁是硬件木马。硬件木马是经有意或者无意植入芯片的缺陷模块,有时也叫恶意电路。

我国芯片制造产业面临芯片制造基础薄弱、核心技术缺失、技术人才匮乏等难题,自产半导体芯片无法供应国内市场的芯片需求,呈现出“供不应求”的现象,大部分芯片需求需要通过进口满足,安全方面存在重大隐患。

本节介绍芯片制造过程、芯片安全事件、芯片面临的安全威胁、硬件木马的分类及防护等内容。

3.3.1 芯片制造过程

集成电路制造过程包含 5 个主要部分:设计、版图生成、制造、封装以及测试。具体又可以细分为可信阶段、半可信阶段、不可信阶段,可由图 3.5 表示。

可以看出,在集成电路的生产过程中,大多数阶段并不是可信的,这就带来了很多安全隐患,特别是对那些无法自主研发芯片的国家,几乎是将其网络空间安全全部交给了芯片制造厂商。

3.3.2 芯片安全事件

近十几年来,针对芯片安全的事件愈发严重,其影响之广几乎可以涉及社会的各个层面。

2005 年,美国国防报告指出集成电路供应中可能会存在安全问题,这是由于生产过程

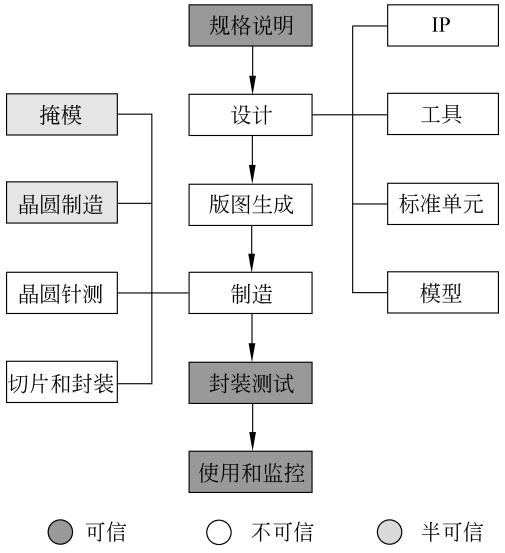

图 3.5　集成电路制造流程

与 IC 设计分离所引起的;同年,还有希腊首相及其诸多官员手机遭窃听事件。

2007 年 9 月,叙利亚最先进的雷达未能检测出以色列的喷气战斗机,导致其东北部一处疑似核设施被轰炸。该雷达未能提前预警的问题受到了各方的关注和讨论,有观点指出,叙利亚雷达的芯片可能被植入了“病毒”或者“后门电路”。攻击者通过对芯片植入的“病毒”进行编程控制,破坏集成电路的功能,从而影响雷达的正常运作。

2010 年,戴尔公司对其用户发布警告称部分出售的 PowerEdge 服务器主板存在恶意程序代码。近几年来,就连英特尔、苹果、微软等知名公司也陆续承认他们生产的芯片存在漏洞,并加紧研发安全补丁。包括近年爆出的 Meltdown 和 Spectre 这两个 CPU 漏洞,都极大威胁了用户的隐私安全。类似的安全事件屡见不鲜,但是更多的漏洞其实还不为人们所知。

3.3.3　芯片安全威胁

目前,集成电路主要面临以下 3 方面安全威胁。

首先是硬件木马,这也是芯片最主要的安全威胁来源。硬件木马指芯片中具有恶意功能的程序代码或者冗余电路,能够篡改电路信息、破坏电路功能、窃取数据信息等。

其次是芯片来源的问题。IC 可能是来自非法制造商产出的赝品 IC,即伪造 IC;也可能来自制造商非法产出的过量制造的 IC 和产出的有漏洞的 IC。这些 IC 不符合生产标准,但是外观上与标准 IC 一致。目前业界已经有相对较为完备的手段来检测伪造 IC,但是伪造 IC 的发展十分迅速,伪造手段也不断升级,这对芯片安全研究人员将是一个重大的挑战。

最后是逆向工程的问题。主要是对 IC 制造过程进行逆向研究和分析,推导出 IC 设计原理来获取一些关键信息或敏感信息。

这 3 种威胁都具有低成本、易实现、难防护等特点,严重威胁着知识产权和信息的安全。

其中，赝品 IC 虽然在性能、质量、使用周期等方面不及正规 IC，但仍可以“放心”使用；逆向工程主要涉及知识产权保护问题；硬件木马是更为主要的芯片安全威胁，部分潜伏于 IC 中的硬件木马难以被检测出来，其主要原因有以下三点。

(1) 随着 IC 的不断发展，其集成度和复杂度的提高导致传统的功能、逻辑测试方法越来越难以满足高精度硬件木马检测要求。

(2) 硬件木马影响和工艺噪声扰动十分相近，且规模较小，难以被有效区分。

(3) 目前硬件木马种类繁多、负面功能各不相同，没有通用的防护技术手段来对芯片进行保护。

前文提到硬件木马是芯片最主要的安全威胁。下面就硬件木马的分类进行讨论。

3.3.4 硬件木马分类

关于硬件木马，可以从很多角度对它进行分类。Wang、Tehranipoor 和 Plusquellic 首次提出了详尽的硬件木马分类方法。基于芯片结构和功能可能存在多张形式的恶意修改，该分类方法主要考虑物理特征、激活特征和行为特征，分别在这三种特征下对木马进行分类，如图 3.6 所示。尽管硬件木马可能有多种分类特征(例如，木马可能包含多种激活特征)，但该方法仍然能够体现木马的基本特征，并且有助于定义和评估木马的检测策略。目前行业内缺少评估木马检测方法有效性的度量标准，Wang 等提出的该分类方法能够让研究人员针对不同类的木马来验证木马检测方法。

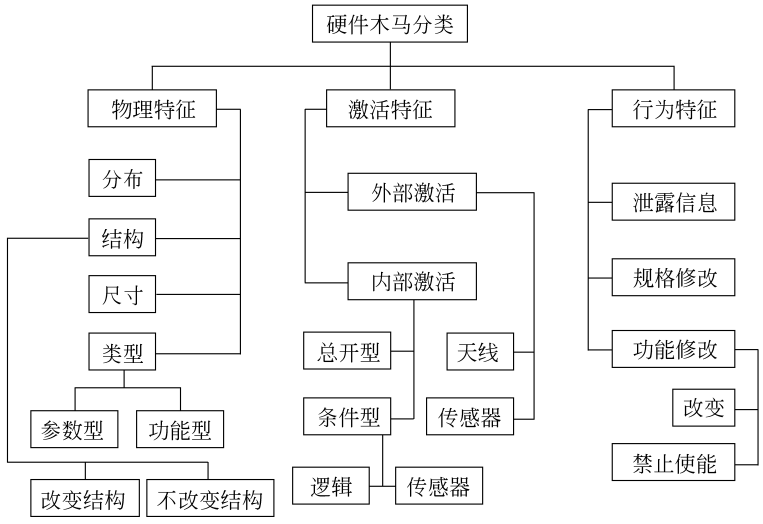

图 3.6 硬件木马分类

物理特征分类描述了木马的多种外部特征。该分类将木马分为功能类和参数类两类。功能类指那些在物理上增加或减少晶体管或门电路而实现的木马，而参数类是指通过修改既有线路和逻辑来实现的木马。

激活特征是指能使木马激活并实施破坏功能的条件。木马激活特征被分为两类：外部激活(例如，被与外部世界相互影响的天线或传感器激活)和内部激活(通常被进一步分为总开型和条件型)，如图 3.6 所示。“总开型”(亦称常开型)是指木马始终处于活跃状态，它能

够在任何时候中断芯片功能。该分类的木马能通过修改芯片的几何结构来实现，使得某个节点或者路径对故障有很高的敏感性。“条件型”是指在特定条件下才激活的木马。激活条件可以基于传感器的输出，也可以基于内部逻辑状态（例如，某个特定的输入模式，或者某个内部计数器的值）。

行为特征描述了木马所造成的破坏行为类型。如图 3.6 所示的分类方案中，将木马行为分为三类：泄露信息、规格修改和功能修改。泄露信息类是指给敌方发送关键信息的木马。规格修改类指的是改变芯片参数性能的木马。功能修改类指的是通过增加、移除或绕过现有逻辑来改变芯片功能的木马。

3.3.5 硬件木马防护

这里从整个集成电路生产过程去考虑防范木马的手段。

如图 3.7 所示，在 IC 测试阶段，检测方式可划分为破坏性和非破坏性。

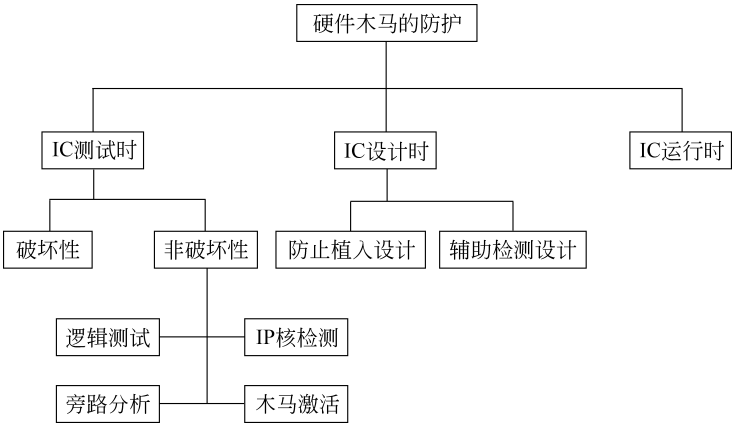

图 3.7 硬件木马防护手段

破坏性检测利用逆向技术重构电路结构图，对比电路需求，判断其中是否含有硬件木马，这种方法会对电路本身造成破坏，并且耗时长，但是可以获得绝对不包含木马的“金片”。

非破坏性检测是将待检测芯片的各项数据与金片的数据对比，比如旁路分析中通过测试电路未激活时，各部分的温度与金片的温度对比，找出不同部分，但是这种方法容易受到工业噪声的影响，并且需要绝对安全的芯片。

在 IC 设计时，增加辅助检测功能或者某些功能可以有效防止集成电路在生产过程中被植入恶意程序段，不过这往往伴随芯片生产规格和生产成本的增加。

防止集成电路在生产过程中被植入恶意程序段，还可以通过在 IC 设计阶段添加一些功能实现，不过会增加其生产成本和规格。

最后是在 IC 运行时，可以通过编程的手段，实现类似于软件木马查杀的方法来检测硬件木马，但是由于硬件木马的种类繁多，并且，并不是所有木马在集成电路运行时都马上运行的，本身硬件木马激活的概率就很小，所以，这种方法可行性还有待加强。

3.4 可信计算

可信计算是一项新型的信息安全技术，具有高度可靠性，同时在信息安全领域研究中一个热门的研究分支便是可信计算。在近些年来，虽然可信计算领域的相关工作取得了不错的进展，但是其仍然有着许多亟待解决的关键技术问题。

本节将介绍一些可信计算的基本概念及其关键技术，并简单介绍一下可信技术目前的应用。

3.4.1 可信计算的出现

20 世纪 30 年代，英国发明家、计算机先驱 Babbage 的论文首次提出了“可信计算”一词。20 世纪 60 年代，可信概念开始萌芽，研究人员设计出了可信电路。20 世纪 70 年代，有关可信系统的概念被提出，并为今后可信计算的出现奠定了坚实的基础。1985 年，由美国国防部(DoD)颁布了计算机系统安全评估的第一个正式标准——《可信计算机系统评价标准》，即 TCSEC 准则，其标志着可信计算的出现。此后，信息安全领域掀起了关于可信计算的研究热潮。

20 世纪 90 年代，随着科学研究体系化发展，可信计算组织和标准逐渐形成体系化并完善。1992 年，Laprie 对可信性进行了系统性阐述，丰富了“可信”的内涵。1999 年，由 IBM、英特尔和微软等科技巨头公司组织成立了可信计算平台联盟(Trusted Computing Platform Alliance，TCPA)。2003 年，TCPA 又改组成可信计算组织(Trusted Computing Group，TCG)。TCPA 和 TCG 制定了一系列有关于可信计算的技术规范行为，并对这一系列技术规范不断进行升级和完善，此举也促进了可信计算研究的良好发展。

21 世纪初期，我国也开始关注可信计算的相关领域研究。同一时期，由武汉瑞达和武汉大学合作，在 2004 年研制开发出了中国第一款可信平台模块(Trusted Platform Module，TPM)。此后，联想、长城等基于 TPM 生产了相关的可信个人计算机。同年，中国首届 TCP 论坛和中国可信计算与信息安全第一届学术会议均在武汉顺利召开。在随后一年，国家正式出台了“十一五”规划和“863”计划，并正式把“可信计算”列入重点支持科研项目。在此之后，我国出现了一系列有关可信计算的产品。在国家科技部等国家部门以及国家颁布的鼓励可信计算研究政策的支持下，我国可信计算事业迎来了“春天”。

可信计算是在为提高硬件安全性的背景之下提出的。可信计算是通过建立一种特定的完整性度量机制，使计算平台运行时具备分辨可信程序代码与不可信程序代码的能力，从而对不可信的程序代码建立有效的防止方法和措施。

3.4.2 概念与标准体系

1. 基本概念

现阶段“可信度”有多种定义。

国际标准化组织(International Organization for Standardization)和国际电子技术委员会(ISO/IEC)在目录服务系列标准的“基于行为预期”一节中定义了“可信性”：遵循第一个

实体的预期操作时，第一个实体认定第二个实体是可信的。1999 年，ISO/IEC 在 15408 规范中正式将“可信赖”一词定义为：在任意条件下参与计算、操作或整个过程的组件都是“可预测的”，并且能抵抗计算机病毒，在一定程度上也能抵挡物理干扰。

可信计算组织（TCG）将“可信”定义为：如果一个实体的行为是可以通过一个预期的方式朝着指定的预期总体目标运行，则这个实体是具有可信度的。TCG 对可信架构的科学做法是通过利用把可信平台模块（Trusted Platform Module，TPA）在硬件系统上应用来提高计算机的安全系数。这种技术方式在现阶段已经得到业界的广泛认可。

电气与电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）将可信度定义为：计算机系统的可信度是可论证的，关键是在于其系统的软件稳定性和可用性。

在国内，中国学者将可信计算系统定义为：一个可信系统应该能够具有可靠性、可用性、信息和行为安全性，并且可信体应该体现在很多方面，比如准确率、可靠性、安全性、实用性、高效率等诸多方面，其中，安全性和可靠性是可信性最主要的两个内容，可信计算系统也可以简单地表达为：可信＝可靠＋安全。

众多不同的定义都有一个共同点，即关注实体行为的可预测性，关注系统软件的安全性和可靠性。

2. 可信计算标准体系

自 1999 年以来，可信计算经历了相关概念定义、科学技术研究的发展，最后到相关技术规范的逐步形成。国际上已经产生了一系列由 TPM 芯片为信任根的 TCG 标准。此外，中国也已经产生了一系列由 TCM 芯片为信任根的双系统架构的可信标准。

可信计算标准体系国际规范和中国规范之间最重要的区别如下。

（1）相关的信任芯片是否能够使用国产加密算法。由中国国家密码局为主导提出了关于中国商用密码可信计算的应用规范，其中就指明严禁在中国市场上销售和装载国际算法的可信计算相关应用产品。

（2）一些中国学者认为，国标提出的 CPU 先加电，再利用密码芯片打造信任链这一模式的强度不足。因此，他们提出了基于 TPCM 芯片的双系统计算安全架构。除了密码功能外，TPCM 芯片还必须先于 CPU 加电、先于衡量 BIOS 的完整性。

（3）可信软件栈是否能够支持操作关于系统层面的透明可信控制。我国部分学者认为，国际标准不能主动在计算机操作系统中进行度量，而是需要通过程序被动地调用可信接口。因此这部分学者提出，要在操作系统内核层面对应用程序完整性和程序行为进行透明可信判定及控制。

3.4.3 基本思想

自 20 世纪 90 年代中期以来，一些国外的计算机制造商便开始研发并提供相关可信的计算技术解决方案。最主流的方案是通过把安全模块应用至硬件层，并建立基于密码技术的可靠根、安全存储机制和信任链，即实现了可信计算机有关的安全目标。具体来说，首先，在计算机系统中建立信任根，通过建立相关物理安全、技术安全和管理安全来确保信任根的可信性；然后建立计算机系统中的信任链，从信任根到软硬件平台，再到操作系统，再到应用程序，通过这种信任扩展到整个计算机系统，能够保证整个计算机系统的可信性。

TCG 通过应用设备将可信计算细化为可信网络服务器、可信 PC、可信 PDA 和可信移动智能终端。可信计算 TCG 的系统架构和关键技术也在慢慢产生，产生了一系列的标准规范；TCG 可信计算不仅考虑信息的安全性，还指出信息的真实性、有效性和一致性。

可信计算平台是指计算平台具有可信计算的安全机制，能够为使用者提供可信的安全服务。其中最关键的特征是是否具有信任根，以信任根为基础搭建有关信任链机制，并且其应该具有度量存储报告的安全机制，可以提供相关可信的服务项目。如其能够确保软件系统数据库的安全性和完整性、数据安全存储和平台远程控制验证。最典型的可信计算平台分别包括可信 PC、可信 Web 服务器和可信 PDA。

可信计算平台通过可信度量根的核心(Core Root of Trust for Measurement)为出发点，所有平台资源通过利用信任链的方法来管理其一致性，将度量值存储在 TPM 平台设备的内存中，根据 TPM 平台来学习其可用性。上报关于其信息的实体路线，并且提供访问者辨别平台是否具有可信度，从而由访问者自行决定是否进行交互。这种工作机制称为信任度量、报告和存储机制，是可信计算机与一般电子计算机在安全机制上的最大区别。

3.4.4 信任根与信任链

1. 信任根

可信计算组织(TCG)定义的信任根由三个根组成。其中，可信度量根(RTM)负责度量完整性；可信报告根(RTR)负责报告信任根；可信存储根(RTS)负责存储信任根。其中，RTM 是一个软件模块、RTR 是由 TPM 的平台配置寄存器(PCR)和背书密钥(EK)组成、RTS 是由 TPM 的 PCR 和存储根密钥(SRK)组成。

在实践中，当建立信任链时，可信度量根首先向可信存储根传递信息，形成完整性度量。再由可信存储根使用其 TPM 平台配置的寄存器存储度量的扩展值，最后使用 TPM 平台中加密服务功能来保护测量的日志。

可信报告根主要用于远程证明过程，并将 TPM 平台可信状态信息传递给实体。主要内容包括 TPM 平台配置信息、审计日志以及身份密钥(它通常被处理为由背书密钥或以背书密钥保护的身份密钥)。

2. 信任链

以信任根为核心基础的信任链，其最主要功能是将其已有的信任关系扩展到整个计算机应用平台。它可以通过其自身的可信度度量机制来获取到那些能够影响平台可信度数值的相关数据，并将这些数据与预期数据进行比较，并最终计算出平台的可信度数值。

信任链的建立需要遵循以下三个规则。

(1) 在被度量之前，除了可信度量根的核心 CRTM(以信任链构建为起点，运行的第一段用于可信度量的代码程序)之外的所有其他组件或者模块都是不可信的。只有通过可信度量计算并最终得到的数据与预期数据一致的组件或者模块才可以被纳入可信边界之内。

(2) 可以将可信边界内部的组件或者模块作为验证的代理部分，对等待验证的组件或者模块进行完整性的验证。

(3) 只有成功通过可信验证的组件或者模块才能最终获得有关于 TPM 的控制权，可信边界外的组件或者模块将会受到限制和无法使用可信平台的模块部分。

在可信计算组织的可信个人计算机技术规范中提出了关于可信个人计算机中的信任链。如图 3.8 所示，可信计算组织的信任链很好地体现了有关于度量存储的报告机制。即相关平台测量的可行性，并存储测量的可信值。

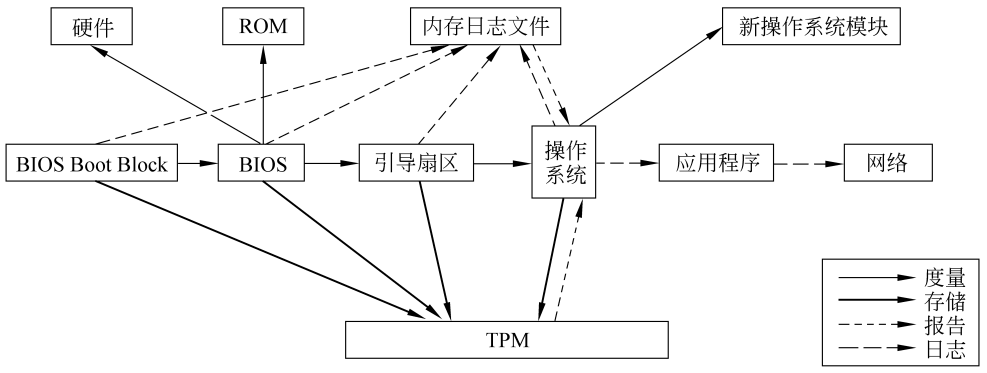

图 3.8　PC 中的信任链

度量：信任链使用基本输入/输出系统(Basic Input/Output System)引导区和可信任安全平台模组(TPM)作为信任根。其中，基本输入/输出系统中的引导区是可信度量根(RTM)，可信任安全平台模组(TPM)是可信存储根(RTS)、可信报告根(RTR)。从基本输入/输出系统中的引导区开始，到程序载入器(OS Loader)，再到操作系统(OS)，最终再到应用程序(Application Program)，形成了一条完整的信任链。沿着这条信任链，可以实现一级度量一级，达到一级信任一级效果，最终得以确保平台资源的完整性。

存储：由于可信任安全平台模组(TPM)的存储空间有限，因此为了利用有限的存储空间，则使用度量扩展方法(即当前度量值与新度量值相连再次进行散列计算)记录度量值并存储在来自可信任安全平台模组的计算机的程序控制暂存器中，与此同时，把可信任安全平台模组的详细信息存储在磁盘中作为记录测量数据和测量数据结果。存储在磁盘中的度量记录和存储在计算机的程序控制暂存器中的度量值进行数据值的相互确认，以防止记录在磁盘中被恶意修改。

报告：通过存储和度量，当访问者需要进行访问时，可以向访问者提供相关报告，最终由访问者自行判断平台的可信状态。提供给访问者的报告包括程序控制暂存器中的度量值和日志。为了保证报告内容的可靠性，必须采用加密、数字签名和认证等相关技术。

3.4.5　关键技术

一个完备的可信计算系统应该至少包含以下 5 个关键技术：签注密钥(Endorsement Key)、安全输入/输出(Secure Input/Output)、存储器屏蔽(Memory Curtaining)、密封存储(Sealed Storage)、远程认证(Remote Attestation)等。

签注密钥：指的是由一对 2048 位的公开密钥密码体制 RSA 密钥对，其中分别包括公开和私有两种不同的密钥，它们在芯片生产时随机生成并且在生成后不能进行修改。其中，私有密钥被嵌入在芯片内部，公开密钥则是用于验证和加密发送敏感数据到芯片中去。

安全输入/输出：指的是用户在使用计算机软件进行交互时的信息数据传输路径进行

保护。目前，不少恶意软件通过监听计算机用户的键盘或者以截屏等方式恶意拦截计算机用户和软件进程之间产生传送的信息数据，因此关于安全的输入和输出是必不可少的。

存储器屏蔽：指的是一种更为安全的数据存储保护技术，提供了一块完全独立的数据存储区域，其自身的操作系统也没有获得完全的访问权限。因此，即使入侵者控制了设备的操作系统，也能够保证用户数据的安全。

密封存储：指的是通过把软硬件平台配置信息与私有信息进行捆绑，实现保护用户私有信息的目的。密封后的信息数据只有在软硬件匹配的情况下才能够进行读取。例如，某个用户在其个人计算机中存储了一段经过密封存储的视频，但是由于该个人计算机中没有相关播放视频的许可证，则无法获取该段视频信息。

远程认证：远程认证技术允许用户使用存储在外部认证服务上的凭证向系统认证，用户计算机上的改变可以被授权方获取。

3.4.6 可信计算的应用

可信计算的应用主要包括以下几方面。

第一个应用是“数字版权管理”：公司可以通过“可信计算”技术建立相关的数字版权管理系统来管理其数字版权。这个在当今的各种软件产品上经常可以看见。

第二个应用是“身份盗用保护”：“可信计算”可以通过认证证书的方式，实现“防止身份盗用”。

第三个应用是“游戏防作弊”：“可信计算”可以利用“安全输入/输出”等关键技术来打击在线游戏作弊。

第四个应用是“保护系统”：操作系统可以通过软件的数字签名，识别带有间谍软件的应用程序，进而实现系统保护的目的。

第五个应用是“保护数据”：是指可以通过“可信计算”技术进行生物的身份认证鉴别，通过相关设备保护数据安全。

第六个应用是“计算结果”：是指可以通过“可信计算”保证网格中计算系统的参与者所返回的计算数据是真实的。

3.4.7 研究现状与展望

1. 目前研究现状

目前，国内外的学者和相关机构针对可信计算进行了广泛和深入的研究，内容包括以下几方面。

(1) 可信程序开发工具和方法。

一些软件开发人员在开发软件系统时往往过分注重实现其功能性，而对于代码本身理应具备的安全性缺乏考虑，这就会给黑客找到机会利用代码存在的安全漏洞。我们需要认识到，仅借助安全功能模块保护系统的安全是无济于事的，因此，在一开始编码就必须把软件安全性纳入考量，安全性应贯穿整个编码过程。可信程序开发工具和可信程序开发方法是开发系统过程中的重要步骤，它可以使得软件开发人员不需要通过复杂的操作就可以显著提高系统安全性，从而降低系统引发安全问题的可能性。

(2) 构件信任属性的建模、分析和预测。

未来的软件很有可能是由各种构件组装而成的,可以使用或者借助许多现有的构件,而并不需要完完全全地从零开始开发一个新的软件。基于构件的软件开发技术正在逐渐发展,并具有可能成为主流的软件开发技术的势头。在这样的大背景下,实现可信系统软件的重要前提就是可信的构件,只有这样才能更加有效地使用各种构件组装成系统软件。如何对一个构件的信任属性进行适当的评估解读,以及如何对其进行建模、分析和预测正是关键所在,针对构件信任属性的研究将会成为未来的一个研究热点。

(3) 容错与容侵系统研究。

随着科技、社会的发展,当代计算机技术已经渗透到人们日常社会生活的方方面面,而诸多的计算机系统恶意攻击也席卷而来,针对系统的容错性和容侵性展开的研究已然成为一个需要关注的重要课题,系统的容错性和容侵性也成为评判计算机系统性能的核心技术指标之一。软件开发人员需要更加关注如何从硬件和软件两个层面上提升系统容错性,尤其需要关注分布式系统的容错性。我们不可能完全消除计算机系统中的安全隐患,研究者和开发人员需要做的是不断研究和提升容侵系统,从而使计算机系统对于恶意攻击具有抵抗性,使其受到恶意攻击后也不会很快瘫痪,仍然可以运行一些关键操作,甚至可以进行自我修复。

(4) 安全分布式计算。

网络可以链接全球的计算机资源,网格计算、公式计算、Web 服务、公用计算、对等计算等概念逐渐兴起,互联网环境的规模不断扩大,复杂性不断提高,分布式计算也正在逐渐成为主流的计算模式。在复杂的网络环境下,传统的安全技术将会被淘汰。因此,针对分布式环境下的认证、授权以及审计等安全技术的开发刻不容缓,如何为分布式计算提供更具安全性和保障性的环境是一大研究热点。

2. 可信计算的未来

随着数字时代的到来,互联网对人们的生活带来了很大的影响。首先,计算机和网络已经渗入社会的各个方面和领域,成为人类社会不可分割的一部分;其次,政府和商业活动也越来越多地在互联网中进行,如电子商务、电子政务等应用的兴起。

然而,现有的网络与信息的可信程度尚不能满足社会发展的需求,如何构建新一代适应信息发展需求的高可信性计算环境仍将是信息科学技术领域最重要的分支。

可信计算提出了解决信息安全的很好的思路,但离全面应用还需要一段时间。可信计算领域的发展离不开学术界和企业界的共同努力:一方面,学术界需要在现有研究课题的基础上展开可信计算平台的研究,理论上需要实现设备安全、数据安全、内容安全与行为安全,完善系统可信、软件开发环境、自芯片而上的硬件平台、系统软件、应用软件、网络系统及拓扑结构所应遵循的设计策略。另一方面,企业界需要充分接受可信计算环境的思路,并将其融入产品、设计、研发过程中,为可信计算平台的构建设立统一的工业标准,从而让不同厂商的软、硬件产品得以彼此兼容。通过学术界和企业界的共同努力,才能营造安全可信计算的环境、共创可信计算的未来。

针对可信计算所开展的一系列研究以及相关平台的建设,既是顺应全球信息化发展的潮流,也是涉及我国国家信息安全的重要战略。自 20 世纪 80 年代以来,我国就开始了对可信计算的研究,研究领域涉及容错计算、安全操作系统构建、计算机系统可信性评估、可信软

件评测、可信数据库建设、网络与信息安全等各方面。进入21世纪以来，信息安全已经上升到国家战略层面，将国家等级保护防御体系提升到了一个新的科学高度和战略高度。面对计算机和信息技术不断增长的需求，我们必须全方位加强针对可信计算技术的研究，促进我国信息技术的发展，为国家信息安全提供保障，为构建全球可信计算平台展现中国智慧、贡献中国力量。

习题

1. 物理安全隔离卡的作用是什么？
2. 介绍一下影响工控安全的因素，并且试着提出解决方案。
3. 你认为芯片安全重要吗？为什么？
4. 芯片制造过程中哪些阶段容易出现问题？
5. 简单叙述一下硬件木马的分类。
6. 谈一谈硬件木马的检测困难在哪儿。
7. 谈一谈可信计算的定义。
8. 介绍一下可信计算的实现原理。
9. 你在生活上遇到过可信计算的实例吗？介绍一下。