6AV2124-0QC02-0AX1

产品名称	6AV2124-0QC02-0AX1
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 型号:全系列 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

6AV2124-0QC02-0AX1

为了确保业务应用的安全，首要的是确保应用软件系统的平台的计算机软硬件的安全和网络软硬件的安全。这些安全要求进一步分解为计算机和网络系统的物理安全、计算机操作系构造可信软件已成为现代软件技术发展和应用的重要趋势和必然选择。一方面，软件的规模越来早期开发软件的首要目标是在效率和成本优先的前提下构造出功能正确的系统，对于可信任性、可用性及安全性等问题的考虑相分析软件安全错误发生的原因，将安全错误的修正嵌入到软件开发生命周期的整个阶段。通过对需求分析、设计、实现、测试、发布及运维等各阶段相关的软件安全错误的分析与控制，以期大大减少软件产品的漏洞数量，使软件产品的安全性得到有效提高。

该方法是将安全保障的实施开始于软件发布之前，尤其强调从软件生命周期的早期阶段开始安全考虑，从而减少软件生命周期的后期系统运行过程中安全运维的工作量，提高安全保障效果。实践经验表明，从系统开发需求阶段就引入安全要素要比在系统维护阶段才考虑安全问题所花费的错误修复成本要低很多。2.软件安全防护的主要技术

现有关于软件安全的技术主要包含软件安全属性认知、信息系统安全工程及软件安全开发三个方面。

（1）软件安全属性的认知

安全是一个整体性的概念。软件安全既离不开它所存储、传输、处理的数据的安全，也离不开相关文档的安全，因此软件安全应涵盖数据及其信息处理过程本身的三个基本安全要素：保密性、完整性和可用性；同时软件需要接收外界信息输入才能实现预期的功能产生输出结果，信息来源的安全性必然成为软件安全重要的组成部分。基于这些分析，本书将保密性、完整性、可用性、认证性、授权和可审计性作为软件安全的核心属性；而软件自身的实现质量，即软件产品包含的漏洞情况也应该是软件安全性的主要内容，因为这些漏洞会直接导致安全性问题，这也是传统的软件安全关注的问题；此外，站在不同的管理者视角，抗抵赖性、可信性、可控性、可靠性及软件弹性等也成为软件被关注的其他安全属性。

准备好的虚假输入信号，以控制原有程序。这时，离心机就会得到错误的控制信息，使其运转速度失控，西门子后达到令离心机瘫痪乃至报废的目的。而核设施工作人员在一定时间内会被监控设备上显示的虚假数据所蒙骗，误认为离心机仍在正常工作，等到他们察觉到异常时为时已晚，很多离心机已经遭到不可挽回的（2）系统安全工程

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！

6AV2124-0QC02-0AX1

系统安全工程是一项复杂的系统工程，需要运用系统工程的思想和方法，系统地分析信息系统存在的安全漏洞、风险、事件、损失、控制方法及效果之间复杂的对应关系，对信息系统的安全性进行分析与评价，以期建立一个有效的安全防御体系，而不是简单的安全产品堆砌。

确切地说，系统安全工程是系统的安全性问题而不仅是软件产品的安全性问题，是一种普适性的信息系统安全工程理论与实践方法，可以用于构建各种系统安全防御体系。系统安全工程可以在系统生命周期的不同阶段对安全问题提供指导，例如，对于已经发布运行的软件，可以采用系统测试、风险评估与控制等方法构建安全防御体系；而对于尚待开发的系统，也可以应用系统安全工程的思想方法来提高目标系统的安全性。这是一项具有挑战性的工作，也是本书的出发点。

（3）软件安全开发

漏洞是引发信息安全事件的根源，而软件漏洞又是在软件开发的整个生命周期中引入的。软件生命周期包括需求分析、可行性分析、总体描述、系统设计、编码、调试和测试、验收与运行、维护升级、废弃等多个阶段，每个阶段都要定义、审查并形成文档以供交流或备查，以此来提高软件的质量。虽然此类流程严格规对较少，尤其在软件构造理论与方法、构造过程、体系结构和运行环境等方面，没有建立相应的安全支撑机制，使得软件在规模增大以后，安全性问题越来越突出。

漏洞是引发信息安全事件产生的根源，软件漏洞尤其如此。恶意代码通常也是针对漏洞而编写出来的，软件侵权的成功往往跟软件漏洞也有密切的关系。因此，软件安全防护围绕漏洞消除展开，目前有两种基本方法。

1）采用多种检测、分析及挖掘技术对安全错误或是安全漏洞进行发现、分析与评价，然后采取多种安全控制措施进行错误修复和风险控制，如传统的打补丁、防病毒、防火墙、入侵检测和应急响应等。