<<安全性设计分析与验证>>

图书基本信息

书名：<<安全性设计分析与验证>>

13位ISBN编号：9787118072884

10位ISBN编号：7118072885

出版时间：2011-4

出版时间：国防工业

作者：赵廷弟 编

页数：357

<<安全性设计分析与验证>>

内容概要

《安全性设计分析与验证》主要面向工程技术人员，以“危险”为核心，阐述了装备研制中的安全性工程工作、技术体系及具体技术方法，强调工程实用性。
《安全性设计分析与验证》介绍了安全性工程的地位和作用以及发展历程；在介绍安全性度量与要求及安全性工程基本概念的基础上，梳理分析了装备研制、生产、使用各阶段的安全性分析工作，结合不同装备特点有针对性地介绍了各类产品的安全性设计原则和方法；详细阐述了安全性分析、设计技术方法。
同时，《安全性设计分析与验证》针对装备中的软件安全性工作，介绍了相关的技术方法。
最后，介绍了安全性验证的管理与技术方法。

《安全性设计分析与验证》供工程技术人员及管理人员在开展安全性工程工作时学习和参考，也可作为培训教材使用。
同样也可用于高等院校高年级本科生及研究生学习参考。

<<安全性设计分析与验证>>

书籍目录

章节摘录

版权页：插图：2）软件与信息技术对安全性工程的挑战随着信息技术的不断发展，软件在装备中逐渐发挥重要的作用，软件的规模和复杂性日益增加，软件错误导致的安全性事故也在不断增多。
例如，2007年12架F一22战斗机从夏威夷飞往日本，途经国际日期变更线时，计算机系统发生故障，这是在软件需求中没有考虑到经过国际日期变更线的时间处理问题而产生的严重后果，若在战时这些战机很可能会因此而被击落。
近20年来软件安全性获得越来越多的关注，在航天、航空、兵器、医疗、核工业以及交通等领域，众多的机构对其进行了深入的研究，例如，美国国防部（DOD）、美国航空宇航局（NASA）、美国联邦航空局（FAA）、欧洲航天局（ESA）、英国国防部（MOD）以及国际电工委员会（IEC）、电气和电子工程师协会（IEEE）、航空无线电技术委员会（RTCA）以及以麻省理工学院（MIT）等。
这些机构获得了丰富的研究成果，并形成了一些广为认可的软件安全性规范，有些已成为广为应用的行业标准，用以指导实际的软件安全性工作的开展，例如，美国联合军种软件系统安全性委员会发布的《软件系统安全性手册》、RTCADO-178B、IEC-61508以及NASA-GB-8719.13等。
在不同标准中，软件安全性.工作思路有所侧重，RTCADO-178B在强调开展软件安全性分析的前提下，注重在软件工程过程中的验证策略及过程管理；美军JSSSC的《软件系统安全性手册》是以危险的识别、消除、控制为核心开展软件安全性工作；澳大利亚国防部标准DEF（AUST）5679则比较注重计划的制定以及证据的收集，而N.ASA-GB一8719.13及其指南则以软件开发过程为主线，更全面地从安全性分析、设计和验证及过程和管理等方面对软件安全性工作进行规范。
我国软件安全性的研究和应用起步较晚，但随着工程需要，我国的软件安全性研究也逐步开展起来。已制定的相关标准有GJB／Z102-97《软件可靠性和安全性设计准则》和GJB142-2004《军用软件安全性分析指南》，以及一些相关的行业标准。
与此相适应，各类安全性标准中都增加了软件安全性工作项目，要求在装备研制过程中针对软件系统开展安全性分析、评价和验证工作。
例如，在美国信息技术协会最新的安全性标准中，将软件安全性工作分为危险分析和软件集成.（integrity）两个过程，强调从系统整体层面来研究软件故障、危险和事故的影响；要求在软件设计、开发和测试过程中并行开展危险分析，并制定和检验是否达到规定要求。

编辑推荐

<<安全性设计分析与验证>>

版权说明