ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.1—2006/IEC 61508-1:1998

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

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1:General requirements

(IEC 61508-1:1998,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1部分:一般要求
GB/T 20438.1—2006/IEC 61508-1:1998
*
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 2.75 字数 77千字
2007年1月第一版 2007年1月第一次印刷
*
书号:155066·1-28708 定价 19.00元

GB/T 20438.1-2006

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，不仅要考虑各独立系统中所有元器件的问题（如传感器、控制器、执行器等），而且要考虑由所有安全相关系统构成的组合安全相关系统的问题。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，所需的安全措施将依赖于应用中的具体因素。GB/T 20438 使这些措施规范化，以便将来引入到应用部门标准中。

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安全生命周期的各阶段（如初始构思，整个设计、实现、运行、维护及停用）。

——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。

——采用了一种基于风险的方案来确定安全完整性等级要求。

——建立了 E/E/PE 安全相关系统的数值化目标失效量，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、技术和措施方法以达到 E/E/PE 安全相关系统的功能安全，但未使用失效-安全的概念，虽然这个概念在很好定义了失效模式和复杂性相对较低时可能非常有用。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

前　言

GB/T 20438 由下列几部分构成：

——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 1 部分。

本部分等同采用国际标准 IEC 61508-1:1998《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》(英文版)。

本部分的附录 A、附录 B 为资料性附录。

本部分与 IEC 61508-1:1998 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 b)，因为该项只适合于 IEC 61508-1 的法文版。

d) 删除国际标准中 1.4 中的注，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。

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/TC124)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：冯晓升、王莉、梅恪、郑旭、欧阳劲松等。

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

1　范围

1.1　GB/T 20438 包含电气/电子/可编程电子系统在执行安全功能时要考虑的各个方面。GB/T 20438的一个主要目的是促进各应用领域的技术委员会制定应用领域的国家标准。这样将能充分考虑与应用有关的所有因素,因此可满足应用领域的需要。GB/T 20438 的另一个目的是在没有应用领域国家标准的情况下能够开发电气/电子/可编程电子系统。

1.2　GB/T 20438 尤其:

a)　适用于包含有一个或几个电气/电子/可编程电子装置的安全相关系统。

注1:对于简单的 E/E/PE 安全相关系统,GB/T 20438 规定的有些要求是不必要的,可以不按这些要求(见 4.2 和 GB/T 20438.4—2006 的 3.4.4 中简单 E/E/PE 安全相关系统的定义)。

注2:尽管人也是安全相关系统的一部分(见 GB/T 20438.4—2006 的 3.4.1),但 GB/T 20438 未细致考虑 E/E/PE 安全相关系统设计中人的因素。

b)　包含了 E/E/PE 安全相关系统所执行的安全功能失效引起的可能危险,这种可能危险应与 E/E/PE设备本身产生的危险(如电击等)加以区分。

c)　不包括在如下情况时的 E/E/PE 系统:

——提供必要的风险降低能力的单一 E/E/PE 系统;并且

——E/E/PE 系统安全完整性的要求低于规定的安全完整性等级 1(GB/T 20438 规定的最低安全完整性等级)。

d)　主要针对其失效将对人和/或环境安全产生影响的 E/E/PE 安全相关系统;但是,失效的后果也将对经济产生严重影响。从这个角度讲,GB/T 20438 也涵盖了用于保护设备和产品的E/E/PE系统。

e)　考虑了 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施,以便能系统地、以基于风险的方式确定 E/E/PE 安全相关系统的安全规范。

f)　用整体安全生命周期模型作为技术框架,系统地论述了为保证 E/E/PE 安全相关系统功能安全所需的活动。

注3:整体安全生命周期的初期阶段如需要还可包括其他技术安全相关系统和外部风险降低设施,以便能系统地、以基于风险的方式制定 E/E/PE 安全相关系统的要求规范。

注4:整体安全生命周期尽管是针对 E/E/PE 安全相关系统提出的,但同时也提供了一个考虑任何安全相关系统的技术框架,而不论这种安全相关系统使用何种技术(例如机械的、液压的或气动的)。

g)　不对各领域应用规定安全完整性等级(这要以领域应用的详细信息和知识为基础),这要由负责制定各应用领域标准的技术委员会在相应的标准中做出规定。

h)　对于尚无标准的各应用领域提供一个 E/E/PE 安全相关系统的通用要求。

i)　不包括防止未经批准人员对 E/E/PE 安全相关系统的损伤和/或对 E/E/PE 安全相关系统的安全功能产生不利影响的预防措施。

1.3　本部分是一般要求,它适用于 GB/T 20438 所有部分。GB/T 20438 其他部分涉及更具体的问题:

——第 2 部分和第 3 部分对 E/E/PE 安全相关系统(硬件和软件)提出了更多的和具体的要求;

——第 4 部分规定 GB/T 20438 中使用的术语定义和缩略语;

——第 5 部分用举例的方法,对应用第 1 部分时如何确定安全完整性等级提供指南;

——第 6 部分给出了应用第 2 部分和第 3 部分的指南;

——第 7 部分包括技术和措施概述。

1.4 GB/T 20438.1、GB/T 20438.2、GB/T 20438.3、GB/T 20438.4 是基础安全标准，虽然它们不适用于简单的 E/E/PE 安全相关系统(见 GB/T 20438.4—2006 的 3.4.4)，但作为基础安全标准，各技术委员会可以在 IEC 导则 104 和 ISO/IEC 导则 51 的指导下制定相关标准时使用。对于每个技术委员会，都有责任在其制定的标准中使用基础标准。同时，GB/T 20438 也是一个可独立使用的标准。

1.5 图 1 表示了 GB/T 20438 的总体框架，同时明确了在达到 E/E/PE 安全相关系统功能安全过程中本部分的作用。

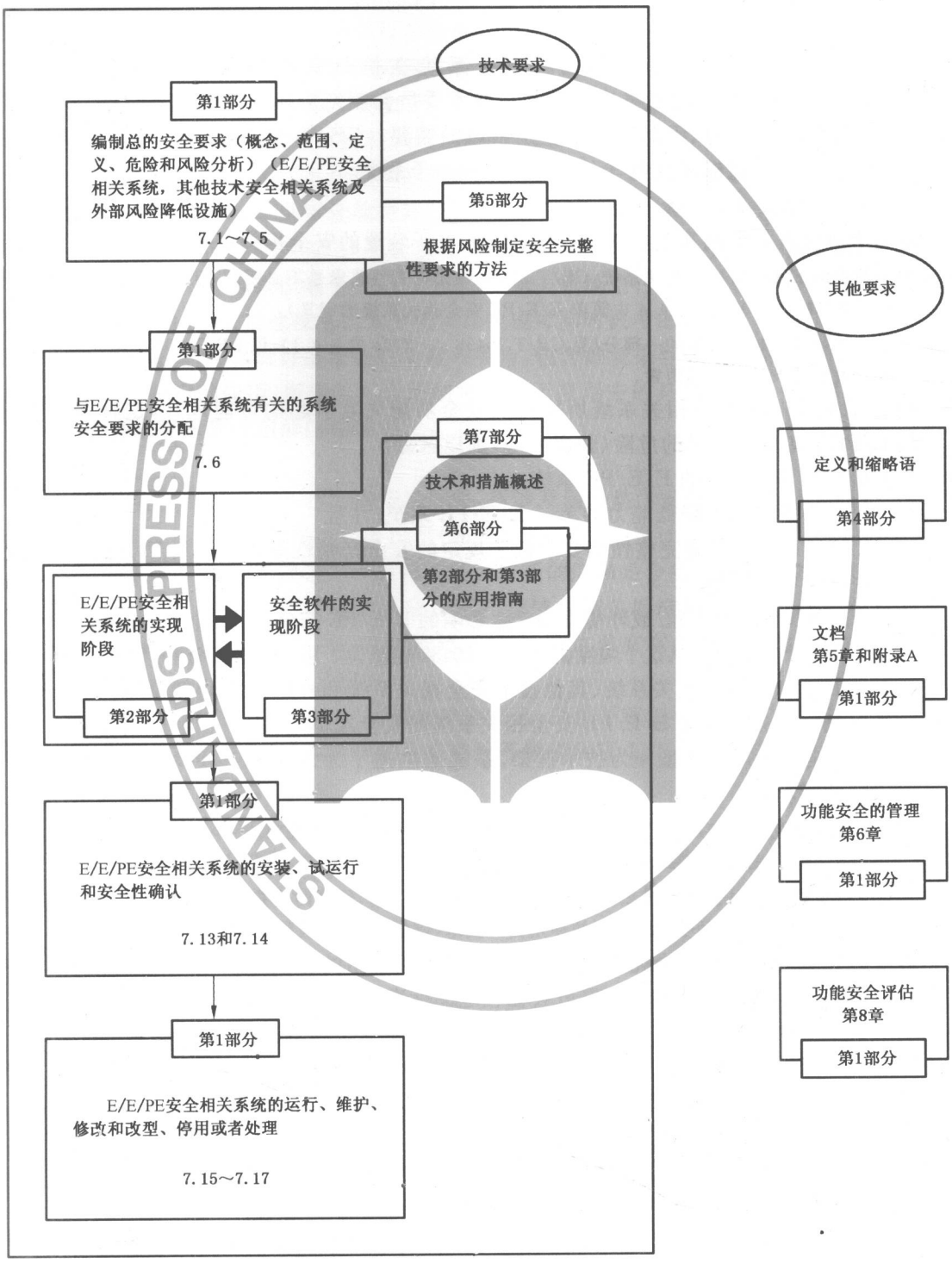


图 1 GB/T 20438 的总体框架

2 规范性引用文件

下列文件中的条款通过 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。

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：对电气/电子/可编程电子安全相关系统的要求(IEC 61508-2:2000，IDT)

GB/T 20438.3—2006 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(IEC 61508-3:1998，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出版物的应用

3 定义和缩略语

本部分采用 GB/T 20438.4—2006 中规定的定义和缩略语。

4 与 GB/T 20438 的符合性

4.1 要满足 GB/T 20438 的要求，必须证明提出的所有要求符合 GB/T 20438 的规定(如安全完整性等级)并已达到各章和各条的要求。

注：一般不能选择某一个参数来确定满足某一要求的程度(严格程度)，而是根据与整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期各阶段和活动有关的一些因素来确定，这些因素是：

——后果及风险降低；
——危险性质；
——安全完整性等级；
——实现技术类型；
——系统规模；
——涉及团队的数量；
——物理分布；
——设计的新颖程度。

4.2 GB/T 20438 规定了对 E/E/PE 安全相关系统的要求，以满足与这种系统相关联的全范围的复杂性。但对于简单的 E/E/PE 安全相关系统(见 GB/T 20438.4—2006 的 3.4.4)，如有能为达到要求的安全完整性提供必要的置信度的可靠现场经验的情况下，有下列几种选择：

——在有关应用领域标准中实现 GB/T 20438.1～GB/T 20438.7 要求时，有些要求也许不必要，不满足这些要求也是可接受的。

——如在有关领域没有相应标准，则可直接应用 GB/T 20438，如有理由认为 GB/T 20438 中的某些要求不必要，不满足这些要求也是可接受的。

4.3 按 GB/T 20438 框架开发的 E/E/PE 安全相关系统的应用领域国家标准，将包含 ISO/IEC 导则 51 和 IEC 导则 104 中的要求。

5 文档

5.1 目的

5.1.1 规定能够有效执行整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期各阶段所必需的信息，这些信息将被文档化。

5.1.2 规定能够有效执行功能安全管理(见第 6 章)、验证(见 7.18)以及功能安全评估等活动所必需的信息，这些信息也将被文档化。

注 1：GB/T 20438 要求的文档是信息方面的文档，而不是实际文档，这些信息不要求包括在实际文档之中，除非在相关条款中做了明确说明。

注 2：文档可以有不同的形式(如纸张、胶片或任何可显示于屏幕或显示器上的数据媒体)。

注 3：有关可能的文档结构见附录 A。

注 4：见参考文献[4]。

5.2 要求

5.2.1 文档中应包括 E/E/PES 的和软件的以及整体的安全生命周期中各阶段的足够信息，这些信息是有效执行各阶段和验证活动所必需的。

注：什么是足够的信息取决于许多因素，包括 E/E/PE 安全相关系统的复杂程度和系统规模以及具体应用的有关要求。

5.2.2 文档中应包括管理功能安全所要求的足够信息(见第 6 章)

注：见 5.1.2 的注。

5.2.3 文档中应包括实现功能安全评估所需的足够信息，也包括从任何功能安全评估得到的结果和信息。

注：见 5.1.2 的注。

5.2.4 除了在功能安全计划编制中已作调整或应用领域标准中已规定外，要文档化的信息应同 GB/T 20438各章中所述一样。

5.2.5 相对于标准的条款，文档应足够充分以便于执行。

注：承担特定活动并被 GB/T 20438 所需要的信息才有必要列于相关部分。

5.2.6 文档应：

——准确简明；

——让使用者容易理解；

——能达到预期目的；

——可存取和可维护。

5.2.7 文档或信息集应有指示内容的标题或名称，以及一些形式的检索，以便于访问标准中所需的信息。

5.2.8 文档的结构可根据公司规程和应用领域的工作实践来确定。

5.2.9 文档或信息集应有修订检索(版本号)，以区别文档的不同版本。

5.2.10 文档或信息集应结构化以便于查找相关信息，以及易于识别文档或信息集的最新修订版(版本)。

注：文档的实际结构应根据多种因素而改变，如系统规模、复杂程度和组织要求。

5.2.11 所有有关文档应修订、补充、复审、批准，并按照适当的文档控制方案进行控制。

注：在用自动或半自动工具产生文档的情况下，专用规程对保证措施的有效性是必要的，这些工具在管理版本或控制文档的其他方面时应安装到位。

6 功能安全的管理

6.1 目的

6.1.1 确定整体的、E/E/PES 的和软件的安全生命周期所有阶段的管理和技术活动。这些阶段是达到 E/E/PE 安全相关系统要求的功能安全所必需的。

6.1.2 确定人员、部门和机构对整体的、E/E/PES 的和软件的安全生命周期各阶段或各阶段中活动所负的责任。

注：本章中涉及的组织措施用于有效实现技术要求并仅针对达到和保持 E/E/PE 安全相关系统的功能安全。保持功能安全所需的技术要求一般作为 E/E/PE 安全相关系统供货商提供的信息的一部分。

6.2 **要求**

6.2.1 为确保 E/E/PE 安全相关系统达到并保持所要求的功能安全，对整体的、E/E/PES 的或软件的安全生命周期的一个或几个阶段负全责的组织或个人应规定所有的管理和技术活动，尤其要考虑以下各点：

a) 达到功能安全的方针和战略、以及是否达到的评价方法，和为确保安全作业的素质，在组织内部进行交流的方法。

b) 对整体的、E/E/PES 的或软件的安全生命周期各阶段负责执行和复核的人员、部门或组织的识别(包括有关的发证当局或安全管理机构)。

c) 整体的、E/E/PES 的或软件的安全生命周期被实施的阶段。

d) 信息结构化和扩展信息文档化的方法(见第 5 章)。

e) 用于满足某一规定条款要求所选的措施或技术。

f) 功能安全评估活动(见第 8 章)。

g) 对 E/E/PE 安全相关系统建议的满意解决和及时跟踪的规程，可由下列几项得出：

——危险和风险分析(见 7.4)；

——功能安全评估(见第 8 章)；

——验证活动(见 7.18)；

——确认活动(见 7.8 和 7.14)；

——配置管理(见 6.2.1 的 o)，7.16 和 GB/T 20438.2 及 GB/T 20438.3)。

h) 保证与整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期活动有关的相应责任部门的规程能胜任其活动，尤其应规定下列几点：

——对工作人员进行针对诊断和修复故障以及系统测试的培训；

——操作人员的培训；

——对工作人员进行定期再培训。

注 1：附录 B 给出了整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期任何活动中人的资格要求的指南。

i) 保证危险事故(或产生危险的潜在事故)分析，以及提出使其重复发生的概率降到最低之建议的规程。

j) 对操作和维护性能进行分析的规程，尤其是：

——识别危及功能安全的系统故障的规程，包括用于检测重复性故障的日常维护所使用的规程；

——评估需求率和在操作和维护期间的失效率是否和系统设计期间的假设一致。

k) 本条的定期功能安全审核要求，包括：

——功能安全审核频率；

——审核责任部门和人员的独立性水平的考虑；

——文档和后续活动。

l) 启动对安全相关系统进行修改的规程(见 7.16.2.2)。

m) 进行修改所需要的批准规程和主管部门。

n) 保持潜在危险和安全相关系统信息准确的规程。

o) 在整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期阶段中，E/E/PE 安全相关系统的配置管理规程，尤其要对下列各项进行规定：

——实现正式配置控制的阶段；

——用于对一个项(硬件和软件)的全部要素进行唯一标识的规程；

——防止未授权项进入服务的规程；

注 2：管理的细节参见参考文献[7]和[8]。

p) 在适当场合的培训条款和应急服务信息。

6.2.2 应实现并连续监视由 6.2.1 所规定的活动。

6.2.3 由有关机构正式复审根据 6.2.1 所编制的要求并取得一致。应正式得到相关机构的评审，并得到最终签署。

6.2.4 应告知所有对功能安全活动负有管理责任的各方分配给他们的职责。

6.2.5 对于对整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期(见 6.2.1)的一个或多个阶段负全责的组织，供方应按其规定提供产品和服务，并应具有适当的质量管理系统。

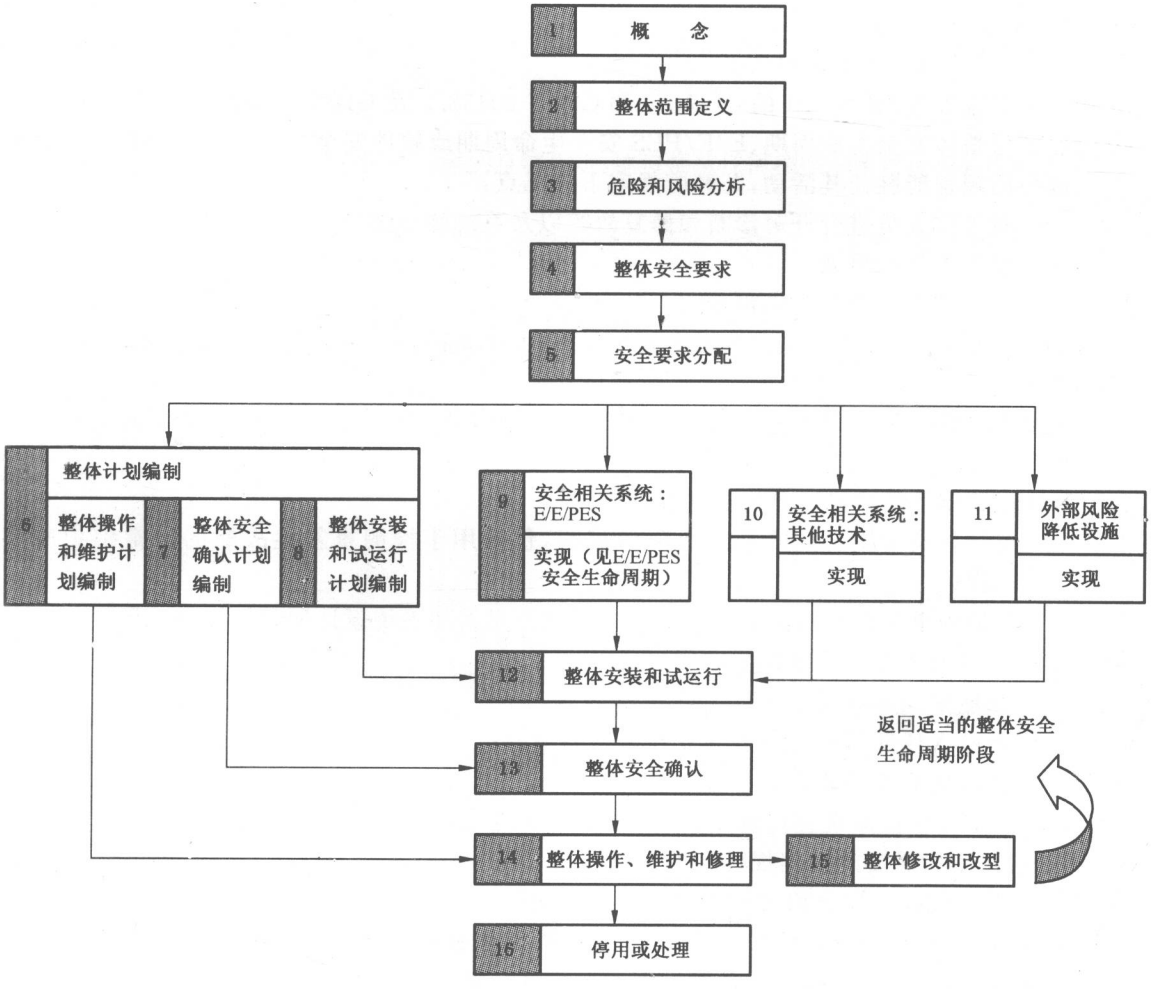
7 整体安全生命周期的要求

7.1 一般要求

7.1.1 简介

7.1.1.1 为了系统地安排为达到要求的 E/E/PE 安全相关系统安全完整性等级所需的全部活动，GB/T 20438采用了一种整体安全生命周期的技术框架(见图 2)。

注：图 2 所示为 GB/T 20438 应满足的目的和要求，整体安全生命周期应作为声明对 GB/T 20438 符合性的一个基础，此外不同的整体安全生命周期也可使用图 2。



注 1：为清楚起见，与功能安全验证、功能安全管理以及功能安全评估有关的活动未在图中显示，但这些都与整体的、E/E/PES 的和软件的安全生命周期各阶段有关。

注 2：方框 10 和 11 所表示的阶段不在 GB/T 20438 范围之内。

注 3：GB/T 20438.2 和 GB/T 20438.3 涉及方框 9(实现)，但有关部分也涉及方框 13、14 和 15 的可编程电子方面(硬件和软件)。

图 2 整体安全生命周期

7.1.1.2 整体安全生命周期包含下列风险降低的方法：

——E/E/PE 安全相关系统；

——其他技术安全相关系统；

——外部风险降低设施。

7.1.1.3 在整体安全生命周期中，涉及 E/E/PE 安全相关系统的组成部分被扩展并示于图 3。它定义了 E/E/PES 安全生命周期并构成了 GB/T 20438.2 的技术框架。图 4 显示了软件安全生命周期并构成了 GB/T 20438.3 的技术框架。图 5 显示了整体安全生命周期中 E/E/PES 安全生命周期和软件安全生命周期之间的关系。

7.1.1.4 整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期图(图 2～图 4)仅是实际情况的一个简化图，尚未涉及细节，整体的 E/E/PES 的和软件的安全生命周期的基础部分是由这些细节来描述的。

7.1.1.5 有关功能安全的管理(见第 6 章)、验证(7.18)和功能安全评估(见第 8 章)的活动没有表示在整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期中，这样做是为了减少整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期图的复杂性。必要时，这些活动可加到整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期的相关阶段中。

7.1.2 目的和要求：一般要求

7.1.2.1 整体安全生命周期各阶段的目的和要求规定于 7.2～7.17，相应的 E/E/PES 和软件的安全生命周期各阶段的目的和要求规定于 GB/T 20438.2 和 GB/T 20438.3 中。

注：7.2～7.17 对应于图 2 的特定方框(阶段)，这一信息在相应各条款的注中有说明。

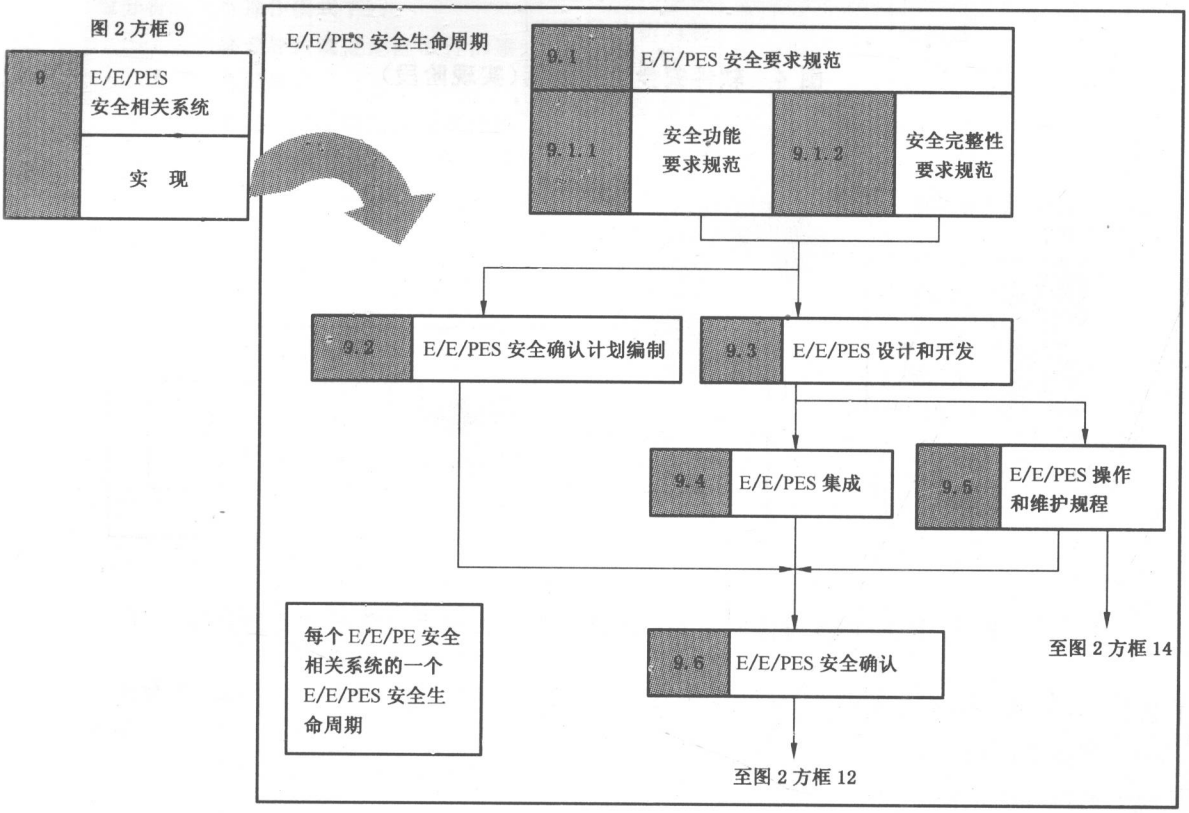


图 3 E/E/PES 安全生命周期(实现阶段)

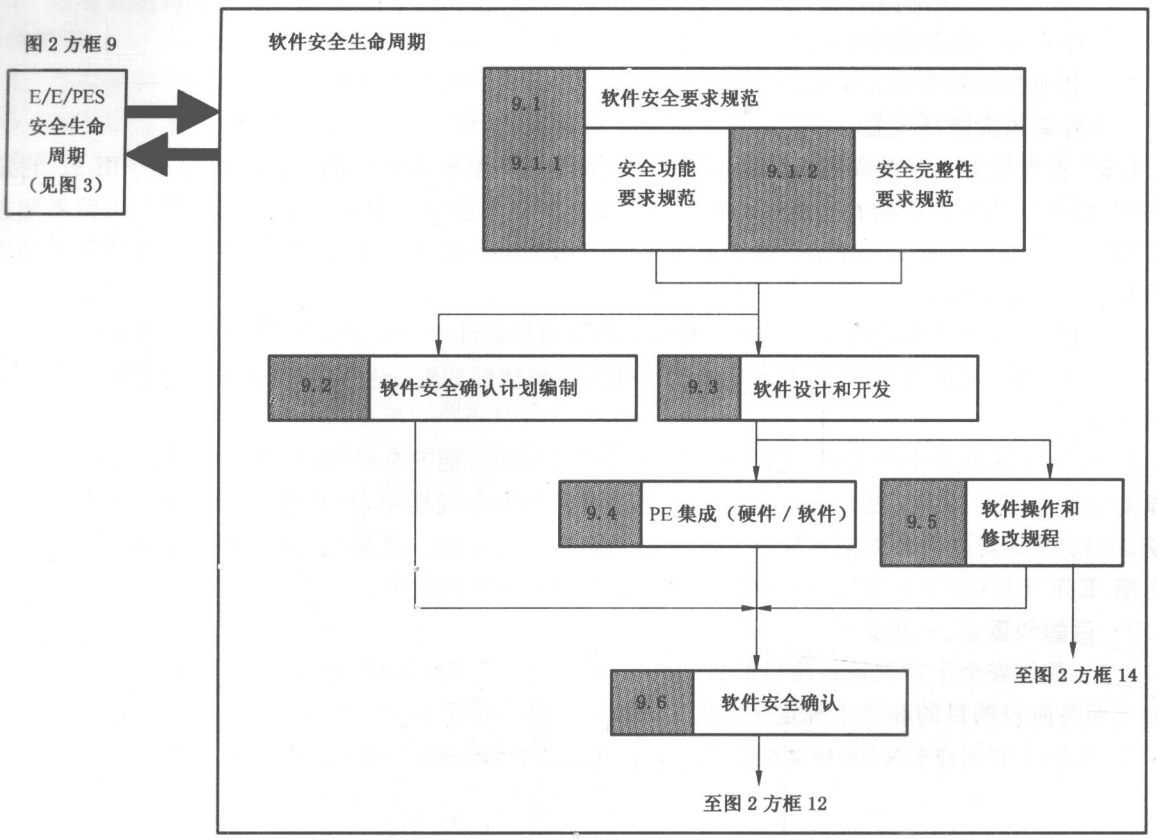


图 4　软件安全生命周期(实现阶段)

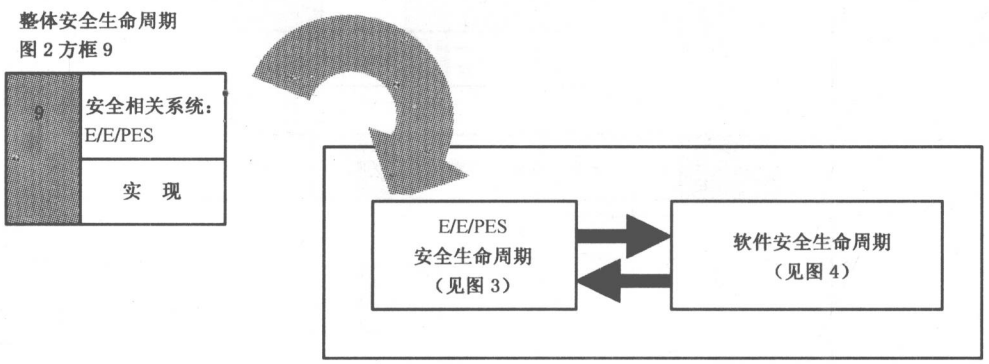


图 5　E/E/PES 整体安全生命周期和软件安全生命周期之间的关系

7.1.2.2　对于整体安全生命周期的所有阶段，表 1 指出：

——要达到的目的；

——各阶段的范围；

——要求所在条款；

——各阶段所要求的输入；

——符合要求的输出。

表 1　整体安全生命周期:概述

安全生命周期阶段		目　　的	范　　围	要求所在的条款	输　　入	输　　出
图 2 的方框号	标　题					
1	概念	7.2.1: 提高对 EUC 及其环境(实际的、法律的等)的理解水平,以满足执行其他安全生命周期活动的需要	EUC 及其环境(实际的、法律的等)	7.2.2	满足该条要求所必需的所有有关信息	从 7.2.2.1～7.2.2.6 获取的信息
2	整体范围定义	7.3.1: 确定 EUC 和 EUC 控制系统的边界; 规定危险和风险分析的范围(如过程危险、环境危险等)	EUC 及其环境	7.3.2	从 7.2.2.1～7.2.2.6 获取的信息	从 7.3.2.1～7.3.2.5 获取的信息
3	危险和风险分析	7.4.1: 对包括故障状况和误用在内的所有合理的可预见的情况,确定 EUC 和 EUC 控制系统的危险和危险事件(所有操作模式下); 确定导致既定危险事件的事件顺序; 确定伴随已确定危险事件的 EUC 风险	范围与达到的整体的、E/E/PES 的和软件的安全生命周期阶段有关(因为可能需要进行几次危险和风险分析);初步危险和风险分析的范围包括 EUC、EUC 控制系统和人的因素	7.4.2	从 7.3.2.1～7.3.2.5 获取的信息	危险和风险描述以及与危险和风险有关的信息
4	整体安全要求	7.5.1: 为达到要求的功能安全,根据安全功能要求和安全完整性要求为 E/E/PE 安全相关系统,其他技术安全相关系统和外部风险降低设施编制整体安全要求规范	EUC、EUC 控制系统和人的因素	7.5.2	危险和风险分析的描述及与危险和风险有关的信息	根据安全功能要求和安全完整性要求规定的整体安全要求规范
5	安全要求分配	7.6.1: 为指定的 E/E/PE 安全相关系统,其他技术安全相关系统和外部风险降低设施分配安全功能,这些安全功能包含于整体安全要求(安全功能要求和安全完整性要求)规范之中; 给每个安全功能分配安全完整性等级	EUC、EUC 控制系统和人的因素	7.6.2	根据安全功能要求和安全完整性要求规定的整体安全要求规范	安全要求分配的信息和结果

表 1（续）

安全生命周期阶段		目　　的	范　　围	要求所在的条款	输　　入	输　　出
图 2 的方框号	标　题					
6	整体操作和维护计划编制	7.7.1： 拟定 E/E/PE 安全相关系统的操作和维护计划，以确保在操作和维护过程中保持所要求的功能安全	EUC、EUC 控制系统和人的因素； E/E/PE 安全相关系统	7.7.2	根据安全功能要求和安全完整性要求确定的整体安全要求规范	E/E/PE 安全相关系统操作和维护计划
7	整体安全确认计划编制	7.8.1： 拟定对 E/E/PE 安全相关系统的整体安全进行确认的计划	EUC、EUC 控制系统和人的因素； E/E/PE 安全相关系统	7.8.2	根据安全功能要求和安全完整性要求确定的整体安全要求规范	E/E/PE 安全相关系统的确认计划
8	整体安装和试运行计划编制	7.9.1： 拟定受控方式下的 E/E/PE 安全相关系统的安装计划，以保证达到要求的功能安全；拟定受控方式下的 E/E/PE 安全相关系统的试运行计划，以保证达到要求的功能安全	EUC 和 EUC 控制系统； E/E/PE 安全相关系统	7.9.2	根据安全功能要求和安全完整性要求确定的整体安全要求规范	E/E/PE 安全相关系统安装计划； E/E/PE 安全相关系统试运行计划
9	E/E/PE 安全相关系统：实现	7.10.1 和 GB/T 20438.2、GB/T 20438.3： 建立符合 E/E/PE 安全要求规范（包括 E/E/PE 安全功能要求规范和 E/E/PE 安全完整性要求规范）的 E/E/PE 安全相关系统	E/E/PE 安全相关系统	7.10.2 GB/T 20438.2 和 GB/T 20438.3	E/E/PES 安全要求规范	每个 E/E/PE 安全相关系统满足 E/E/PES 安全要求规范的证实
10	其他技术安全相关系统：实现	7.11.1： 建立其他技术安全相关系统，以满足为该系统规定的安全功能要求和安全完整性要求（此内容不在 GB/T 20438 范围之内）	其他技术安全相关系统	7.11.2	其他技术安全要求规范（不在 GB/T 20438 范围之内，并且以后 GB/T 20438 也不涉及此内容）	每个其他技术安全相关系统满足该系统的安全要求的证实

表 1（续）

安全生命周期阶段		目　　的	范　　围	要求所在的条款	输　　入	输　　出
图 2 的方框号	标　题					
11	外部风险降低设施：实现	7.12.1： 建立外部风险降低设施，以满足该设施的安全功能要求和安全完整性要求（此内容不在 GB/T 20438 的范围之内）	外部风险降低设施	7.12.2	外部风险降低设施安全要求规范（不在 GB/T 20438 范围之内，并且今后 GB/T 20438 也不会涉及此内容）	每个外部风险降低设施满足该设施的安全要求的证实
12	整体安装和试运行	7.13.1： 安装 E/E/PE 安全相关系统； 试运行 E/E/PE 安全相关系统	EUC 和 EUC 控制系统； E/E/PE 安全相关系统	7.13.2	安装 E/E/PE 安全相关系统的计划； 试运行 E/E/PE 安全相关系统的计划	已安装就绪的 E/E/PE 安全相关系统； 经充分试运行过的 E/E/PE 安全相关系统
13	整体安全确认	7.14.1： 确认 E/E/PE 安全相关系统满足整体安全要求规范，该规范基于整体安全功能要求和整体安全完整性要求，同时考虑了按 7.6 拟定的 E/E/PE 安全相关系统的安全要求分配	EUC 和 EUC 控制系统； E/E/PE 安全相关系统	7.14.2	E/E/PE 安全相关系统的整体安全确认计划； 基于安全功能要求和安全完整性要求的整体安全要求规范； 安全要求分配	所有 E/E/PE 安全相关系统满足基于安全功能要求和安全完整性要求，同时考虑了按 7.6 拟定的 E/E/PE 安全相关系统的安全要求分配的整体安全要求规范的证实
14	整体操作维护和修理	7.15.1： 为保持要求的功能安全，操作、维护和修理 E/E/PE 安全相关系统	EUC 和 EUC 控制系统；E/E/PE 安全相关系统	7.15.2	E/E/PE 安全相关系统的整体操作和维护计划	可持续满足 E/E/PE 安全相关系统所需的功能； 按时间排序的 E/E/PE 安全相关系统的操作、修理和维护文档