这部分主要是架构师综合知识的介绍，相关系列文章如下所示。

可靠性Reliablity是指产品在规定的条件下和规定的时间内完成规定功能的能力。软件可靠性可以基于使用条件、规定时间、系统输入、系统使用和软件缺陷等变量构建的数学表达式。其中比较重要的概念如下。

规定时间：包含3中情况，为自然时间、运行时间和执行时间。

失效概率：常把软件运行开始，到某一时刻t为止，出现失效的概率看做关于软件运行时间的一个随机函数，初始时失效概率为0，在时间域上单调递增，失效概率在运行时间不断增长时趋向1。

可靠度：在规定时间内不发生失效的概率，R(t)=1-F(t)，常见的可靠度为90，99，99.99，99.9999。

失效强度(Failure Intensity)：单位时间软件系统出现失效的概率。

失效率：风险函数，在运行至此软件系统为出现失效的情况下，单位时间软件系统出现失效的概率。

影响软件可靠性的因素包括：运行环境（剖面）、软件规模、软件内部结构、软件的开发方法和开发环境、软件的可靠性投入等。

常见的软件可靠性模型：种子法模型、失效率类模型、曲线拟合类模型、可靠性增长模型、程序结构分析模型、输入域分类模型、执行路径分析方法模型、非齐次泊松过程模型、马尔科夫过程模型、贝叶斯分析模型。

典型的测试用例包括：测试用例标识、被测对象、测试环境及条件、测试输入、操作步骤、预期输出、判断输出结构是否符合标准、测试对象的特殊需求。

软件可靠性设计包括：容错设计技术，恢复块设计、N版本程序设计、冗余设计；检错技术，检测对象、检测延时、实现方式、处理方式；降低复杂度设计。

在实际应用中，面对安全威胁，可以通过如下5个方面进行准备：认证鉴别、访问控制、内容安全、冗余恢复和审计响应。

相关信息安全标准：TCSEC(美国)、ITSEC（欧洲）、加拿大(CTCPEC)、ISO7498-2-1989标准。我国的信息安全主管部门包括公安部、信息产业部和国家技术标准局。

1．信息系统安全体系



验证(Authentication):验证用户是否可以获得访问权，认证信息包括用户名、用户密码和认证结果。

授权(Authorization):授权用户可以使用哪些服务，授权包括服务类型及服务相关信息等。

审计(Accounting)：记录用户使用网络资源的情况，用户IP地址、MAC地址掩码等。

2．网络安全体系架构设计

国家标准《信息处理系统工程开放系统互联基本参考模型—第二部分：安全体系结构》给出了基于OSI参考模型的7层协议之上的信息安全体系结构。

网络安全体系结构的基础包括：多点技术防御，网络和基础设施、边界、计算环境；分层技术防御，公钥基础设施、检测和响应基础设施。

网络安全体系结构的相关框架包括：鉴别框架（验证）、访问控制框架（授权）、机密性框架（加密）、完整性框架、抗抵赖框架。

此外，数据库系统的安全性主要通过数据库完整性设计来解决。

。，