1. **物理安全**
   1. 概念：实体安全（Physical Security），是保护计算机设备、设施（网络及通信线路）免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施和过程。主要是指对计算机及网络系统的环境、场地、设备和通信线路等采取的安全技术措施。
   2. 包括：环境安全、电源系统安全、设备安全和通信线路安全。
   3. 环境安全：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。
      1. 机房安全；
      2. 机房防盗：装监控、贴磁条、光缆串接+在线监测是否联通；
      3. 三度：温度、湿度、洁净度；
      4. 防火防水。
   4. 电源系统安全：电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。
      1. 供电安全；
      2. 防静电：不挂毯、采用聚乙烯材料、装防静电地板、保持合适湿度；
      3. 接地与防雷；
   5. 设备安全：要保证硬件设备随时处于良好的工作状态，建立健全使用管理规章制度，建立设备运行日志。同时要注意保护存储媒体的安全性，包括存储媒体自身和数据的安全。
      1. 硬件设备的维护与管理：建立设备使用情况日志、故障情况登记表、对设备的物理访问权限限制在最小范围内；
      2. 电磁辐射防护：电磁辐射有泄密的风险。

防护措施：

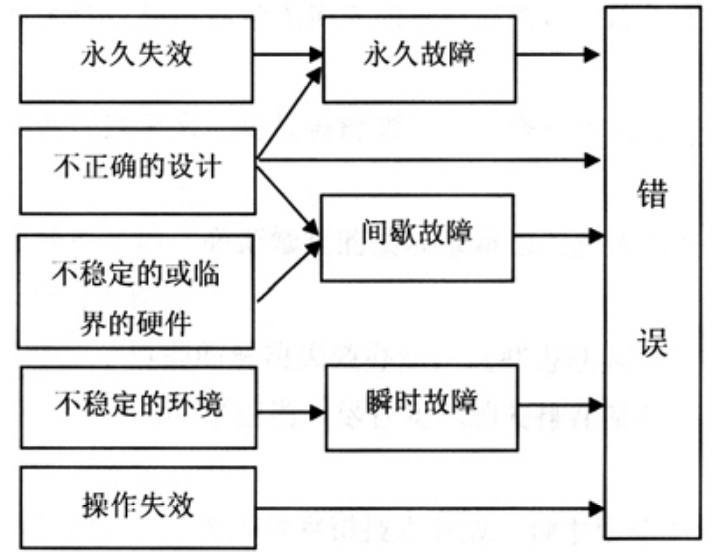
* + - 1. 对传导发射的防护：对电源线和信号线加装**滤波器**；
      2. 对辐射的防护：
         1. 采用各种电磁屏蔽措施；
         2. 干扰的防护措施：利用干扰装置产生一种与计算机系统辐射相关的**伪噪声**向空间辐射来掩盖计算机系统的工作频率和信息特征。
    1. 信息存储媒体安全；
  1. 通信线路安全：包括防止电磁信息的泄漏、线路截获，以及抗电磁干扰。

通信电缆密封在塑料套管中，并在线缆的两端充气加压。线上连接了带有报警器的监示器，用来测量压力。如果压力下降，则意味电缆可能被破坏了，技术人员还可以进一步检测出破坏点的位置，以便及时进行修复。

1. **容错和可靠性**
   1. 失效：硬件**物理特性**异变，或软件不能完成规定功能的能力。
   2. 故障：硬件或软件的错误状态，是失效在逻辑上的等效。一个故障可以用**种类、值、影响范围**和**发生时间**来描述。
      1. 按逻辑性分：

* 逻辑故障：造成逻辑值发生变化的故障
* 非逻辑故障：造成象时钟（clock）或电源出错等错误的故障
  + 1. 按时间分：
* 永久性故障：调用**诊断程序**进行故障定位，然后采取纠错措施；
* 间隔性故障：可以通过**更换硬件或软件**等途径来达到修复的目的；
* 偶然性故障：只能靠**改善环境条件**等努力来减少这类故障。
  1. 错误：程序或数据结构中的故障表现形式，是故障和失效所造成的后果。

错误的根源：



* 1. 容错设计的软件可以**有某些规定数目的故障**但**不导致失效**，但对无容错的软件而言，故障即失效。
  2. 可靠性：【广义】一切旨在避免、减少、处理、度量软件/硬件故障（错误、缺陷、失效）的分析、设计、测试等方法、技术和实践活动。【狭义】软件/硬件无效运行的定量度量。
* 可靠度：在规定的**运行环境**中和**规定的时间**内软件**无失效运行的机会**。
  1. 系统可靠性的指标：
     1. 可靠性（Reliability）：计算机在**规定条件**和**规定时间**内完成**规定功能**的概率。

失效：产品在规定条件下和规定时间内丧失了规定功能。

失效率：计算机在**某一瞬间**元件**失效数**与**元件总数**的比率。

**规定条件**：环境条件，使用条件，维修条件， 操作技术等。

* + 1. 可维性（Serviceability）：在**规定时间**内，按照**规定的程序和方法**进行维修时，保持或恢复到**能完成规定的功能**的能力。

即从**判定故障**到**排除故障**所需要的时间，包括**故障诊断**、**故障定位**、**系统校正**和**恢复**等时间。

可保持性（Maintainability）：系统在**给定的时间内**可**隔离故障**或**修复**的概率。表征了系统可以**正常运行的效率**。

* + 1. 可用性（Availability）：【**有效率**或**利用率**】可维修部件在**某时间**具有**维持规定功能**的能力，即计算机系统的**利用效率**，也是系统在执行任务的任意时刻能**正常工作的概率**。
  1. 排错：避免故障，通过对组成系统的**部件**进行严格的**筛选**、对系统进行严格的**测试**、对系统进行**屏蔽**以**减少外界的干扰**等方法来提高系统的可靠性。
  2. 容错：即容忍故障，一旦发生故障能自动检测出故障并使系统自动恢复正常运行，使计算机系统在发生故障后仍能正确运行。当出现某些指定的硬件**故障**或软件**错误**时，系统仍能执行规定的一组程序，或者说程序**不会因系统中的故障而中止或被修改**，并且执行**结果也不包含系统中故障所引起的差错**。

容错技术：设计与分析容错计算机系统的各种技术。

* 从**系统结构**方面来提高计算机系统的可靠性
* 容错技术与排错技术并**不是相互对立**的，它们可以**相互补充**，构成高可信的计算机系统
  1. 实现容错计算的四个方面：
     1. 不希望事件的检测。

**不希望事件**：失效、 故障、差错等。

* + 1. 损坏估价。在作出一个被检测的故障有关的决定之前，有必要判定系统已被破坏的程度。

原因：故障的出现和它的失效结果之间可能存在延迟，故障可能已经传播到该系统的其他地方，导致故障的扩大。

影响因素：设计策略、探测技术。

* + 1. 不希望事件的恢复。把目前的错误系统状态转换成一个正确的系统状态。
    2. 不希望事件处理和继续服务。确保已被恢复的不希望事件效应不会立即再现，以使系统继续提供规定的服务。
  1. 容错系统的一般阶段：
     1. 故障限制：把故障效应的传播限制到一个区域内，防止污染其他区域。
     2. 故障检测：大多数失效最终导致产生逻辑故障，可用奇偶校验、一致性校验检测出来。

脱机检测设备不能进行有用工作；联机检测提供实时检测能力；联机检测技术包括奇偶校验和二模冗余校验。

* + 1. 故障屏蔽：把失效效应掩盖起来，可以说是冗余信息战胜了错误信息，如**多数表决冗余设计**。
    2. 重试：在许多场合（尤其是瞬间故障），对一个操作的第二次试验可能是成功的。
    3. 诊断：如果故障检测技术没有提供有关**故障位置**和/或**性质**的信息，那么就需要一个诊断。
    4. 重组：当发生永久故障时，**重组系统器件**以便替代失效的器件或把失效的器件与系统其他部分**隔离**开来，也可使用**冗余系统**，系统能力不降低。
    5. 恢复：系统回到故障检测前处理过程的某一点，并从该点重新开始操作（称作**卷回**）。通常需要后备文件、校验点和应用记录方法。
    6. 重启动：破坏过多或无恢复功能时，使用重启动。

热重启：仅系统未受任何破坏，可从故障检测点恢复所有操作。

温重启：仅有某些过程可以毫无损失的重新启动。

冷重启：系统需要完全重新加载。

* + 1. 修复：把诊断为故障的器件换下来，可联机也可脱机。
    2. 重构：对元件进行物理替换之后，把修复的模块重新加入到该系统中去。对联机修复来说，实现重构不中断系统的工作。
  1. 容错技术的发展概况
     1. 第一代：
* 元件：电子管、继电器及延迟线存储器
* 问题：**元件的失效率**相当高，并易受**瞬时故障**的影响
* 措施：特别设置的**硬件故障检测**和**人工恢复**
  + 1. 第二代：
* 元件：晶体管及磁芯存储器
* 问题：失效率比第一代计算机元件大为降低
* 措施：**避错技术**占统治地位，对故障一般采用**诊断程序**进行**脱机检测**
  + 1. 第三代
* 元件：集成电路
* 问题：元件的失效率继续降低，但计算机应用范围扩大，对计算机系统的**可信性**要求更高
* 措施：容错技术重新提出，并得到了较快的发展，并出现了许多**容错计算机**
  + 1. 第四代
* 元件：大规模和超大规模集成电路
* 问题：硬件可靠性大大提高而价格却大幅度降低，使采用各种容错技术在经济上**更易接受**
* 需求：容错技术应用范围扩展于**银行事务处理**及各种**实时控制系统**，甚至许多**通用计算机**系统也采用了容错技术
  + 1. 80年代以来

出现商用容错计算机市场、分布式容错计算机系统、容错的VLSI技术、人工智能在容错技术上的应用——计算机故障诊断专家系统

* 1. 容错技术主要内容
     1. 故障检测与诊断技术

检测的作用：确认系统是否发生了故障，指示故障的状态，即查找**故障源**和**故障性质**。只能找到错误点（错误单元），不能准确找到故障点。

诊断的作用：给出故障定位。

技术基础：检错纠错码技术。奇偶校验码、循环码、海明码等。

* + 1. 故障屏蔽技术

作用：防止系统中的故障在该系统的信息结构中产生差错。

措施/实质：在故障效应达到模块的输出以前，利用冗余资源将故障影响 掩盖起来，达到容错目的。

特点：不改变系统的结构，即系统部件之间的逻辑关系相互固定，又称**静态冗余技术**。

* + 1. 动态冗余技术
    2. 软件容错技术
    3. 信息保护技术