ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.3—2006/IEC 61508-3:1998

电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements

(IEC 61508-3:1998,IDT)

2006-07-25 发布　　2007-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中华人民共和国
国家标准
电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求
GB/T 20438.3—2006/IEC 61508-3:1998
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.5 字数 67千字
2007年1月第一版 2007年1月第一次印刷
*
书号:155066·1-28709 定价 18.00元

GB/T 20438.3-2006

前　言

GB/T 20438 由下列 7 部分构成：

——第 1 部分：一般要求；

——第 2 部分：电气/电子/可编程电子安全相关系统的要求；

——第 3 部分：软件要求；

——第 4 部分：定义和缩略语；

——第 5 部分：确定安全完整性等级的方法示例；

——第 6 部分：GB/T 20438.2 和 GB/T 20438.3 的应用指南；

——第 7 部分：技术和措施概述。

本部分是 GB/T 20438 的第 3 部分。

本部分等同采用国际标准 IEC 61508-3:1998《电气/电子/可编程电子安全相关系统的功能安全 第 3 部分：软件要求》(英文版)。

本部分的附录 A、附录 B 为规范性附录。

本部分与 IEC 61508-3:1998 在技术内容上没有差异，为便于使用做了下列编辑性修改：

a) 将“IEC 61508”改为“GB/T 20438”。

b) 本“国际标准”一词改为“本标准”。

c) 删除国际标准中 1.2 的注 2，因为此注所表述的是 IEC 61508 在美国和加拿大等国的应用情况，与我国的实际不符，所以删除。

d) 用小数点“.”代替作为小数点的逗号“,”。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量和控制标准化技术委员会(SAC/TC 124)归口。

本部分由机械工业仪器仪表综合技术经济研究所负责起草。

本部分主要起草人：王莉、冯晓升、梅恪、郑旭、欧阳劲松等。

引　言

由电气和电子器件构成的系统，多年来在许多领域中执行其安全功能，以计算机为基础的系统（一般指可编程电子系统（PES））在许多领域中用于非安全目的，但也越来越多地用于安全目的，为使计算机系统技术更有效安全地使用，有必要进行安全方面的指导。

GB/T 20438 针对由电气或电子和可编程电子部件构成的、起安全作用的电气/电子/可编程电子系统（E/E/PES）的整体安全生命周期，提出了一个通用的方法。建立统一的方法的目的是为了针对以电子为基础的安全相关系统提出一种一致的、合理的技术方针，主要目标是促进应用领域标准的制定。

在许多情况下，可用多种基于不同技术的防护系统来保证安全（如机械的、液压的、气动的、电气的、电子的、可编程电子的，等等）。从安全战略角度，不仅要考虑各系统中元器件的问题（如传感器、控制器、执行器等），而且要考虑构成组合安全相关系统的所有安全相关系统。因此 GB/T 20438 对电气/电子/可编程电子（E/E/PE）安全相关系统进行了规定。GB/T 20438 还提出了一个框架，在这个框架内，基于其他技术的安全相关系统也可同时被考虑进去。

在各种应用领域里，存在着许多潜在的危险和风险，包含的复杂性也各不相同，从而需应用不同的 E/E/PES。对每个特定的应用，则根据应用的不同而确定所需的安全量。GB/T 20438 仅是使这些量值规范化。

GB/T 20438

——考虑了当使用 E/E/PES 执行安全功能时，所涉及到的整体安全生命周期、E/E/PES 安全生命周期以及软件生命周期的各阶段（如初始构思，整个设计、实现、运行和维护到停用）。

——针对飞速发展的技术，建立一个足够健壮而广泛的能满足今后发展需要的框架。

——有利于促进 E/E/PES 安全相关系统在不同领域中相关标准的制定，各应用领域和交叉应用领域相关标准应在 GB/T 20438 的框架下制定，使之具有高水平的一致性（如基础原理，术语等的一致性），并将既安全又经济。

——为达到 E/E/PE 安全相关系统所需的功能安全，提供了编制安全要求规范的方法。

——使用了一个安全完整性等级，此安全完整性等级规定了 E/E/PE 安全相关系统要实现的安全功能的目标安全完整性等级。

——采用了一种可确定安全完整性等级要求的基于风险的方案。

——建立了 E/E/PE 安全相关系统的数值目标失效量，这些量都同安全完整性等级相联系。

——建立了危险失效模式中目标失效量的一个下限，此下限是对单一 E/E/PE 安全相关系统的要求。这些系统运行在：

1）低要求操作模式下，为了执行它的设计功能，一旦要求时，就把下限设定成平均失效概率为 10^{-5}；

2）高要求操作模式或者连续操作模式下，下限设定成危险失效概率为 10^{-9}/h。

注：单一 E/E/PE 安全相关系统不一定是单通道结构。

——采用广泛的原理、技术和措施以达到 E/E/PE 安全相关系统的功能安全，但不使用失效-安全的概念，这个概念是在很好定义了失效模式，并且复杂性相对较低时的一个数值。由于 E/E/PE 安全相关系统的复杂性均在 GB/T 20438 范围之内，因此不适用失效-安全的概念。

目　次

电气/电子/可编程电子安全相关系统的功能安全　第3部分:软件要求

1　范围

1.1　GB/T 20438的本部分:

a)　使用应建立在充分理解GB/T 20438.1、GB/T 20438.2的基础上。

b)　适用于任何在GB/T 20438.1、GB/T 20438.2范围内构成与安全相关系统的一部分有关的或用于开发安全相关系统的软件。这种软件定义为安全软件。

——安全软件包括操作系统、系统软件、通信网络中的软件、人机界面功能、支持工具、固件以及应用程序。

——应用程序包括高级语言、低级语言程序和使用有限可变语言的特殊用途程序(见GB/T 20438.4—2006的3.2.7)。

c)　软件安全功能和软件安全完整性等级的要求应明确。

注1:如果这一要求作为电气/电子/可编程安全相关系统(见GB/T 20438.2—2006的7.2)有一部分已提出,则在此处不需重复。

注2:规定软件安全功能和软件安全完整性等级是一个重复的程序,见图2和图6。

注3:文档结构要求见GB/T 20438.1—2006的第5章和GB/T 20438.1—2006的附录A。文档结构应考虑公司规程和特殊应用领域的工作实际情况。

d)　建立安全生命周期阶段和在设计、开发与安全有关的软件(软件安全生命周期软件模块)阶段和行为的要求。这些要求包括根据安全完整性等级分等的、在软件中用于避免和控制故障及失效的措施和技术的应用。

e)　对向执行电气/电子/可编程集成的机构提供与软件安全性确认有关的信息提出要求。

f)　对操作和维护E/E/PE安全相关系统的用户所需的与软件有关的信息和规程的准备提出要求。

g)　对修改与安全有关的软件的机构提出要求。

h)　结合GB/T 20438.1、GB/T 20438.2提出对支持工具的要求,如设计开发工具、语言翻译器、测试和调试工具、配置管理工具。

注4:图4和图6表示了GB/T 20438.2和GB/T 20438.3之间的关系。

1.2　GB/T 20438.1、GB/T 20438.2、GB/T 20438.3和GB/T 20438.4是基础的安全标准,尽管它们不适用于简单E/E/PE安全相关系统(见GB/T 20438.4—2006的3.4.4),作为基础的安全标准,根据IEC导则104和ISO/IEC导则51中包含的原则,各技术委员会在起草标准时应考虑使用这些标准,因为技术委员会的责任之一是在起草自己标准时凡是适用之处都应贯彻基础安全标准。GB/T 20438同时也可作为独立的标准去使用。

1.3　图1表示了GB/T 20438的整体框架同时明确了在达到E/E/PE安全相关系统功能安全阶段中本部分的作用。GB/T 20438.6—2006的附录A描述了GB/T 20438.2和GB/T 20438.3的应用。

2　规范性引用文件

下列文档中的条款通过GB/T 20438的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

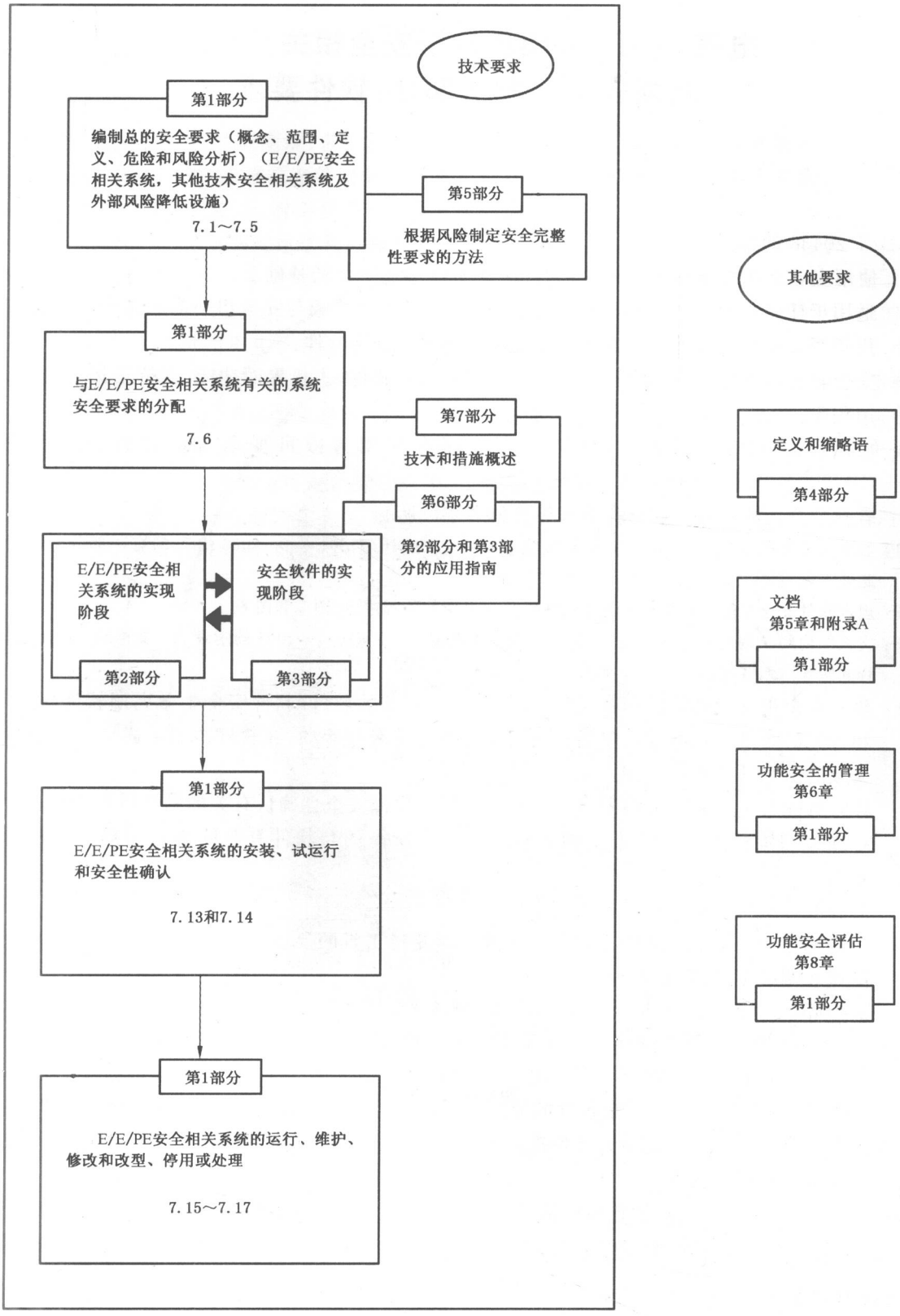


图 1　GB/T 20438 的总体框架

GB/T 20438.1—2006 电气/电子/可编程电子安全相关系统的功能安全 第1部分:一般要求(IEC 61508-1:1998,IDT)

GB/T 20438.2—2006 电气/电子/可编程电子安全相关系统的功能安全 第2部分:电气/电子/可编程电子安全相关系统的要求(IEC 61508-2:2000,IDT)

GB/T 20438.4—2006 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语(IEC 61508-4:1998,IDT)

GB/T 20438.5—2006 电气/电子/可编程电子安全相关系统的功能安全 第5部分:确定安全完整性等级的方法示例(IEC 61508-5:1998,IDT)

GB/T 20438.6—2006 电气/电子/可编程电子安全相关系统的功能安全 第6部分:GB/T 20438.2和GB/T 20438.3的应用指南(IEC 61508-6:2000,IDT)

GB/T 20438.7—2006 电气/电子/可编程电子安全相关系统的功能安全 第7部分:技术和措施概述(IEC 61508-7:2000,IDT)

ISO/IEC 导则51:1990 安全方面 在标准中引入安全条款的指南

IEC 导则104:1997 安全出版物的编写及基本安全出版物和分类安全出版物的应用

3 定义和缩略语

见GB/T 20438.4。

4 标准的符合性

见GB/T 20438.1—2006的第4章。

5 文档

见GB/T 20438.1—2006的第5章。

6 软件质量管理系统

6.1 目的

见GB/T 20438.1—2006的6.1。

6.2 要求

6.2.1 见GB/T 20438.1—2006的6.2,以下为附加要求。

6.2.2 功能安全计划应定义E/E/PE安全相关系统的安全完整性等级所要求的软件获取、开发、集成、确认和修改的战略。

注:该方法的理念是在编制计划时考虑E/E/PE安全相关系统部件所要求的各种安全完整性,制定标准。本部分的7.4.2.8将考虑E/E/PE安全相关系统中使用不同安全完整性等级的组件时的情况。

6.2.3 软件配置管理

a) 应在软件安全生命周期阶段中使用行政和技术控制,以管理软件变化和保证有关软件安全的规定要求始终能得到满足。

b) 应确保所有必需的操作已被执行以说明获得了所要求的软件安全完整性。

c) 应保持精确的和维护E/E/PE安全相关系统完整性所必需的所有配置项的唯一识别。配置项至少包括:安全分析和要求;软件规范和设计文档;软件源代码模块;测试计划和结果;将要被安装于E/E/PE安全相关系统的已存在的软件组件和软件包;所有用于创建、测试或执行E/E/PE安全相关系统软件的工具和开发环境。

d) 应采用变更控制规程用于防止非授权的修改;对修改请求文档化;分析建议修改的影响以批准或拒绝请求;对所有准许修改的细节和授权文档化;在软件开发阶段中适当点建立配置基线,并对判断基线(部分)的集成测试文档化(见7.8);确保所有软件基线的构成(包括早期基

线的重建)。

注:为指导、加强行政和技术控制的使用,有必要进行管理决定和授权。

e) 应对下列信息文档化,以用于随后的审核:配置状态、发布状态、对所有修改的判断和通过、修改的细节。

f) 安全软件发布应正式文档化。软件的主要备份和所有有关文档在已发布软件的操作生命周期内应被保存以允许维护和修改。

注:对于配置管理的更详细的信息,见 ISO/IEC 12207。

7 软件安全生命周期要求

7.1 一般要求

7.1.1 目的

将软件开发纳入到规定的各阶段和活动中(见表 1 和图 2～图 5)。

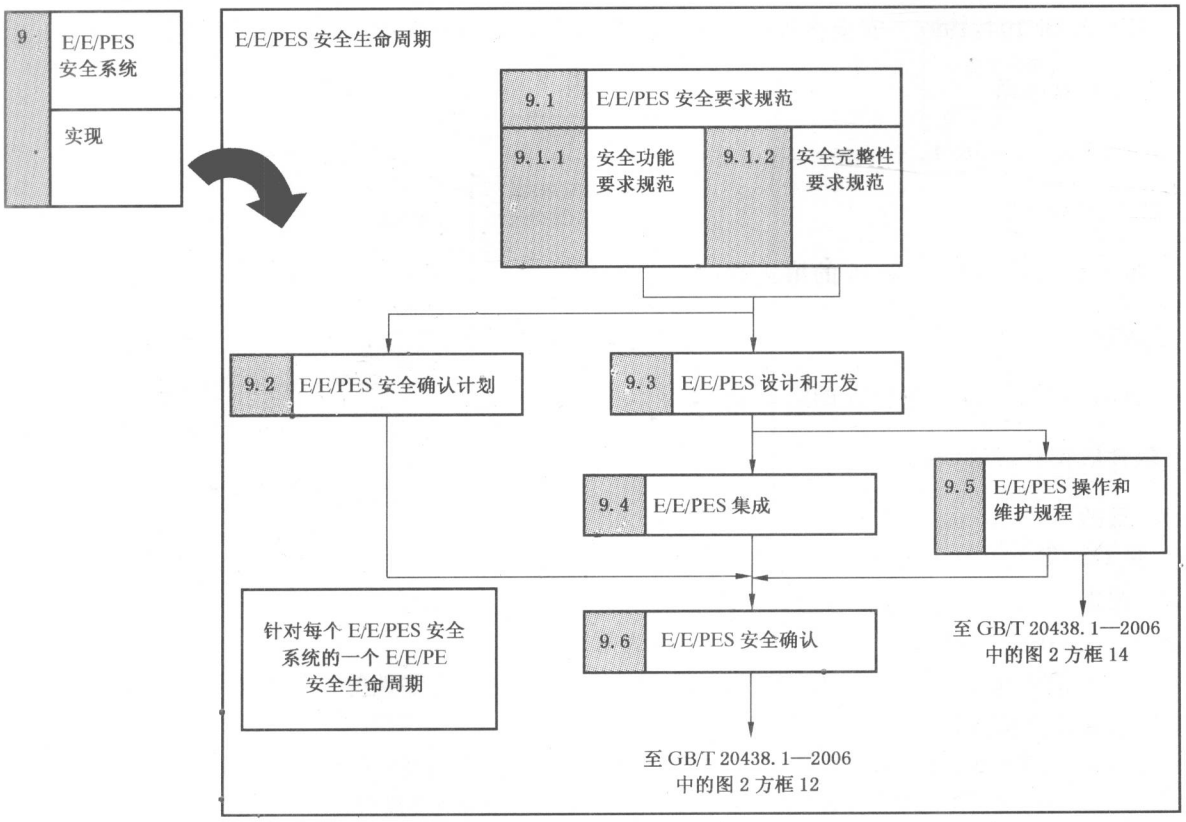


图 2 E/E/PE 安全生命周期(实现阶段)

7.1.2 要求

7.1.2.1 软件开发的安全生命周期应根据 GB/T 20438.1—2006 第 6 章在编制安全计划期间进行挑选和规定。

注:一个满足 GB/T 20438.1—2006 第 7 章要求的安全生命周期模型可根据某工程项目或机构的特殊需要来定制。

7.1.2.2 质量和安全保证规程应集成到安全生命周期活动中。

7.1.2.3 软件安全生命周期的各阶段应根据各阶段规定的范围、输入和输出分成基本的活动。

注 1:对于生命周期各阶段的更详细的信息,见 ISO/IEC 12207。

注 2:GB/T 20438.1—2006 第 5 章考虑了安全生命周期各阶段的输出。在开发一些 E/E/PE 安全相关系统的阶段中,一些安全生命周期阶段的输出可能是一个明确的文档,而从几个阶段输出的文档可被合并。基本的要求是安全生命周期阶段的输出应符合其预定的目的。在简单开发阶段中,一些安全生命周期阶段可被合并(见 7.4.5)。

7.1.2.4 假如软件安全生命周期满足图3和表1要求，允许根据项目的安全完整性和复杂性改变V模型中阶段的深度、数量和工作范围。

注：表1中所有生命周期阶段的列表适用于大型新开发的系统。在小系统中也可能适用，例如合并软件系统设计和结构设计阶段。

7.1.2.5 在本条所有的目的和要求可以满足时，允许以不同于GB/T 20438组织结构的其他方式编排软件工程项目(如使用其他的软件安全生命周期模型)。

7.1.2.6 对每一个生命周期阶段，应使用适当的技术和措施。附录A和附录B给出了推荐。只通过从附录A和附录B中选择技术不能保证能满足安全完整性的要求。

7.1.2.7 软件安全生命周期中的活动结果应文档化(见第5章)。

7.1.2.8 如果在软件安全生命周期的任一阶段，要求生命周期的前一阶段改变时，则应重复安全生命周期的前一阶段和随后的阶段。

表1 软件安全生命周期：概述

安全生命周期阶段		目的	范围	要求所在的条款	输入(要求的信息)	输出(产生的信息)
图3中的方框号	标题					
9.1	软件安全要求规范	根据软件安全功能要求和软件安全完整性要求规定软件安全要求； 对每个需实现一定安全功能的E/E/PES安全相关系统规定软件安全功能的要求； 规定每一个E/E/PES安全相关系统对于软件集成的要求，以保证获得这一E/E/PES系统分配的每一安全功能需达到的安全完整性等级	PES； 软件系统	7.2.2	E/E/PES安全要求规范(GB/T 20438.2)	软件安全要求规范
9.2	软件安全确认计划编制	拟定软件安全确认计划编制	PES； 软件系统	7.3.2	软件安全要求规范	软件安全确认计划
9.3	软件设计和开发	结构： 创建软件结构以满足不同的安全完整性等级中对软件安全规定要求； 复审和评价E/E/PES安全相关系统硬件结构对软件的要求，包括E/E/PES系统中软件和硬件相互作用对受控设备安全性的影响	PES； 软件系统	7.4.3	软件安全要求规范； E/E/PES硬件结构设计(见GB/T 20438.2)	软件结构设计描述； 软件结构集成测试规范； 软件/可编程电子集成测试规范(同GB/T 20438.2的要求)
		支持工具和编程语言： 在用于辅助验证、确认、评价和修改的软件的整个生命周期中，根据要求的安全完整性等级选择合适的工具集，包括语言和编译器	PES； 软件系统； 支持工具； 编程语言	7.4.4	软件安全要求规范； 软件结构设计描述	开发工具和编码标准； 开发工具的选择

表 1(续)

安全生命周期阶段		目的	范围	要求所在的条款	输入(要求的信息)	输出(产生的信息)
图 3 中的方框号	标题					
9.3	软件设计和开发	详细设计和开发(软件系统设计): 设计和实现软件,以满足不同的安全完整性等级对软件安全的规定要求,这种软件可分析、验证并能被安全地修改	软件结构设计的主要组件和子系统	7.4.5	软件结构设计描述; 支持工具和编码标准	软件系统设计描述; 软件系统集成测试规范
		详细设计和开发(单个软件模块设计): 设计和实现软件,以满足不同的安全完整性等级对软件安全的规定要求,这种软件可分析、验证并能被安全地修改	软件系统设计	7.4.5	软件系统设计规范; 支持工具和编码标准	软件模块设计规范; 软件模块测试规范
		详细代码实现: 设计和实现软件,以满足不同的安全完整性等级对软件安全的规定要求,这种软件可分析、验证并能被安全地修改	单个软件模块	7.4.6	软件模块设计规范; 支持工具和编码标准	源代码清单; 代码复审报告
		软件模块测试: 验证已满足软件安全要求(根据规定的软件安全功能和软件安全完整性),说明每一软件模块实现其预定的功能,不实现非预定的功能	软件模块	7.4.7	软件模块测试规范; 源代码清单; 代码复审报告	软件模块测试结果; 验证和测试软件模块
		软件集成测试: 验证已满足软件安全要求(根据规定的软件安全功能和软件安全完整性),说明所有软件模块、组件和子系统相互正确作用来实现其预定的功能,不实现非预定的功能	软件结构; 软件系统	7.4.8	软件系统集成测试规范	软件系统集成测试结果; 验证和测试软件系统;
9.4	PE 集成(硬件和软件)	在目标可编程电子硬件上集成软件; 将软件和硬件结合到与安全有关的可编程电子上以保证其兼容性和满足预定安全完整性等级的要求	可编程电子硬件; 集成软件	7.5.2	软件结构集成测试规范; 可编程电子集成测试规范(同 GB/T 20438.2 要求); 集成可编程电子	软件结构集成测试结果; 可编程电子集成测试结果; 验证和测试集成的可编程电子

表 1(续)

安全生命周期阶段		目的	范围	要求所在的条款	输入(要求的信息)	输出(产生的信息)
图 3 中的方框号	标题					
9.5	软件操作和修改规程	提供软件有关的信息和规程以保持操作和修改阶段中 E/E/PE 安全相关系统的功能安全	同上	7.6.2	与上面所有内容相关的	软件操作和修改规程
9.6	软件安全确认	保证集成系统符合在预定安全完整性等级上对软件安全的规定要求	同上	7.7.2	软件安全确认计划	软件安全确认结果; 已确认软件
—	软件修改	修正、增强或调整确认软件以保证维持所要求的软件安全完整性等级	同上	7.8.2	软件修改规程; 软件修改请求	软件修改影响分析结果; 软件修改日志
—	软件验证	达到所需的安全完整性等级,测试和评价给定软件安全生命周期阶段的输出,以保证当输入该阶段时提供的输出与标准的正确性和一致性	根据阶段	7.9.2	适当的验证计划(根据阶段)	适当的验证报告(根据阶段)
—	软件功能安全评估	调查和对 E/E/PE 安全相关系统所获得的功能安全做出判断	所有以上阶段	8	软件功能安全评估计划	软件功能安全评估报告

7.2 软件安全要求规范

注 1:另见表 A.1 和表 B.7。

注 2:这一阶段是图 3 中的方框 9.1。

7.2.1 目的

7.2.1.1 根据软件安全功能要求和软件安全完整性要求规定软件安全要求。

7.2.1.2 对每个需实现一定安全功能的 E/E/PES 安全相关系统规定软件安全功能的要求。

7.2.1.3 规定每一个 E/E/PES 安全相关系统对于软件集成的要求,以保证获得这一 E/E/PES 系统分配的每一安全功能需达到的安全完整性等级。

7.2.2 要求

注:这些要求大多情况下可由通用嵌入软件和特殊应用软件共同满足。要求两者结合来提供满足下列条款的特性。两者之间的精确划分依据所选择的软件结构(见 7.4.3 和图 6)。

7.2.2.1 如果软件安全的要求已在 E/E/PE 安全相关系统的要求中规定(见 GB/T 20438.2—2006 的 7.2),则此处不必重复。

7.2.2.2 软件安全要求的规定应由 E/E/PE 安全相关系统规定的安全要求和任一安全计划编制的要求(见第 6 章)中得出(见 GB/T 20438.2),软件开发人员应能获取这些信息。

注:这一要求并不意味着 E/E/PES 开发人员和软件开发人员之间没有重复(GB/T 20438.2 和 GB/T 20438.3),当软件安全要求和软件结构(见 7.4.3)变得更加精确时,将会对 E/E/PES 硬件结构产生影响,因此软件和硬件开发人员之间的密切合作就变得非常必要了,见图 4。

7.2.2.3 软件安全要求的规定应足够细致以使设计和实现能获得要求的安全完整性,并允许执行功能安全的评估。

注:规范的细致程度可根据应用的复杂程度确定。

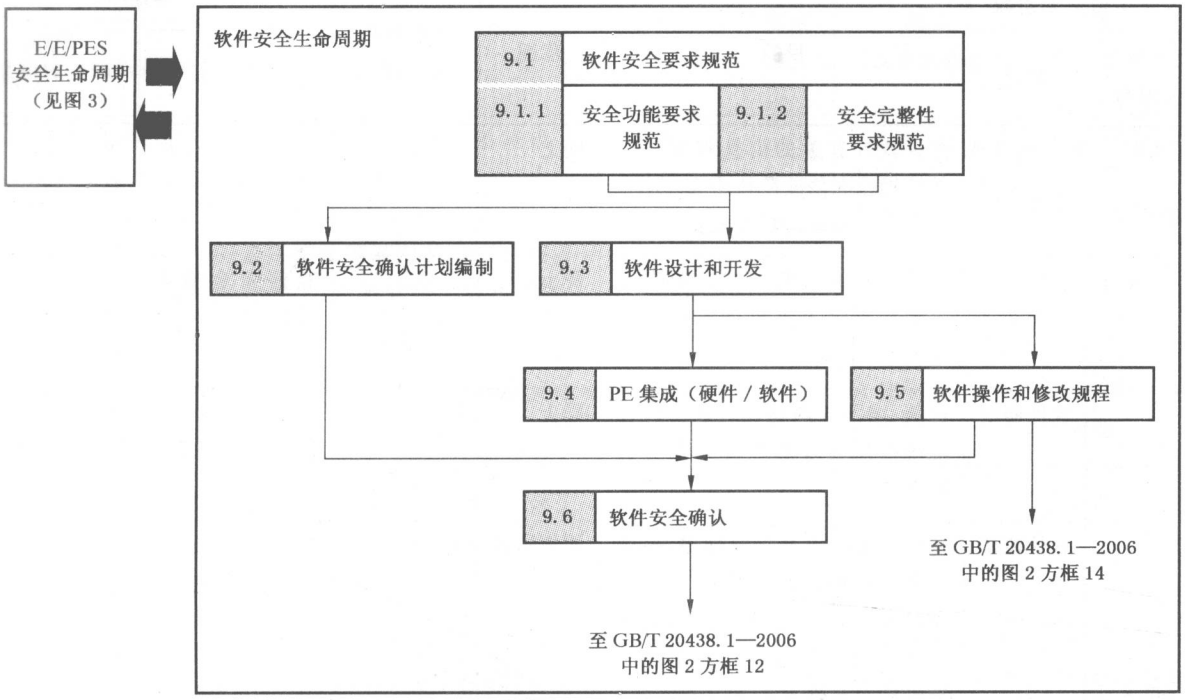


图 3　软件安全生命周期（实现阶段）

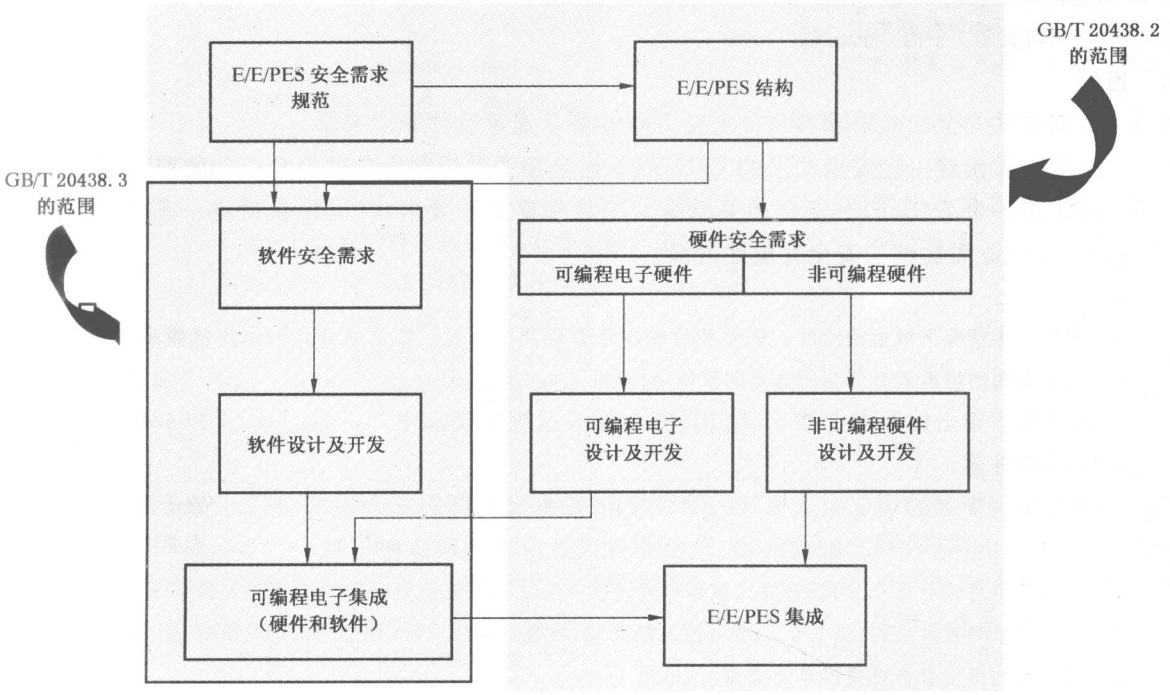


图 4　GB/T 20438.2 和 GB/T 20438.3 的范围及关系

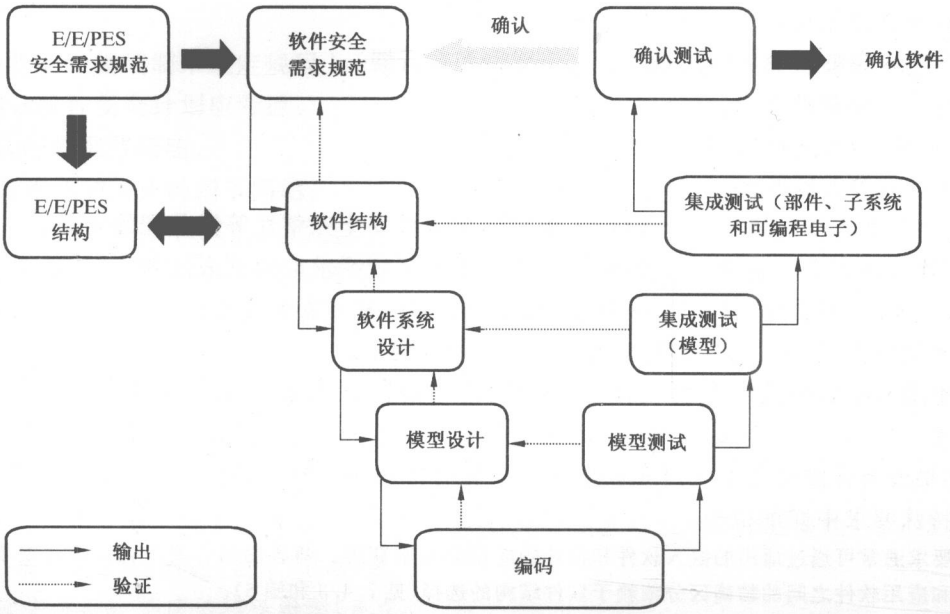
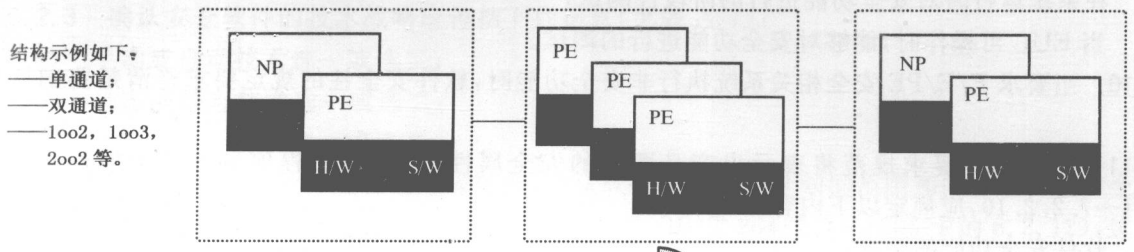


图 5　软件安全完整性的开发生命周期(V 模式)



可编程电子结构		
PE 硬件结构	PE 软件结构（S/W 结构包括嵌入 S/W 和应用 S/W）	
PE 硬件中通用特性和特殊应用特性：	PE 嵌入软件	PE 应用软件
示例包括：	示例包括：	示例包括：
——诊断测试；	——通信驱动器；	——输入 / 输出功能；
——冗余处理器；	——故障处理；	——派生功能（如不作为嵌入软件服务的检测传感器）
——双 I/O 卡	——可执行软件	

关键词：PE——可编程电子；NP——非可编程装置；
H/W——硬件；S/W——软件；
MooN——N 中的 M(如 1oo2 为 2 中的 1)

图 6　可编程电子硬件和软件结构的关系

7.2.2.4 软件的开发人员应复审 7.2.2.2 中的信息以确保对要求全面规定，应特别考虑以下环节：

a) 安全功能；

b) 系统配置或结构；

c) 硬件安全完整性要求(可编程电子、传感器和执行器)；

d) 软件安全完整性要求；

e) 能力和响应时间性能；

f) 设备和操作人员界面。

7.2.2.5 软件开发人员应建立一个规程，以解决任何软件安全完整性等级分配的矛盾。

7.2.2.6 在要求的安全完整性等级范围内，软件安全的规定要求应得到表达和组织，以使其：

a) 清楚、准确、不含糊、可验证、可测量、可维护、可行，并与安全完整性等级相当；

b) 可回溯到 E/E/PE 安全相关系统的安全要求的规定；

c) 不使用不明确的或在软件安全生命周期任一阶段使用这些文档的人所不能理解的术语和描述。

7.2.2.7 如果没有详细定义 E/E/PE 安全相关系统的特殊安全要求，所有 EUC 的有关操作模式应在软件安全的特殊要求中详细说明。

注：这种要求通常可通过通用的嵌入软件和特殊的应用软件来获得。两者的结合要求提供满足要求的特性，通用软件和应用软件之间的精确区分依赖于软件结构的选择(见 7.4.3 和图 6)。

7.2.2.8 软件安全要求规范应对软件和硬件间的任何与安全有关的或相应的约束进行规范并文档化。

7.2.2.9 在 E/E/PE 硬件结构设计描述的范围内，软件安全规范应考虑如下内容：

a) 软件自监视(如见 GB/T 20438.7—2006 中的 C.2.5 和 C.3.10 的示例)；

b) 可编程电子硬件、传感器和执行器的监视；

c) 在系统运行时对安全功能进行的阶段性测试；

d) 当 EUC 可操作时，能够对安全功能进行的测试。

7.2.2.10 当要求 E/E/PE 安全相关系统执行非安全功能时，软件安全性的规定要求将清楚鉴别这些功能。

7.2.2.11 软件安全要求规范将表示出产品要求的安全属性，但不是工程项目的安全属性。参考 7.2.2.1～7.2.2.10，应规定以下内容：

a) 软件安全功能的要求：

——使 EUC 获得或维持安全状态的功能；

——与可编程电子硬件中故障的探测、通告和管理有关的功能；

——与传感器和执行器故障的探测、通告和管理有关的功能；

——与软件自身(软件自监视)中的故障的探测、通告和管理有关的功能；

——与在线安全功能阶段性检查有关的功能(软件自监视)；

——与离线安全功能阶段性检查有关的功能；

——允许 PES 安全修改的功能；

——非安全功能界面；

——能力和反应性能；

——软件与 PES 之间的界面。

注 1：界面包括在线和离线。

b) 软件安全完整性要求包括：

——以上 a)中每一功能的安全完整性等级。

注 2：在软件组件中分配安全完整性信息见 GB/T 20438.5—2006 中的附录 A。

7.3 软件安全确认计划编制

注：这一阶段对应图 3 中的方框 9.2。

7.3.1 **目的**

拟定软件安全确认计划编制。

7.3.2 **要求**

7.3.2.1 应执行计划编制来规定规程上和技术上步骤，用以证明软件满足其安全要求(见 7.2)。

7.3.2.2 确认软件安全计划应考虑：

a) 确认时的细节问题。

b) 执行确认的人员的细节问题。

c) EUC 操作的有关模式的识别包括：

——使用的准备，包括设置和调整；

——启动、教学、自动化、手动、半自动化、操作的稳定状态；

——重置、关机、维护；

——合理的可预见异常条件。

d) 在开始试运行前，需要确认 EUC 操作的每一模式安全软件的识别。

e) 确认的技术战略(如分析方法、统计测试等)(见 7.3.2.3)。

f) 根据 e)，用于确定符合软件安全功能(见 7.2)规定要求和软件安全完整性(见 7.2)规定要求的每一安全功能的措施(技术)和规程。

g) 软件安全规定要求的特殊参考(见 7.2)。

h) 进行确认活动时所需的环境(如测试将包括调校工具和设备)。

i) 通过/失败准则(见 7.3.2.5)。

j) 评价确认结果，特别是评价失效的方针和规程。

注：这些要求基于 GB/T 20438.1—2006 中 7.8 的一般要求。

7.3.2.3 确认安全软件的技术战略应包括下列信息(见表 A.7)：

a) 手动或自动技术选一或选二；

b) 动态或静态技术选一或选二；

c) 分析或统计技术选一或选二。

7.3.2.4 作为确认安全软件规程的组成部分，确认软件安全性的计划的范围和内容应根据安全完整性等级的要求由评估方或代表评估方的一方进行复审(见 GB/T 20438.1—2006 中的 8.2.12)，这一规程应就在测试中评估方的出席做出说明。

7.3.2.5 完成软件确认的通过/失败准则应包括：

a) 要求的输入信号及其次序和值；

b) 预期的输出信号及其次序和值；

c) 其他可接受的准则，如内存使用、定时、值的允许偏差。

7.4 **软件设计和开发**

注：这一阶段为图 3 中的方框 9.3。

7.4.1 **目的**

7.4.1.1 创建软件结构以满足不同的安全完整性等级中对软件安全的规定要求。

7.4.1.2 复审和评价 E/E/PES 安全相关系统硬件结构对软件的要求，包括 E/E/PES 系统中软件和硬件相互作用对受控设备安全性的影响。

7.4.1.3 用于辅助验证、确认、评价和修改的软件的整个的生命周期中，根据要求的安全完整性等级选择合适的工具集，包括语言和编译器。

7.4.1.4 设计和实现软件，以满足不同的安全完整性等级对软件安全的规定要求，这种软件可分析、可验证并能被安全地修改。

7.4.1.5 验证已满足软件安全要求(根据规定的软件安全功能和软件安全完整性)。