# 西门子Smart模块6ES7-288-5CM01-0AA0

| | |
|---|---|
| 产品名称 | 西门子Smart模块6ES7-288-5CM01-0AA0 |
| 公司名称 | 浔之漫智控技术（上海）有限公司 |
| 价格 | .00/件 |
| 规格参数 | 品牌:西门子<br>型号:全系列<br>产地:德国 |
| 公司地址 | 上海市松江区石湖荡镇塔汇路755弄29号1幢一层A区213室 |
| 联系电话 | 157****1077 157****1077 |

# 产品详情

西门子Smart模块6ES7-288-5CM01-0AA0

在规定的时间周期内所述条件下程序执行所要求的功能的能力。

由上述定义可知，软件可靠性不但与软件存在的缺陷和/或差错有关，而且与系统输入和系统使用有关。提高软件可靠性就是要减少软件中的缺陷或错误，提高软件系统的健壮性。因此，软件可靠性通常涉及软件安全性的要求，但是软件可靠性要求不能完全取代软件安全性的要求。

软件保障已经成为信息安全的核心，它是多门不同学科的交叉，其中包括信息确保、项目管理、系统工程、软件获取、软件工程、测试评估、保险与安全、信息系统安全工程等。目前国内被广泛认知的软件保障模型为方滨兴院士等提出的软件确保模型。该模型建立了分析和确保软件质量的保证模型，并指出软件确保是信息保障、测试评估及信息系统安全工程的核心。全的可存活性是指信息系统的这样一种能力：它能在面对各种攻击或错误的情况下继续提供核心的服务，而且能够及时恢复全部软件工程是指，采用工程的概念、原理、技术和方法来开发和维护软件，把经过时间考验而证明正确的管理技术和当前分别给出了外部质量和内部质量模型，以及使用质量模型来描述软件质量。外部质量和内部质量模型包含6个特性（功能性、可靠性、易用性、效率、维护性和可移植性），并进一步细分为若干子特性。使用质量的属性分类为4个特性：有效性、生产率、安全性和满意度。由此可见，安全性是软件质量的一个重要属性能够得到的西门子好的技术方法结合起来，从而经济地开发出高质量的软件并有效地进行维护。概括地说，软件工程是指导计算机软件开发和维护的一门工程学科，是技术与管理紧密结合形成的工程学科。

通常把软件生命周期全过程中使用的一整套技术方法的集合称为方法学。软件工程方法学包含3个要素：方法、工具和过程。其中，方法是完成软件开发的各项任务的技术方法，是回答“ 怎样做 ”的问题；工具是为运用方法而提供的自动的或半自动的软件工程支持环境；过程是为了获得高质量的软件所需要完成的一系列任务的框架，它规定了完成各项任务的工作步骤。

由于软件漏洞、恶意软件和软件侵权等安全问题而导致的系统可靠性受到威胁，会危及信息系统基础设施（如工控系统）和个人隐私（如信用卡账户信息）的安全，给整个社会带来破坏，阻碍经济有序发展，因而软件安全开发、软件安全检测及软件版权保护是软件工程方法学的重要内容。的服务。

软件作为信息系统的重要组成，可存活性是一个融合信息安全和业务风险管理的新课题，它的焦点不仅是对抗网络入侵者，还要保证在各种网络攻击的情况下业务目标得以实现，关键的业务功能得以保持。安全的可控性是指，对于信息安全风险的控制能力，即通过一系列措施，对信息系统安全风险进行事前识别、预测，并通过一定的手段来防范、化解风险，以减少遭受损失的可能性。

浔之漫智控技术（上海）有限公司（xzm-wqy-shqw）

是中国西门子的佳合作伙伴，公司主要从事工业自动化产品的集成,销售和维修，是全国的自动化设备公司之一。

公司坐落于中国城市上海市，我们真诚的希望在器件的销售和工程项目承接、系统开发上能和贵司开展多方面合作。

以下是我司主要代理西门子产品，欢迎您来电来函咨询，我们将为您提供优惠的价格及快捷细致的服务！

西门子Smart模块6ES7-288-5CM01-0AA0

软件的可控性是一种系统性的风险控制概念，涉及对软件系统的认证授权和监控管理，确保实体（用户、进程等）身份的真实性，确保内容的安全和合法，确保系统状态可被授权方所控制。管理机构可以通过信息监控、审计和过滤等手段对系统活动、信息的内容及传播进行监管和控制。减少软件产品开发中通常在开发后期进行测试以消除编码中的错误或缺陷。这种做法对于减少软件产品中的漏洞数量信息安全中的保软件是访问内部网络、系统与数据库的渠道，因此对于内部敏感信息的访问必须得到批准。认证就是解决这一问题的信息安全概念，它通过验证身份信息来保证访问主体与所声称的身份唯一对应。信息安全的抗抵赖性是指，信息的发送者无法否认已发出的信息或信息的部分内容，信息的接收者无法否认已经接收的信息或信息的部分内容。

软件安全中，抗抵赖性解决的是用户或者软件系统对于已有动作的否认问题。例如，当价格发生变动时，如果软件能够记录假冒的动作变化及施加动作的用户身份，就可以给个人一个否认或者拒绝动作的机会，由此保证抗抵赖性的实现。

实现不可抵赖性的措施主要有数字签名、可信第三方认证技术等，可审计性也是有效实现抗抵赖性的基础。

只有在申请认证的身份信息是可识别的情况下，认证才能成功，所提供的凭证信息必须是真实可信的。凭证西门子常见的形式是用户名和口令的组合，目前，生物特征认证、生物行为认证及多因素认证成为发展的方向。密性是指确保信息资源仅被合法的实体（如用户、进程等）访问，使信息不泄露给未授权的实体。这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，以及个人的秘密和个人隐私（如浏览习惯、购物习惯等）。保密性还包括保护数据的存在性，有时候存在性比数据本身更能暴露信息。特别需要说明的是，对计算机的进程、中央处理器、存储和打印设备的使用也必须实施严格的保密措施，以避免产生电磁泄露等安全问题。有一定的作用，但是系统设计逻辑上的一些缺陷在测试阶段是无法发现的，往往这些漏洞会增加后期系统维护的成本，并且给用户带来巨大的潜在风险。

开发出安全漏洞尽可能少的软件应当是软件开发者或者说是软件厂商追求的目标。不仅要把软件做得更好，而且要更安全，同时，根据现实世界的经验，必须保证该解决方案具有较好的成本效益、操作相关

性和可行性，以及投资的可行性。

事实上，软件安全开发的西门子佳实践是采用从软件开发之初就不允许漏洞发生的方式，在软件开发的各个环节尽可能消除漏洞，这不仅使得软件及其用户更安全，关键基础设施更具弹性，还将节省软件企业的开发成本。

安全的软件和系统是不存在的，软件产品存在漏洞是当前信息安全领域面临的西门子大困境。由于漏洞的产生、利用及相互作用的机理复杂，因此，如何有效减少系统漏洞数量，提高信息系统整体安全性，成为当前急需解决的挑战性问题。

软件已经渗透到社会、经济与国防建设的方方面面，是信息时代所依赖的重要技术与手段，其安全直接关系到国计民生与国家安全，因此，软件安全关乎国家竞争力。系统本身漏洞的存在，仍属于检测型或补偿型控制的被动防护方法。尽管如微软等核心软件公司能够定期发布安全补丁，较为及时地对操作系统、数据库等核心软件的漏洞进行修复，但对于一些零日攻击系统几乎没有防范能力。加之大多数的应用软件开发人员没有能力及时地对应用软件漏洞进行修复，使得系统的运行处于一种危机四伏的状态。传统的安全控制效果不尽如人意，信息安全问题越来越多，攻击形势越来越隐蔽（如APT攻击），智能程度越来越高（技术水平越来越高），组织方式多样化（由西门子初的单个人员入侵发展到利益驱动的有组织、有计划的产业行为），危害程度日益严重。