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

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。

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。

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。

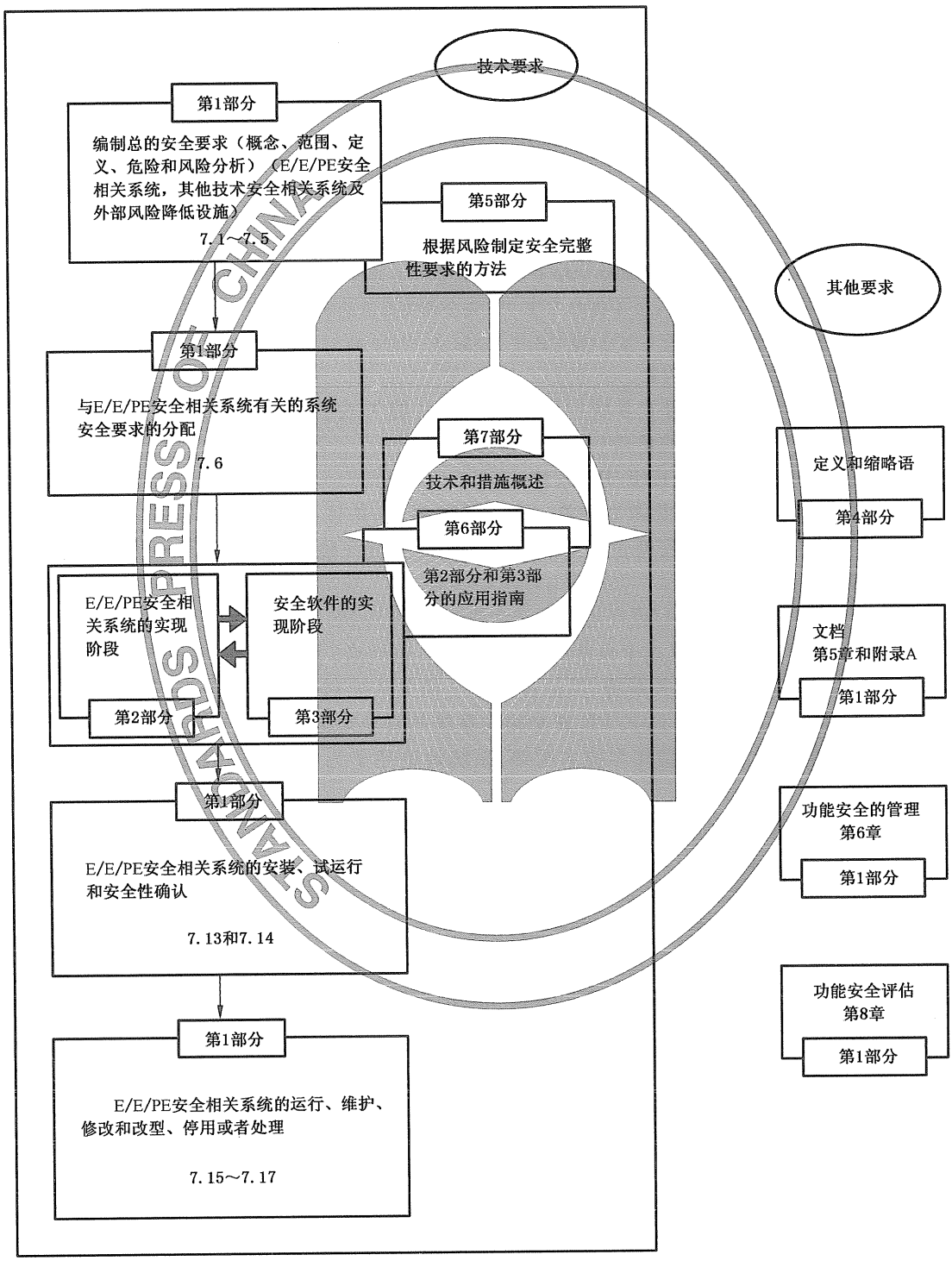


图 1 GB/T 20438 的总体框架

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。

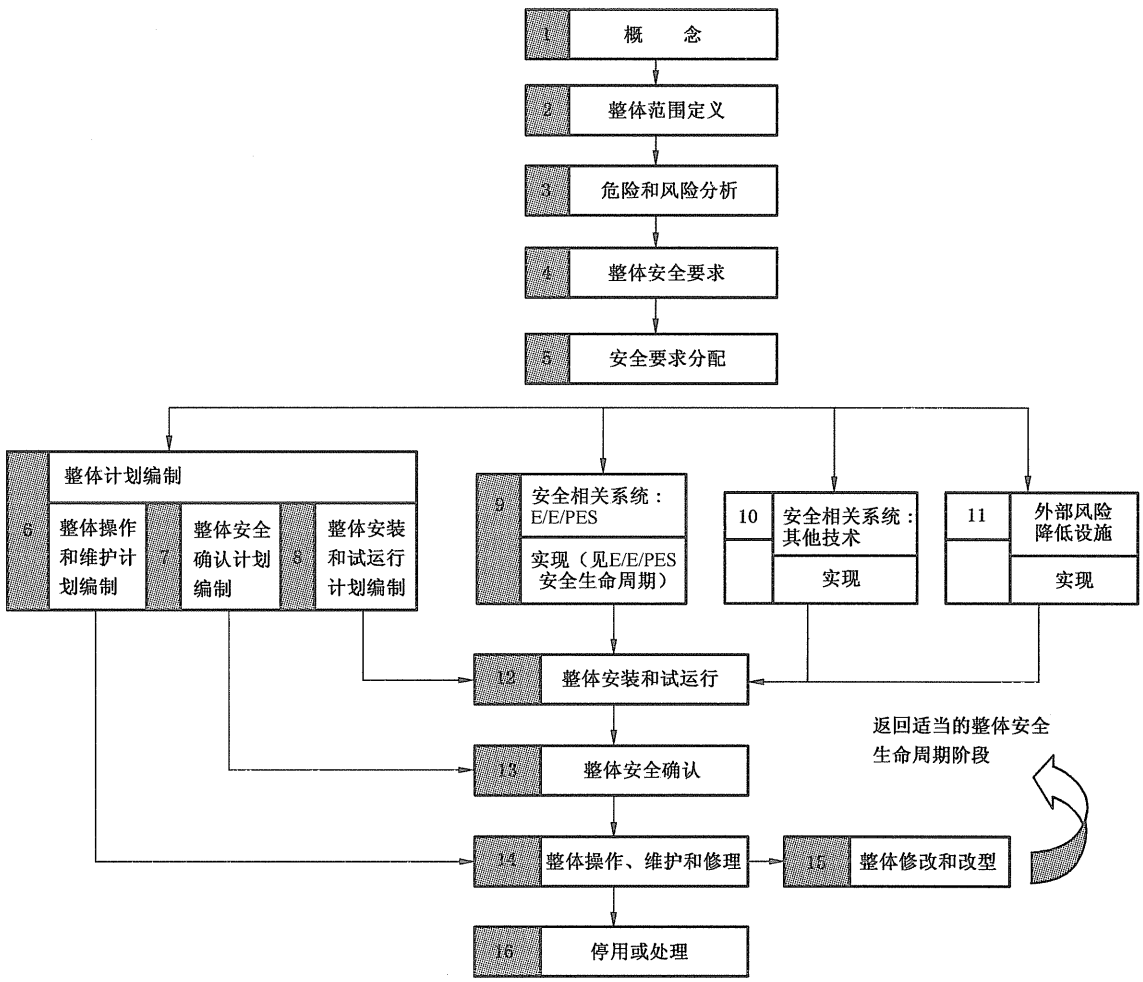
7 整体安全生命周期的要求

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。

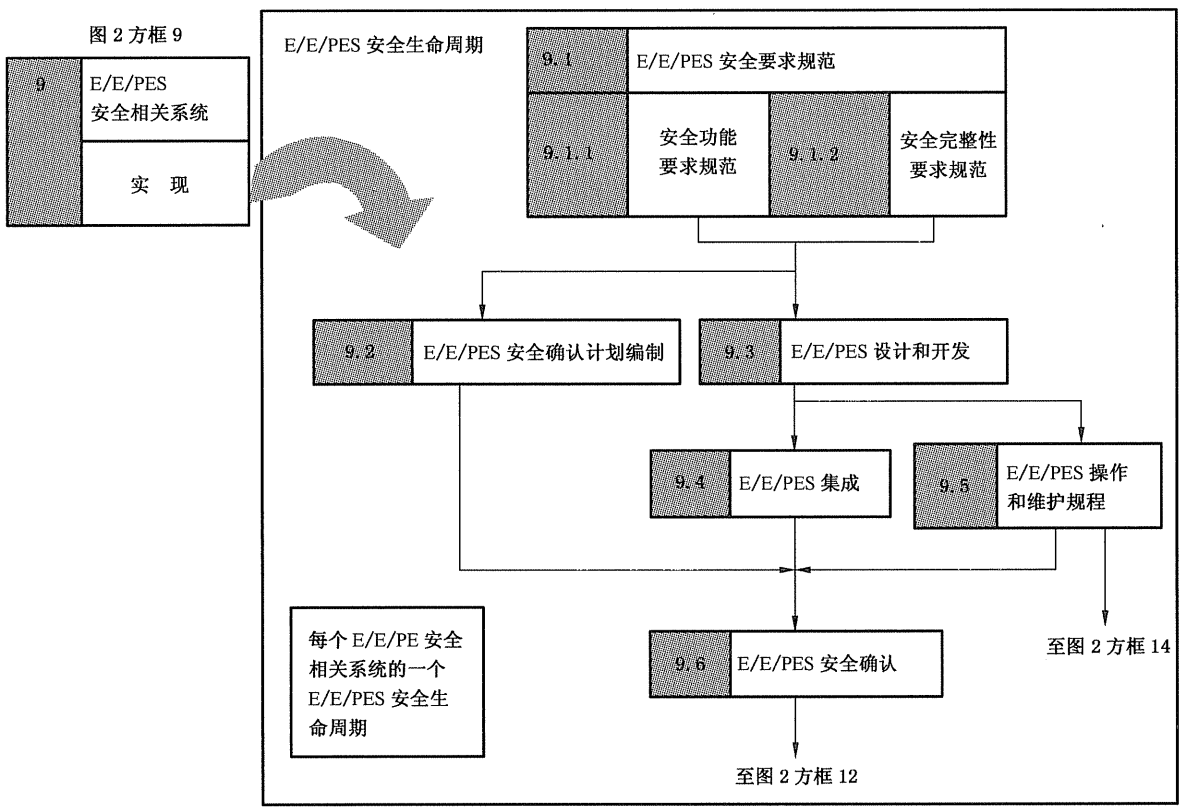


图 3 E/E/PES 安全生命周期(实现阶段)

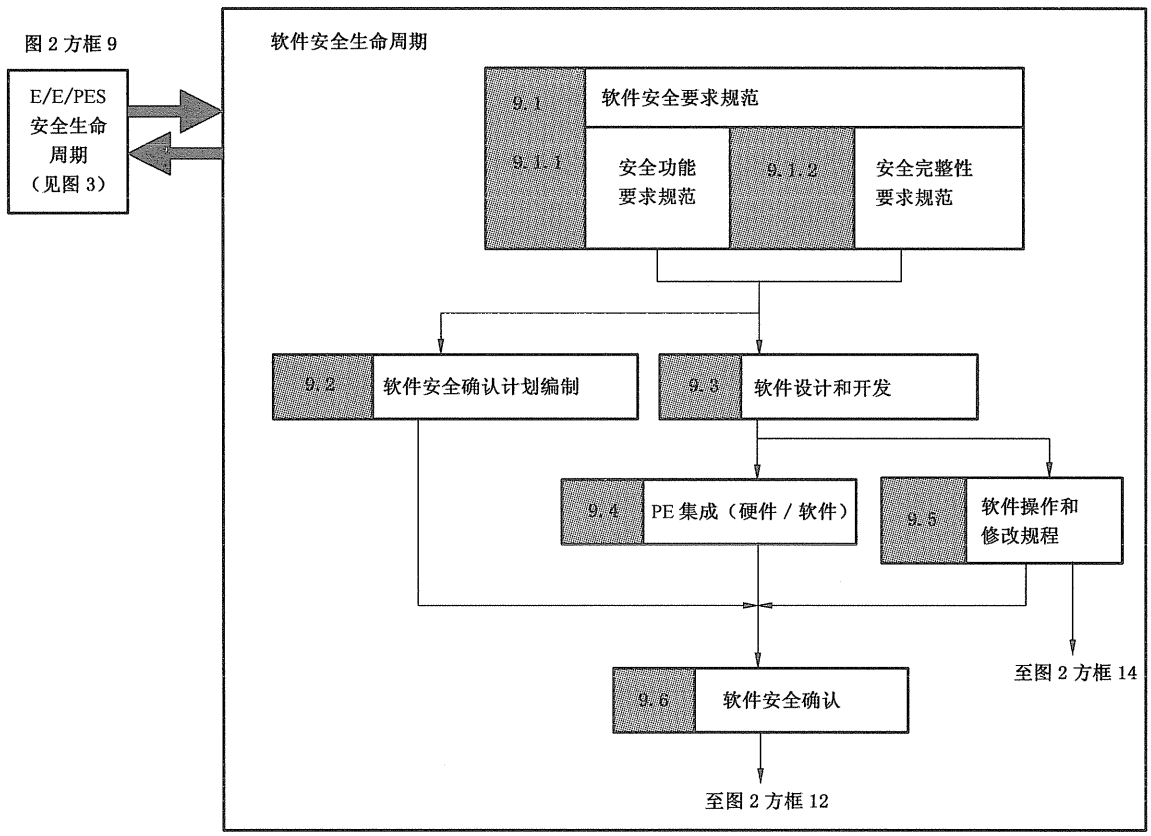


图 4　软件安全生命周期（实现阶段）

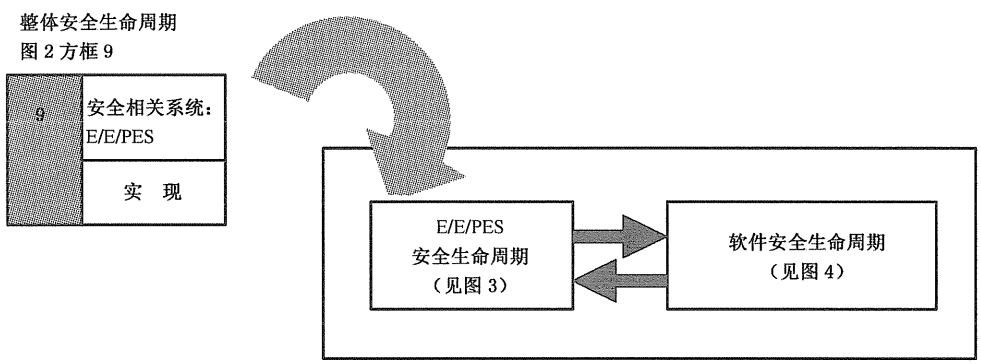


图 5　E/E/PES 整体安全生命周期和软件安全生命周期之间的关系

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

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					
15	整体修改和改型	7.16.1： 在修改和改型阶段中及阶段后保证 E/E/PE 安全相关系统具有合适的功能安全	EUC 和 EUC 控制系统； E/E/PE 安全相关系统	7.16.2	根据功能安全管理规程对修改或改型的请求	在修改和改型阶段中及阶段后，均可达到 E/E/PE 安全相关系统要求的功能安全； 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
16	停用和处理	7.17.1： 在 EUC 的停用及处理活动中及活动后，保证 E/E/PE 安全相关系统的功能安全适应这种情况	EUC 和 EUC 控制系统； E/E/PE 安全相关系统	7.17.2	根据功能安全管理规程对停用或处理的请求	在停用或处理活动中及活动后，均可达到 E/E/PE 安全相关系统要求的功能安全； 按时间排序的停用或处理活动的文档

7.1.3　目的

7.1.3.1　用一种系统的方式构造整体安全生命周期中的各阶段，以达到 E/E/PE 安全相关系统要求的功能安全。

7.1.3.2　将贯穿于整体安全生命周期的 E/E/PE 安全相关系统功能安全的关键信息文档化。

注：文档结构见第 5 章和附录 A。文档的结构可考虑公司的规程和特定应用领域的实际工作情况。

7.1.4　要求

7.1.4.1　图 2 规定了整体安全生命周期，该整体安全生命周期将作为基础用于声明对 GB/T 20438 的符合性。如使用其他的整体安全生命周期，应在功能安全计划编制过程中规定，并应满足 GB/T 20438 的目的和要求。

注：E/E/PES 安全生命周期和软件安全生命周期（它们构成了整体安全生命周期的实现阶段），分别由 GB/T 20438.2和 GB/T 20438.3 规定。其用于声明对 GB/T 20438 的符合性。

7.1.4.2　功能安全管理的要求（见第 6 章）应与整体安全生命周期各阶段并行。

7.1.4.3　除非已做调整，整体安全生命周期的各个阶段都应实施并满足要求。

7.1.4.4　整体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，分成一些基本的活动。

7.1.4.5　每个整体安全生命周期阶段的范围和输入见表 1。

7.1.4.6　除非在功能安全计划编制中已做调整或在应用领域标准中另有规定，由整体安全生命周期的各阶段产生的输出，应如表 1 规定。

7.1.4.7 由整体安全生命周期的各阶段产生的输出，应满足各阶段规定的目的和要求(见 7.2～7.17)。

7.1.4.8 应满足每个整体安全生命周期阶段的验证要求，见 7.18。

7.2 概念

注：这个阶段是图 2 的方框 1。

7.2.1 目的

提高对 EUC 及其环境(实际的、法律的等)的理解水平，使之足以能顺利进行安全生命周期的其他活动。

7.2.2 要求

7.2.2.1 对 EUC 及其要求的控制功能和实际环境进行全面的了解。

7.2.2.2 确定可能的危险源。

7.2.2.3 获取确定危险的有关信息(毒性、爆炸条件、腐蚀性、反应性、易燃性等)。

7.2.2.4 获取当前的安全法规(国际的和国家的)。

7.2.2.5 应考虑相邻近的 EUC(已安装的或将被安装的)之间相互作用所产生的危险。

7.2.2.6 7.2.2.1～7.2.2.5 所要求的信息和结果应文档化。

7.3 整体范围定义

注：这个阶段是图 2 的方框 2。

7.3.1 目的

7.3.1.1 确定 EUC 和 EUC 控制系统的边界。

7.3.1.2 规定危险和风险分析的范围(如过程危险、环境危险等)。

7.3.2 要求

7.3.2.1 应确定危险及风险分析范围内所有的物理设备，包括 EUC 和 EUC 控制系统。

注：见参考文献[1]和[2]。

7.3.2.2 应确定危险及风险分析时要考虑的外部事件。

7.3.2.3 应确定与危险有关的子系统。

7.3.2.4 应确定需要考虑的事故引发事件(如零部件失效、程序故障、人为错误，以及与之有关的可能引起随后一系列意外事故发生的失效机制)的类型。

7.3.2.5 7.3.2.1～7.3.2.4 所要求的信息和结果应文档化。

7.4 危险和风险分析

注：这个阶段是图 2 的方框 3。

7.4.1 目的

7.4.1.1 对于所有可合理预见的情况，包括故障状况和误用，确定 EUC 和 EUC 控制系统的危险和危险事件(在所有操作模式下)。

7.4.1.2 确定导致 7.4.1.1 所确定的危险事件的事件顺序。

7.4.1.3 确定与 7.4.1.1 确定的危险事件相伴的 EUC 风险。

注 1：为使 E/E/PE 安全相关系统的安全要求建立在系统的基于风险方法的基础之上，本条是必需的。这些要在考虑了 EUC 和 EUC 控制系统的前提下才能完成。

注 2：在可对风险、可能的危险、危险事件及其后果进行有效假设的应用领域中，本条(和 7.5)中所需的分析可由 GB/T 20438 应用领域版本的编制者进行，并可把这些分析嵌入到简化的图解要求之中。这种方法的例子见 GB/T 20438.5—2006 的附录 D 和附录 E。

7.4.2 要求

7.4.2.1 进行危险和风险分析时应考虑整体范围定义阶段中的信息(见 7.3)。如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的后期做出的决定，则可能会改变前期所做决定的基础，因此应进行进一步的危险和风险分析。

注1：指南见参考文献[1]和[2]。

注2：可能有必要进行多次危险和风险分析。

注3：把对带安全阀的EUC进行分析作为一个需要深入到整体安全生命周期中进行连续危险和风险分析的例子。一个危险和风险分析可能确定两个导致危险事件的事件顺序，包括阀门开启失效和关闭失效。但是，当分析控制阀门的EUC控制系统的详细设计时，可能发现一个新的失效模式，即阀门振荡，它将引入导致一个危险事件的新事件顺序。

7.4.2.2 应该考虑如何排除危险。

注：尽管不包括在GB/T 20438范围内，但在源头排除EUC已确定的危险是非常重要的，如应用固有安全原理，以及应用优质工程的实践经验。

7.4.2.3 根据合理可预见的情况确定EUC和EUC控制系统的危险和危险事件(包括故障条件和合理可预见的误用)。还包括所有相关的人员因素引起的问题，尤其应注意那些不常见的、异常的EUC操作模式。

注：对于合理可预见的误用，见GB/T 20438.4—2006的3.1.11。

7.4.2.4 应确定7.4.2.3已确定的导致危险事件的事件顺序。

注：一般应考虑用修改过程设计或所用设备的方法排除事件顺序。

7.4.2.5 应对7.4.2.3规定条件下的危险事件的可能性进行评价。

注：一个特定事件的可能性可以定量或定性地表述(见GB/T 20438.3)。

7.4.2.6 应确定7.4.2.3中规定的危险事件所伴随的潜在后果。

7.4.2.7 对每个确定的危险事件应评价或估计EUC风险。

7.4.2.8 可用定性或定量的危险和风险分析技术满足7.4.2.1～7.4.2.7的要求(见GB/T 20438.5)。

7.4.2.9 技术的选用及其使用范围取决于很多因素，包括：

——特定的危险及后果；

——应用领域及其被认可的成功经验；

——法律和安全法规要求；

——EUC风险；

——作为危险和风险分析依据的准确数据的可用性。

7.4.2.10 危险和风险分析应考虑：

——每个确定危险事件和对其起作用的组成成分；

——伴随每个危险事件的事件顺序的后果和可能性；

——每个危险事件的必要风险降低；

——降低和消除危险和风险的措施；

——风险分析中的假设，包括估计的要求率和设备失效率(应详细说明操作约束或人为介入的可信度)；

——安全相关系统在E/E/PES安全生命周期各阶段(如验证和确认活动)引用的关键信息(见第5章和附录A)。

7.4.2.11 构成危险和风险分析的信息和结果应文档化。

7.4.2.12 对EUC和EUC控制系统而言，从危险和风险分析阶段至停用或处理阶段的整个整体安全生命周期全过程中，都应保存构成危险和风险分析的信息和结果。

注：保存危险和风险分析阶段的信息和结果是建立改进危险和风险分析问题解决方案的基本方法。

7.5 整体安全要求

注：这一阶段是图2的方框4。

7.5.1 目的

为达到所要求的功能安全，根据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

设施的安全功能要求和安全完整性要求，编制整体安全要求规范。

注：在应用领域中，可在对风险、可能的危险、危险事件及其后果进行有效假设的情况下，由 GB/T 20438 应用领域版本的编制者进行 7.5(和 7.4)中所需的分析，并可把这些分析嵌入简化的图解要求之中，这种方法的例子见 GB/T 20438.5—2006 的附录 D 和附录 E。

7.5.2 **要求**

7.5.2.1 应规定安全功能，以保证针对每个确定的危险所要求的功能安全。这些安全功能构成了整体安全功能要求的规范。

注：由于在这一阶段，尚不知道实现安全功能的技术和方法，因此在此阶段不规定要执行的安全功能的技术条款。在安全要求分配过程中(见 7.6)，安全功能的描述可能需要修改，以反映专用的实现方法。

7.5.2.2 对每个确定的危险事件应确定必要的风险降低。必要的风险降低可定性和/或定量地确定。

注：为确定对 E/E/PE 安全相关系统、其他技术安全相关系统以及外部风险降低设施的安全完整性要求，需要必要的风险降低。GB/T 20438.5—2006 附录 C 中给出了一个方法。用这种方法，当采用定量法时可确定必要的风险降低。GB/T 20438.5—2006 的附录 D 和附录 E 给出了定性的方法。虽然引用的例子中隐含必要的风险降低，但不是明显地说明。

7.5.2.3 在存在含有直接确定必要的风险降低合适方法的应用领域的国家标准的情况下，可用这个标准来满足本条的要求。

7.5.2.4 在 EUC 控制系统的失效对一个或多个 E/E/PE 或其他技术安全相关系统和/或外部风险降低设施提出要求，以及不想把 EUC 控制系统指定为一个安全相关系统时，应使用下列要求：

a) 对 EUC 控制系统声明的危险失效率应得到通过下列渠道获得的数据的支持：

——在相似应用领域中，EUC 控制系统的实际操作经验；

——对认可的规程进行可靠性分析；

——同类设备的可靠性的工业数据库。

b) EUC 控制系统声明的危险失效率应不低于 10^{-5}/h 危险失效；

注 1：理论上，这个要求是说，如果不把 EUC 控制系统指定为安全相关系统，则对 EUC 控制系统声明失效率应不低于安全完整性等级 1 的较高的目标失效量(10^{-5}/h 危险失效，见表 3)。

c) 在拟定整体安全要求规范时，应确定并考虑所有合理的、可预见的 EUC 控制系统的危险失效模式；

d) EUC 控制系统应是独立的，不依赖于 E/E/PE 安全相关系统、其他技术安全相关系统以及外部风险降低设施。

注 2：如果把安全相关系统已设计成可提供适当的安全完整性，并考虑了 EUC 控制系统的额定要求率，则不必将 EUC 控制系统指定为安全相关系统(并且它的功能不能选定为 GB/T 20438 中的安全功能)。在某些应用中，特别是在需要很高的安全完整性时，通过设计具有比额定失效率低的 EUC 控制系统，降低要求率是合适的，在这种情况下，如失效率小于安全完整性等级 1(见表 3)的目标安全完整性上限时，控制系统将变得与安全有关，并且将使用 GB/T 20438 中的要求。

7.5.2.5 如果不能满足 7.5.2.4a)～d)中包含的要求，则应将 EUC 控制系统指定成一个安全相关系统。分配给 EUC 控制系统的安全完整性等级，应基于 EUC 控制系统所声明的失效率，它与表 2 和表 3 中规定的目标失效量相符。在这种情况下，GB/T 20438 中与分配的安全完整性等级有关的要求应用于 EUC 控制系统。

注 1：例如，如声明 EUC 控制系统的失效率在 10^{-6}/h 失效～10^{-5}/h 失效之间，则应满足安全完整性等级 1 的相关要求。

注 2：另见 7.6.2.10。

7.5.2.6 基于必要的风险降低，应对每个安全功能规定安全完整性要求，这就构成对整体安全完整性要求的规范。

注：安全完整性要求的规范是确定 E/E/PE 安全相关系统要实现的安全功能的安全完整性等级的一个过渡阶段。某些确定安全完整性等级的定性方法(见 GB/T 20438.5—2006 附录 D 和附录 E)，是从风险参数直接进展到安全完整性等级的。在这种情况下，必要的风险降低是隐含的而不是明显的，因为它本身就包含在方法之中。

7.5.2.7 安全功能(见 7.5.2.1)和安全完整性要求(见 7.5.2.6)的规范一起构成整体安全要求的规范。

7.6 安全要求分配

注：这个阶段是图 2 的方框 5。

7.6.1 目的

7.6.1.1 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。

注：如不考虑其他风险降低的量值，则对 E/E/PE 安全相关系统的分配就无法进行，因此要考虑其他技术安全相关系统和外部风险降低设施。

7.6.1.2 对每个安全功能分配安全完整性等级。

注：基于风险降低规定 7.5 中的安全完整性要求。

7.6.2 要求

7.6.2.1 应规定用于达到功能安全要求所指定的安全相关系统，用下列系统达到必要的风险降低：

——外部风险降低设施；

——E/E/PE 安全相关系统；

——其他技术安全相关系统。

注：本条仅适用于安全相关系统中有 E/E/PES 的情况。

7.6.2.2 在给 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时，应考虑在整体安全生命周期的所有阶段中可能利用的技能和资源。

注 1：通常会低估使用复杂技术的安全相关系统的全部内涵。如实现复杂技术时，从规范到维护和操作的所有阶段都要求高等级的能力。而用其他简单技术的解决方案可能有同等效果，且由于降低了复杂性而带来一些好处。

注 2：可用的操作、维护技能和资源以及操作环境对在实际操作中达到所要求的功能安全是关键性的。

7.6.2.3 把按 7.5 建立的每个安全功能及其相应的安全完整性要求，分配给指定的 E/E/PE 安全相关系统，并考虑其他技术安全相关系统和外部风险降低设施所产生的风险降低，以达到安全功能必要的风险降低。这种分配要重复进行，如果发现不能达到必要的风险降低则应修改体系结构并进行重新分配。

注 1：根据必要的风险降低(见 7.5)规定的每个安全功能及其相应的安全完整性要求应分配给一个或多个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。决定把一个特定功能分配给一个还是几个安全相关系统取决于许多因素，但主要取决于安全功能达到风险的降低。要求的风险降低越大，该功能就越可能分配给更多的安全相关系统。

注 2：对于安全要求分配，图 6 给出了本条采用的途径。

7.6.2.4 7.6.2.3 所述的分配应这样进行，即分配所有的安全功能并且满足每个安全功能的安全完整性要求(根据 7.6.2.10 中规定的基本要求)。

7.6.2.5 对每个安全功能的安全完整性要求应可以指出是否达到每个目标安全完整性参数：

——能在要求时就执行其设计功能的平均失效概率(低要求操作模式时)；或

——每小时危险失效概率(高要求或连续操作模式时)。

7.6.2.6 对于概率的组合可使用适当的技术来执行安全完整性要求的分配。

注：可用定量和/或定性的方法进行安全要求分配。

7.6.2.7 进行分配时应考虑共同原因失效的概率。如果 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对于分配而言被看作是独立的，则它们：

——实现功能的途径是多种多样的(即用完全不同的途径达到相同的结果)；

——是以多种技术为基础的(如用不同类型的设备达到相同的结果)；

注 1：要认识到，尽管有多种途径和技术，对失效事件发生时可产生特别严重后果的高安全完整性系统而言，要采取特殊预防措施以抵御低概率的共同原因事件，例如飞机失事和地震。

——不能用因其失效将引起所有系统产生危险模式失效的公用部件、服务或支持系统(如电源)；

——不能使用公用的操作、维护或测试规程；

——应在物理上分开，这样可预见的失效不会影响冗余安全相关系统和外部风险降低设施。

注 2：GB/T 20438 涉及对 E/E/PE 安全相关系统的安全完整性要求的分配并规定了如何进行这种分配的要求。GB/T 20438 没有细致考虑对于其他技术安全相关系统和外部风险降低设施的安全完整性要求的分配。

7.6.2.8 如果不能满足 7.6.2.7 的所有要求，除非进行一次分析并显示出这些系统是充分独立的(从安全完整性的角度看)，否则对于安全完整性分配来说，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都不能视为独立系统。

注 1：相关失效分析的更多信息参见参考文献[9]和[10]。

注 2：充分独立性是指与 E/E/PE 安全相关系统整体安全完整性要求相比，相关失效的概率足够低。

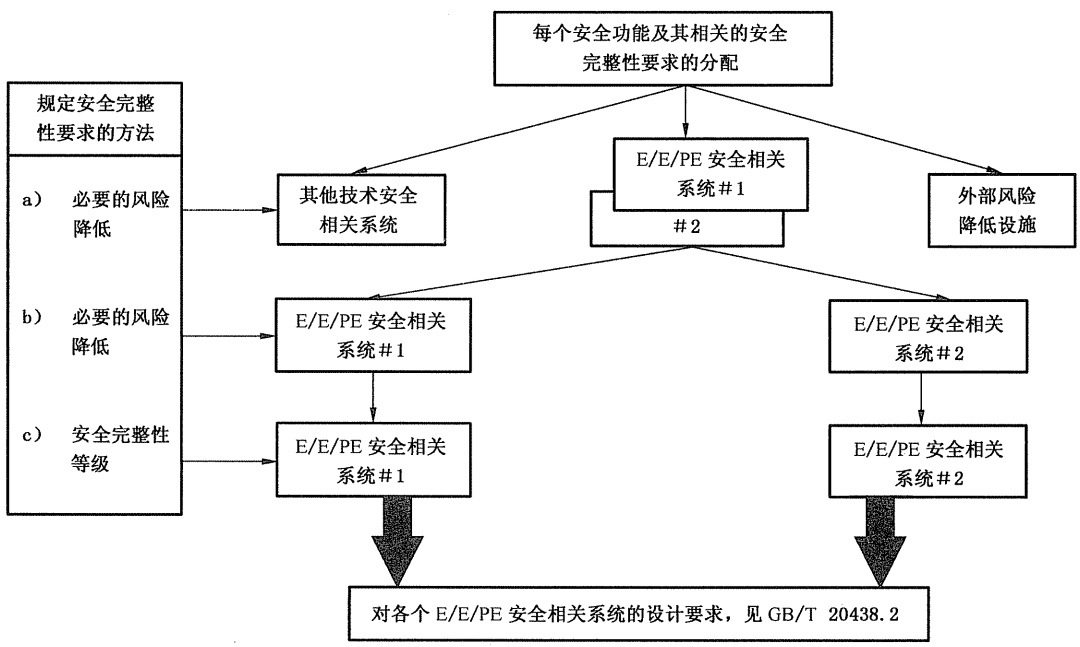
7.6.2.9 当分配已充分进行后，分配给 E/E/PE 安全相关系统每个安全功能的安全完整性要求，应按表 2 和表 3 中的安全完整性等级进行规定，并且加以考核以指出目标安全完整性参数是下列两者之一：

——在要求时就执行其设计功能的平均失效概率(低要求操作模式时)；或

——每小时危险失效概率(高要求或连续操作模式时)。

注 1：先于这一阶段，就应根据风险降低规定安全完整性要求(见 7.5)。

注 2：表 2 和表 3 包含了安全完整性等级的目标失效量。大家公认不可能定量地预计 E/E/PE 安全相关系统的所有方面的安全完整性。就满足目标失效量必需的预防措施而言，不得不使用定性的技术、措施、判断。对于系统安全完整性的情况而言尤为如此(见 GB/T 20438.4—2006 的 3.5.4)。



注 1：在分配前，安全完整性要求与每个安全功能是相关的。

注 2：一个安全功能可以分配给不止一个安全相关系统。

图 6 对 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的安全要求的分配

表 2　安全完整性等级:在低要求操作模式下分配给一个 E/E/PE 安全相关系统的安全功能目标失效量

安全完整性等级	低要求操作模式(在要求时就执行其设计功能要求的平均失效概率)
4	$\geqslant 10^{-5}$ 且 $< 10^{-4}$
3	$\geqslant 10^{-4}$ 且 $< 10^{-3}$
2	$\geqslant 10^{-3}$ 且 $< 10^{-2}$
1	$\geqslant 10^{-2}$ 且 $< 10^{-1}$
注:详细解释见下面的注 3～注 9。	

表 3　安全完整性等级:在高要求或连续操作模式下分配给一个 E/E/PE 安全相关系统的安全功能目标失效量

安全完整性等级	高要求或连续操作模式(每小时危险失效概率)
4	$\geqslant 10^{-9}$ 且 $< 10^{-8}$
3	$\geqslant 10^{-8}$ 且 $< 10^{-7}$
2	$\geqslant 10^{-7}$ 且 $< 10^{-6}$
1	$\geqslant 10^{-6}$ 且 $< 10^{-5}$
注:详细解释见下面的注 3～注 9。	

注 3:对低要求操作模式和高要求或连续操作模式的术语定义见 GB/T 20438.4—2006 的 3.5.12。

注 4:针对高要求或连续操作模式的表 3 中的参数,即每小时危险失效概率有时是指危险失效的频率或危险失效率,以每小时危险失效次数为单位。

注 5:在规定的任务时间内不能发生修理的、按高要求或连续操作模式运行的 E/E/PE 安全相关系统,其某个安全功能要求的安全完整性等级可如下获得:确定在任务时间内要求的安全功能的失效概率,除以任务时间即给出要求的每小时失效概率,然后从表 3 获得要求的安全完整性等级。

注 6:GB/T 20438 在危险失效模式下设置了一个可以声明的目标失效量下限。这些目标失效量是安全完整性等级 4 的下限(即为能在要求时就执行其设计功能的一个 10^{-5} 的平均失效概率,或一个 10^{-9}/h 的危险失效概率),对简单系统而言,有可能设计一个低目标失效量的安全相关系统,但要考虑表中所示的较复杂系统(如可编程电子安全相关系统)目前能达到的限值。

注 7:当使用两个或多个 E/E//PE 安全相关系统时,声明的目标失效量可能优于表 2 和表 3 给出的那些值,其条件是要达到满足要求的独立水平。

注 8:要注意安全完整性等级 1、2、3、4 的失效量是目标失效量。普遍承认在评估目标失效量是否被满足的时候,只有对于硬件安全完整性才可定量化和应用可靠性预测技术(见 GB/T 20438.4—2006 的 3.5.5)。就满足目标失效量必需的预防措施而言,不得不使用定性的技术、判断。

注 9:每一个安全功能的安全完整性要求都将被考核,从而指出每个目标安全完整性参数是否

——能在要求时就执行其设计功能的平均失效概率;或

——每小时危险失效概率(高要求或连续操作模式时)。

7.6.2.10　对用于实现不同安全完整性等级的安全功能的 E/E/PE 安全相关系统,除非显示出这些安全功能的实现之间是充分独立的,否则在实现独立性存在不足时,硬件和软件的那些部分应作为具有最高安全完整性等级的安全功能来对待。因此适用于最高安全完整性等级的要求适用于所有这些部分。

注:另见 GB/T 20438.2—2006 的 7.4.2.4 和 GB/T 20438.3—2006 的 7.4.2.8。

7.6.2.11　仅当满足下列 a)或同时满足 b)和 c)时,才能允许由一个具有安全完整性等级 4 的单一 E/E/PE安全相关系统构成一个体系结构:

a)　通过结合适当的分析方法和测试,已经用实例清楚地说明了目标安全完整性失效量。

b)　已具有作为 E/E/PE 安全相关系统一部分的部件的广泛操作经验;这些操作经验可在相同的环境中获得,并至少已用于复杂性程度可比拟的一个系统中。

c) 具有足够多的从 E/E/PE 安全相关系统的部件中获得的硬件失效数据，从而对所声明的硬件安全完整性目标失效量的可信度是足够的。这些数据与建议的环境、应用和复杂程度相关。

7.6.2.12 对于工作在下列情况的安全相关系统分配给单一的 E/E/PE 安全相关系统的目标安全完整性失效量不低于表 2 和表 3 规定的值：

——低要求操作模式下，为能在要求时就执行其设计功能，下限设于：平均失效概率为 10^{-5}；

——高要求或连续操作模式，下限设于：危险失效概率为 10^{-9}/h。

7.6.2.13 7.6.2.1～7.6.2.12 中获得的安全要求分配的信息和结果连同所作的任何假设和证明都要文档化。

注：对每个 E/E/PE 安全相关系统，都要有安全功能和安全完整性等级的足够的信息。这些信息将构成 GB/T 20438中编制 E/E/PE 安全相关系统安全要求的基础。

7.7 整体操作和维护计划编制

注 1：这一阶段是图 2 的方框 6。

注 2：图 7 所示为操作和维护活动模型的一个例子。

注 3：图 8 所示为操作和维护管理模型的一个例子。

7.7.1 目的

拟定 E/E/PE 安全相关系统的操作和维护计划，以保证在操作和维护期间保持所要求的功能安全。

7.7.2 要求

7.7.2.1 计划应规定以下内容：

a) 保持 E/E/PE 安全相关系统所要求的功能安全的日常行动。

b) 为防止非安全状态、减少对 E/E/PE 安全相关系统的要求或降低危险事件产生的后果采取的必要行动和约束（如在启动、正常操作、例行测试、可预见的干扰、故障和关机过程中的）。

注 1：下列约束、条件和动作是与 E/E/PE 安全相关系统有关的：

——在 E/E/PE 安全相关系统失效或故障时对 EUC 操作的约束；

——在 E/E/PE 安全相关系统的维护中对 EUC 操作的约束；

——解除 EUC 操作约束的时间；

——恢复到正常操作的规程；

——确认已达到正常操作的规程；

——启动特殊操作或测试时，E/E/PE 安全相关系统功能可能被忽略的状况；

——在忽略 E/E/PE 安全相关系统之前、之后、之中应遵循的规程，包括允许工作规程和管理机构级别。

c) 需保存的显示功能安全审核和测试结果的文档。

d) 需保存的危险事故和具有产生危险事件潜力的所有意外事故的文档。

e) 维护活动（与修改活动有区别）的范围。

f) 危险事件发生时应采取的行动。

g) 按时间顺序编排操作和维修活动文档的内容（见 7.5.1）。

注 2：大多数 E/E/PE 安全相关系统具有一些失效模式，仅在常规维护的测试中才可显现。在这种情况下，如果测试的频率不够，则难以达到 E/E/PE 安全相关系统规定的安全完整性。在线测试时，有必要暂时停用 E/E/PE安全相关系统。仅当暂停使用期间发生一次要求的概率很小时才予考虑。当不能保证概率很小时，有必要安装附加的传感器和执行器，以保持测试期间要求的功能安全。

注 3：本条适用于软件供方，要求软件供方提供软件产品的信息和操作规程，以使用户在操作和维护安全相关系统时能保证要求的安全功能。其中包括作为操作或维护要求的结果所产生的软件修改准备规程（另见 GB/T 20438.3—2006 的 7.6），这些规程的实现包括在 7.15 和 GB/T 20438.3—2006 的 7.8 中。作为修改一个安全相关系统的一条要求的后果而产生的进一步软件更改的准备规程，详见 7.16 和 GB/T 20438.3—2006 的 7.6。这些规程的实现包括在 7.16 和 GB/T 20438.2—2006 中的 7.8 中。

注 4：为满足 GB/T 20438.2 和 GB/T 20438.3 中的要求，要考虑已编制的操作和维护规程。

7.7.2.2 用系统分析的方法确定常规维护活动，该活动用于检测尚未揭露的故障。

注：如果未揭露的故障没有被检测到，则可能：

——在 E/E/PE 安全相关系统、其他技术安全相关系统或外部风险降低设施的情况下，导致在要求时操作失效。

——在非安全相关系统的情况下，导致向 E/E/PE 安全相关系统、其他技术安全相关系统或外部风险降低设施提出多次要求。

7.7.2.3 E/E/PE 安全相关系统维护计划应得到今后负责对 E/E/PE 安全相关系统、其他技术安全相关系统、外部风险降低设施和有可能对安全相关系统发出要求的非安全相关系统进行操作和维护的各方的一致认可。

7.8 整体安全确认计划编制

注：这一阶段是图 2 的方框 7。

7.8.1 目的

拟定一个对 E/E/PE 安全相关系统的整体安全执行确认的计划。

7.8.2 要求

7.8.2.1 拟定计划应包括以下内容：

a) 何时进行确认的细节。

b) 何人负责确认的细节。

c) EUC 操作的相关模式规范及其与 E/E/PE 安全相关系统的关系，包括下列适用的场合：

——使用的准备，包括设置和调整；

——启动；

——教学；

——自动；

——手动；

——半自动；

——操作稳定状态；

——重新启动；

——关机；

——维护；

——合理的可预见的异常状况。

d) 针对开始试运行之前的每种 EUC 操作模式，需要进行确认的 E/E/PE 安全相关系统的规范。

e) 确认技术战略（如分析方法、统计测试等）。

f) 用来确认已正确执行安全功能分配的措施方法、技术和规程，包括每个安全功能是否符合下列规范：

——整体安全功能要求的规范；

——整体安全完整性要求的规范。

g) 包括 7.5 和 7.6 输出中的每个元素的特殊参考；

h) 开展确认活动所要求的环境（如进行测试所需要的调校工具和设备等）；

i) 通过和不通过的准则；

j) 确认结果的评价方针和规程，特别是不通过时的评价方针和规程。

注：在整体确认计划编制中，必须考虑 GB/T 20438.2 和 GB/T 20438.3 要求的对 E/E/PES 安全确认和软件确认计划的工作。保证考虑所有的风险降低量之间的相互作用，并达到所有的安全功能（如 7.5 输出中的规定）是很重要的。

7.8.2.2 7.8.2.1 的信息应文档化，并构成 E/E/PE 安全相关系统整体安全的确认计划。

7.9 整体安装和试运行计划编制

注：这一阶段是图 2 的方框 8。

7.9.1 目的

7.9.1.1 拟定在受控方式下的 E/E/PE 安全相关系统的安装计划，以保证达到功能安全的要求。

7.9.1.2 拟定在受控方式下的 E/E/PE 安全相关系统的试运行计划，以保证达到功能安全的要求。

7.9.2 要求

7.9.2.1 E/E/PE 安全相关系统安装计划应规定

——安装日程表；

——不同安装部分的负责人员；

——安装规程；

——总成各种元素的顺序；

——宣布 E/E/PE 安全相关系统全部或者部分已经安装就绪或宣布安装活动结束的准则；

——失效和不兼容性的解决规程。

7.9.2.2 E/E/PE 安全相关系统的试运行计划应规定：

——试运行日程表；

——试运行不同部分的负责方：

——试运行操作规程；

——与不同安装阶段的关系；

——与确认的关系。

7.9.2.3 整体安装和试运行计划应文档化。

7.10 实现：E/E/PES

注：这一阶段是图 2 的方框 9，图 3 和图 4 的方框 9.1～方框 9.6。

7.10.1 目的

建立符合 E/E/PES 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，见 GB/T 20438.2 和 GB/T 20438.3。

7.10.2 要求

必须满足的要求包括在 GB/T 20438.2 和 GB/T 20438.3 中。

7.11 实现：其他技术

注：这一阶段是图 2 的方框 10。

7.11.1 目的

建立其他技术安全相关系统，以满足为此系统规定的安全功能要求和安全完整性要求。

7.11.2 要求

对于其他技术安全相关系统，为满足其安全功能要求和安全完整性要求的规范，不在 GB/T 20438 范围之内。

注：其他技术安全相关系统是基于电气/电子/可编程电子之外的技术（如液压的、气动的等）。为保证完整，其他技术安全相关系统与外部风险降低设施一起包括在整体安全生命周期中（见 7.12）。

7.12 实现：外部风险降低设施

注：这一阶段是图 2 的方框 11。

7.12.1 目的

建立外部风险降低设施，以满足为该设施规定的安全功能要求和安全完整性要求。

7.12.2 要求

对于外部风险降低设施，为满足安全功能要求和安全完整性要求的规范不在 GB/T 20438 范围之内。

注：为保证完整，外部风险降低设施与其他技术安全相关系统一起包括在整体安全生命周期之中（见 7.11）。

7.13 整体安装和试运行

注：这一阶段是图 2 的方框 12。

7.13.1 目的

7.13.1.1 安装 E/E/PE 安全相关系统。

7.13.1.2 试运行 E/E/PE 安全相关系统。

7.13.2 要求

7.13.2.1 安装活动应按照 E/E/PE 安全相关系统的安装计划执行。

7.13.2.2 安装过程中的信息文档应包括：

——安装活动文档；

——失效和不兼容的解决方案。

7.13.2.3 试运行活动应按照 E/E/PE 安全相关系统的试运行计划执行。

7.13.2.4 试运行过程中的信息文档应包括：

——试运行活动文档；

——涉及的失效报告；

——失效和不兼容的解决方案。

7.14 整体安全确认

注：这一阶段是图 2 的方框 13。

7.14.1 目的

确认 E/E/PE 安全相关系统在考虑了按 7.6 拟定的 E/E/PE 安全相关系统的安全要求分配后，满足基于整体安全功能要求和整体安全完整性要求的整体安全要求规范。

7.14.2 要求

7.14.2.1 确认活动应按 E/E/PE 安全相关系统整体安全确认计划执行。

7.14.2.2 作为确认活动一部分的所有定量测量所用的设备，应按国家标准或供方的规范进行校准。

7.14.2.3 确认过程中的信息文档应包括：

——按时间顺序编制的确认活动文档；

——使用的整体安全要求规范的版本；

——要确认的安全功能(用测试或分析的方法)；

——使用的工具和设备以及校准数据；

——确认活动的结果；

——测试时，项目的配置标识、测试环境和使用的规程；

——期望值和实际结果的差异。

7.14.2.4 如果实际结果与预期有差异，要进行分析并决定是继续进行确认还是发布一个改变请求并返回确认的早期阶段，并将上述内容写入文档。

7.15 整体操作、维护和修理

注 1：这一阶段是图 2 的方框 14。

注 2：本条中涉及的组织措施是为有效实现技术要求创造条件，并以完全达到和保持 E/E/PE 安全相关系统的功能安全为目的。为保持功能安全所必须的技术要求一般规定作为 E/E/PE 安全相关系统供方提供的部分信息。

注 3：在维护和修理活动中的功能安全要求，可能与在操作中的要求不同。

7.15.1 目的

操作、维护和修理 E/E/PE 安全相关系统，从而保持要求的功能安全。

7.15.2 要求

7.15.2.1 应遵从下列要求：

——E/E/PE 安全相关系统维护计划；

——E/E/PE 安全相关系统操作、维护和修理规程(见 GB/T 20438.2)；

——软件的操作和维护规程(见 GB/T 20438.3)。

7.15.2.2 实现 7.15.2.1 中规定的项目应包括启动下列活动：

——规程的实现；

——按维护日程表进行维护；

——文档的维护；

——周期地进行功能安全审核(见 6.2.1k))；

——对 E/E/PE 安全相关系统所作修改的文档化。

注 1：操作和维护活动模型的例子见图 7。

注 2：操作和维护管理模型的例子见图 8。

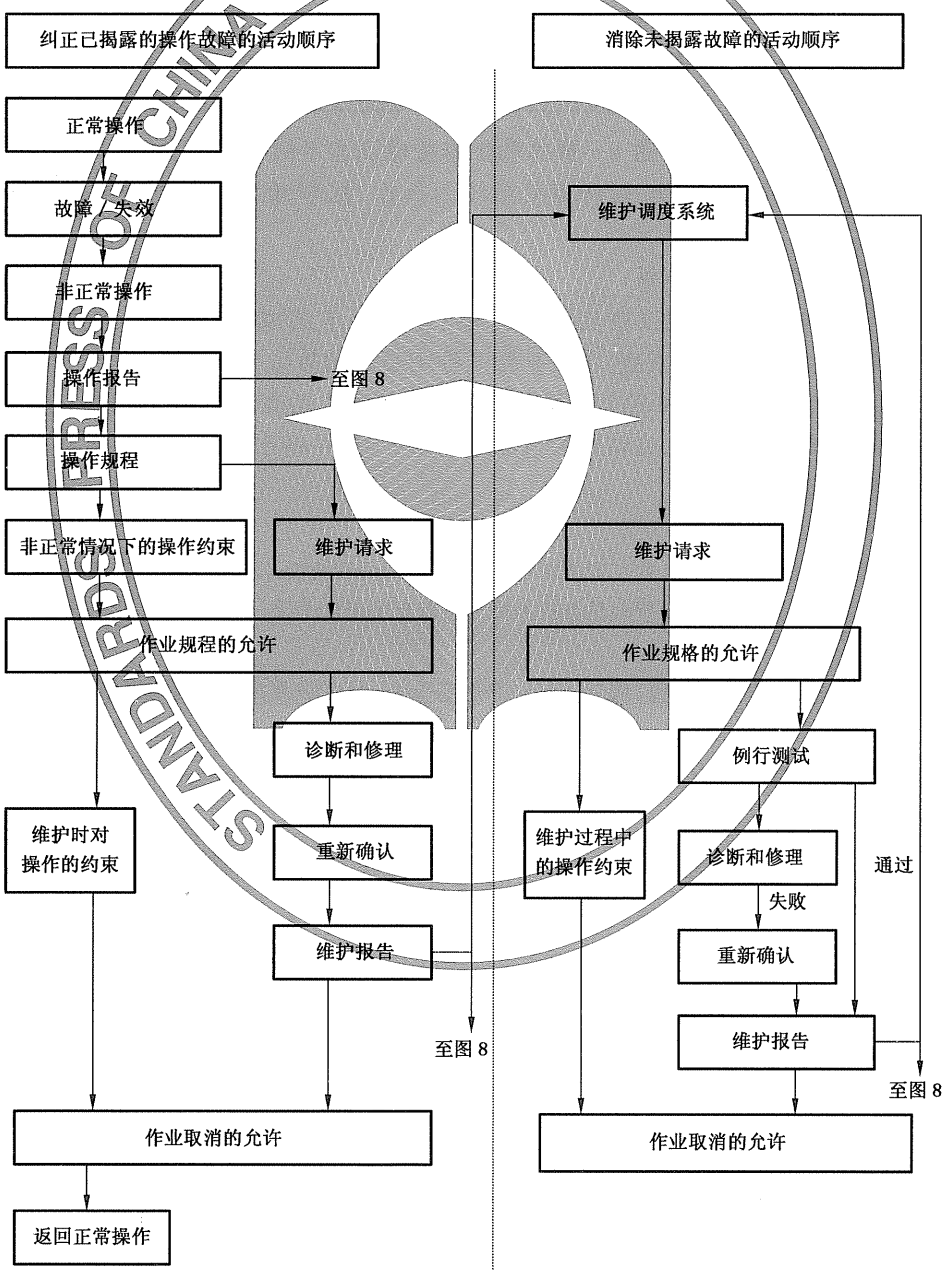


图 7 操作和维护活动模型示例

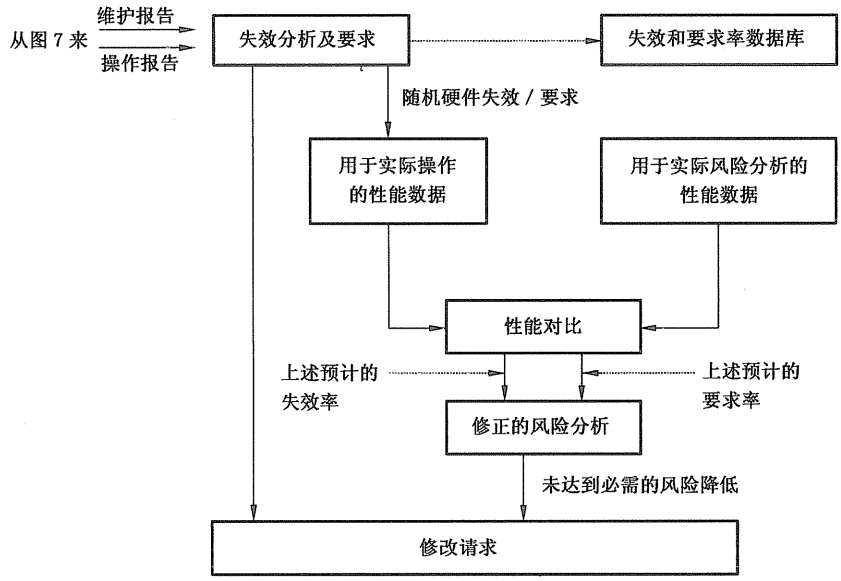


图 8　操作和维修管理模型示例

7.15.2.3　按时间编制的 E/E/PE 安全相关系统的操作、修理和维护文档应妥善保存并包括下列信息：

——功能安全审核和测试的结果；

——向 E/E/PE 安全相关系统（在实际操作中）发出要求的原因和时间，连同收到那些要求时 E/E/PE安全相关系统的表现，以及日常维护中发现的故障等文档；

——对 EUC、EUC 控制系统和 E/E/PE 安全相关系统所作的修改的文档。

7.15.2.4　对按时间编排的文档的确切要求与实际应用有关，并将在应用领域标准中详细说明。

7.16　整体修改和改型

注 1：这一阶段是图 2 的方框 15。

注 2：本条中涉及的组织措施是为有效实现技术要求创造条件，并以完全达到和保持 E/E/PE 安全相关系统的功能安全为目的。为保持功能安全所必须的技术要求一般规定作为 E/E/PE 安全相关系统供方提供的部分信息。

7.16.1　目的

在修改和改型的过程中、过程后，保证 E/E/PE 安全相关系统具有合适的功能安全。

7.16.2　要求

7.16.2.1　在进行修改或改型活动之前，需计划好有关程序（见 6.2.1）。

注：修改程序模型的例子见图 9。

7.16.2.2　只有根据功能安全管理规程（见第 6 章）发布一个经批准的请求，才能启动修改和改型阶段。请求中应包括下列细节：

——可能受影响的已确定的危险；

——建议的更改（硬件和软件）；

——改变的理由。

注：导致修改请求的理由可从下列各项中产生，如：

a）　功能安全低于规定；

b）　系统故障的经验；

c）　新的或已修订的安全法规；

d）　EUC 或其用途的修改；

e）　整体安全要求的修改；

f）　操作和维护性能的分析，分析指示出该性能低于目标值；

g) 例行功能安全审核。

7.16.2.3 应进行影响分析，包括所建议的修改或改型活动对 E/E/PE 安全相关系统影响的评估。评估包括危险和风险分析，此分析足以确定其后整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期各阶段需承担的危险和风险的广度与深度。评估还应考虑同时进行的其他修改或改型活动的影响，以及在修改和改型过程中、过程后的功能安全。

7.16.2.4 7.16.2.3 中所述的结果应文档化。

7.16.2.5 执行所需修改或改型活动的批准有赖于影响分析的结果。

7.16.2.6 对 E/E/PE 安全相关系统功能安全产生影响的所有修改将启动执行活动返回到整体安全生命周期、E/E/PE 安全生命周期或软件安全生命周期的适当阶段，然后所有后续阶段则按照为特定阶段规定的规程执行，该规程应符合 GB/T 20438 的要求。

注 1：有必要进行全面的危险和风险分析，该分析可能产生不同于当前对 E/E/PE 安全相关系统所规定的安全完整性等级的需要。

注 2：在 EUC 在线操作的情况下，不检查它们的有效性和实用性，就不可以使用为初始安装和试运行而制定的测试规程。

7.16.2.7 应建立和保存按时间顺序编排的包括所有修改和改型细节的文档，其内容如下：

——修改或改型请求；

——影响分析；

——数据和结果的重新验证和重新确认；

——受修改和改型活动影响的所有文档。

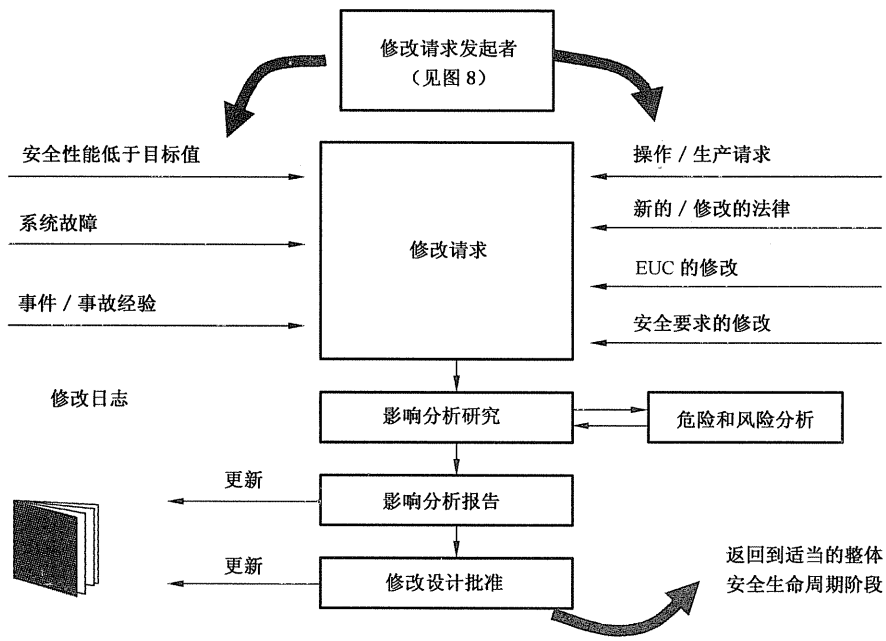


图 9 修改规程模型示例

7.17 停用或处理

注：这一阶段是图 2 的方框 16。

7.17.1 目的

在 EUC 的停用或处理活动中、活动后保证 E/E/PE 安全相关系统的功能安全适应这种情况。

7.17.2 要求

7.17.2.1 在进行停用或处理活动之前应进行影响分析，影响分析包括建议的停用或处理活动对任何 E/E/PE 安全相关系统及其相关的 EUC 的功能安全的影响评估，影响分析还应考虑到相邻的 EUC 以

及对 E/E/PE 安全相关系统的影响。评估包括足以确定其后的整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期各阶段需承担的危险和风险的广度及深度的危险和风险分析。

7.17.2.2 7.17.2.1 所述的结果应文档化。

7.17.2.3 按照功能安全管理规程,仅当发布一个被批准的请求后,才可启动停用和处理阶段(见第 6 章)。

7.17.2.4 执行所需停用或处理的批准有赖于影响分析的结果。

7.17.2.5 在停用或处理之前应制定一个计划,该计划包括下列规程:

——E/E/PE 安全相关系统的关闭;

——E/E/PE 安全相关系统的拆除。

7.17.2.6 如果停用或处理活动会对 E/E/PE 安全相关系统的功能安全产生影响,则将启动执行活动返回到整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期的适当阶段。然后,按照 GB/T 20438中为 E/E/PE 安全相关系统规定的安全完整性等级的有关规程,执行所有后续阶段。

注 1:可能有必要进行全面的危险和风险分析,这种分析需要 E/E/PE 安全相关系统的某个不同的安全完整性等级。

注 2:停用或处理阶段中的功能安全要求可能与操作阶段中的不同。

7.17.2.7 应建立和保存按时间编排的包括停用和处理活动细节的文档,其内容包括:

——用于停用或处理活动的计划;

——影响分析。

7.18 验证

7.18.1 目的

(通过复审、分析和/或测试)证明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的每个阶段,其输出全面满足各阶段规定的要求和目的。

7.18.2 要求

7.18.2.1 对整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期的每个阶段,应在拟定该阶段的同时就建立一个验证计划。

7.18.2.2 验证计划应编入或引用验证活动中所使用的准则、技术、工具。

7.18.2.3 验证应按验证计划进行。

注:验证技术和措施方法的选择以及验证活动的独立程度,取决于很多因素并可能在应用领域的标准中规定。这些因素的例子有:

——工程规模;

——复杂程度;

——设计的新颖程度;

——技术的新颖程度。

7.18.2.4 应收集验证活动的信息并文档化,作为已全面顺利完成该阶段验证工作的证据。

8 功能安全评估

8.1 目的

调查并判断 E/E/PE 安全相关系统所达到的功能安全。

8.2 要求

8.2.1 为判断 E/E/PE 安全相关系统是否达到功能安全要求,应指定一个或几个人进行功能安全评估。

8.2.2 进行安全评估时应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活动及相关信息和设备(硬件和软件)所涉及的所有人员进行访问。

8.2.3 应对整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期的所有阶段进行功能安

全评估。进行功能安全评估时应考虑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的每一个阶段中开展的活动和获得的输出并判断其满足 GB/T 20438 的目的和要求的程度。

8.2.4 功能安全评估应贯穿于整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期，并且可以在每个安全生命周期阶段之后或在几个安全生命周期阶段之后开展，但条件是在已确定的危险出现之前能采取一次功能安全评估。

8.2.5 如果把工具用作整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期任何活动的评价或设计的一部分，这些工具本身也要经受功能安全评估。

注 1：CAD/CAM、系统、编译器和主机目标系统可作为工具的例子。

注 2：需要评价使用这些工具的程度，它取决于这些工具对 E/E/PE 安全相关系统功能安全的影响。

8.2.6 功能安全评估应考虑如下内容：

——先前所做的功能安全评估工作(一般包括以前的安全生命周期阶段)；

——对整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期进一步执行功能安全评估的计划和战略；

——对先前的功能安全评估的建议以及已做更改的程度。

8.2.7 对于整体安全生命周期、E/E/PES 安全生命周期和软件安全生命周期不同阶段的功能安全评估应制定计划并保持一致。

8.2.8 功能安全评估活动计划应规定：

——承担功能安全评估的各方；

——每次功能安全评估的输出；

——功能安全评估的范围；

注：在建立功能安全评估的范围时，有必要规定用作每个评估活动输入的文档和它们的状态。

——所涉及的安全主体；

——要求的资源；

——承担功能安全评估各方的独立水平；

——与应用相关的承担功能安全评估各方的能力。

8.2.9 在进行功能安全评估之前，功能安全评估计划应得到执行功能安全评估的各方和负责正在评估的安全生命周期各阶段功能安全管理的各方的批准。

8.2.10 在功能安全评估结束时应做出接受、有条件地接受或不接受的建议。

8.2.11 承担功能安全评估的各方应能够胜任其工作，请注意附录 B 中评估能力的因素。

8.2.12 除非在应用领域的国家标准中另有说明，进行功能安全评估的人、部门或组织的最低独立水平应按表 4 和表 5 的规定。表 4 和表 5 中的相关内容说明如下：

——HR：它所规定的独立水平是为规定的后果(表 4)或安全完整性等级(表 5)而极力推荐的最低等级。如果使用更低的独立水平则应详细说明不使用 HR 水平的理由。

——NR：它所规定的独立水平对于规定的后果(表 4)或安全完整性等级(表 5)而言，被认为是不够的并不推荐此等级。如果采用该独立水平则应详细说明其理由。

—— —：不推荐或反对使用的规定独立水平。

注 1：应用表 4 之前，有必要考虑应用领域中现有的好的作法，以便定义后果的种类。这些后果出现在要求操作时 E/E/PE 安全相关系统的失效事件中。

注 2：在公司内部，可根据公司的机构和专家的情况而定。如要求独立的人和部门则不得不请某个外部的组织。相反，如果公司存在熟悉风险评估和安全相关系统应用的内部组织，该组织是独立的，并且与公司负责开发的主要组织是分开的(用管理或用其他资源等方法)则可使用它们自身的资源来满足独立组织的要求。

注 3：对于独立的人、独立的部门和独立组织的定义分别见 GB/T 20438.4—2006 的 3.8.10、3.8.11 和 3.8.12。

8.2.13 在表 4 和表 5 中，使用 HR[1] 还是 HR[2](不能两个都用)，取决于特定应用领域的诸多因素，如果

可以使用 HR^1，则 HR^2 被认为是不需要的；如果 HR^2 是可用的，则 HR^1 被认为是 NR(不推荐的)。如应用领域没有标准，应详细说明选择 HR^1 或 HR^2 的理由。选择 HR^2 比选择 HR^1 更合适的因素是：

——相同设计的经验不足；

——复杂程度很高；

——设计新颖度很高；

——技术新颖度很高；

——设计特征标准化程度不足。

8.2.14 在表 5 中，最低独立水平应基于具有最高安全完整性等级的 E/E/PE 安全相关系统执行的安全功能。

表 4 执行功能安全评估各方的最低独立水平[包括整体安全生命周期阶段 1～8 和 12～16(见图 2)]

最低独立水平	后果(见注 2)			
	A	B	C	D
独立的人	HR	HR^1	NR	NR
独立部门	—	HR^2	HR^1	NR
独立组织 (见 8.2.12 的注 2)	—	—	HR^2	HR

注 1：详细说明见 8.2.12(包括注)和 8.2.13。

注 2：典型的后果是：后果 A——较轻的伤害(如功能的暂时丧失)；后果 B——对一个或多个人的严重的、永久的伤害、致一人死亡；后果 C——致多人死亡；后果 D——致使非常多的人死亡。

表 5 进行功能安全评估各方的最低独立水平[整体安全生命周期阶段 9，包括 E/E/PES 安全生命周期和软件安全生命周期的所有阶段(见图 2，图 3 和图 4)]

最低独立水平	安全完整性等级			
	1	2	3	4
独立的人	HR	HR^1	NR	NR
独立部门	—	HR^2	HR^1	NR
独立组织 (见 8.2.12 的注 2)	—	—	HR^2	HR

注：详细说明见 8.2.12(包括注)、8.2.13 和 8.2.14。

附 录 A
（资料性附录）
文档结构范例

A.1 通则

为了满足第5章的要求，本附录给出了一个文档结构的范例以及规定用文档将信息结构化的方法。文档应包括为有效执行下列各项工作所必需的足够信息。

——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各阶段；

——功能安全的管理（第6章）；

——功能安全评估（第8章）。

足够信息的构成成分取决于一系列因素，包括E/E/PE安全相关系统的大小和复杂程度以及特定应用的相关要求。在应用领域标准中可能会规定必要的文档。

每个文档中的信息量可能是几行也可能是很多页，完整的信息集可能只放在一个实际文档中，也可能分开放在几个实际文档中。同样，实际文档的结构也取决于E/E/PE安全相关系统的大小和复杂程度，并且要考虑公司的规程和特定应用领域的工作经验。

本附录中的文档结构范例给出了构成信息的特殊方法和文档加标题的方法，更详细的说明参见参考文献[4]。

文档是一个试图让人理解的众多信息的集合体，可作为用户和系统之间以及系统之间进行交换的一个单元（见参考文献[5]，此术语不仅用于传统意义上的文档，也适用于数据文档或数据库信息。

在GB/T 20438中，文档这个术语一般的理解是指信息而不是实际文档，除非在讲到它的条款中有清楚地说明或能从中清楚地理解。文档可以使用不同形式（如纸张、胶片或任何可在屏幕或显示器上显示的数字媒体）。

本附录中的文档结构示例分两部分：

——文档种类；

——活动或目的。

文档种类在参考文献[3]中规定，并说明了文档内容的特点，如功能描述或电路图。活动或目的描述了内容的范围，如泵控制系统。

本附录中规定的基本文档种类如下：

——规范：规定一个需要的功能、性能或活动（如要求规范）；

——描述：规定一个计划的或实际的功能、设计、性能或活动（如功能描述）；

——说明书：对何时以及如何执行某项作业的说明进行详细规定（如操作员说明书）；

——计划：对何时、如何和由谁执行指定活动的计划进行规定（如维护计划）；

——图：用图（符号和线）表示符号间的信号以规定功能；

——表：用表的形式提供信息（如代码表、信号表）；

——日志：用按时间顺序编制的方式提供事件的信息；

——报告：描述活动，如调查、评估、测试等的结果（如测试报告）；

——请求：提出请求行动的描述，该行动必须经批准和进一步规定（如维护请求）。

基本文档种类也可以有前缀，如要求规范或测试规范，前缀进一步描述其内容的特点。

A.2 安全生命周期文档结构

为满足第5章规定的要求，表A.1、表A.2和表A.3给出了构成信息的文档结构示例，指出了与文

档相关的安全生命周期阶段(通常文档在此阶段中被拟定)。表 A.1、表 A.2 和表 A.3 中规定的文档根据 A.1 提出的方案命名。

除列于表 A.1、表 A.2 和表 A.3 的文档外,可能还有一些为提供详细附加信息或为特定目的而构建的信息的补充文档,如零部件表、信号表、电缆表、接线图、回路图、变量表等。

注:变量是指诸如调整器的值、变量的报警值、在计算机中执行任务的优先权等。一些变量值在系统交付之前就设定了,其他值则在试运行和维护中设定。

表 A.1 与整体安全生命周期有关信息的文档结构示例

整体安全生命周期阶段	信　　息
概念	描述(总体概念)
整体范围　定义	描述(整体范围定义)
危险和风险分析	描述(危险和风险分析)
整体安全要求	规范(整体安全要求,包括:整体安全功能和整体安全完整性)
安全要求分配	描述(安全要求分配)
整体操作和维护计划编制	计划(整体操作和维护)
整体安全确认计划编制	计划(整体安全确认)
整体安装和试运行计划编制	计划(整体安装);计划(整体试运行)
实现	E/E/PE 安全相关系统的实现(见 GB/T 20438.2 和 GB/T 20438.3)
整体安装和试运行	报告(整体安装);报告(整体试运行)
整体安全确认	报告(整体安全确认)
整体操作和维修	日志(整体操作和维修)
整体修改和改型	请求(整体修改);报告(整体修改和改型影响分析);日志(整体修改和改型)
停用或处理	报告(整体停用或处理影响分析);计划(整体停用或处理);日志(整体停用或处理)
所有有关阶段	计划(安全);计划(验证);报告(验证);计划(功能安全评估);报告(功能安全评估)

表 A.2 与 E/E/PES 安全生命周期有关信息的文档结构示例

E/E/PES 安全生命周期阶段	信　　息
E/E/PES 安全要求	规范(E/E/PES 安全要求,包括:E/E/PES 安全功能和 E/E/PES 安全完整性)
E/E/PES 确认计划编制	计划(E/E/PES 安全确认)
E/E/PES 设计和开发	
E/E/PES 结构	描述(E/E/PES 结构设计,包括硬件结构和软件结构)
	规范(可编程电子集成测试)
	规范(对可编程电子和非可编程电子硬件的集成测试)
硬件结构	描述(硬件结构设计)
	规范(硬件结构集成测试)
硬件模块设计	规范(硬件模块设计)
	规范(硬件模块测试)
部件构建和采购	硬件模块
	报告(硬件模块测试)

表 A.2(续)

E/E/PES 安全生命周期阶段	信　　息
可编程电子集成	报告(可编程电子和软件集成测试)(见表 A.3)
E/E/PES 集成	报告(可编程电子和其他硬件集成测试)
E/E/PES 操作和维护规程	说明书(用户) 说明书(操作和维护)
E/E/PES 安全确认	报告(E/E/PES 安全确认)
E/E/PES 修改	说明书(E/E/PES 修改规程) 要求(E/E/PES 修改) 报告(E/E/PES 修改影响分析) 日志(E/E/PES 修改)
E/E/PES 生命周期阶段	信　　息
所有有关阶段	计划(E/E/PES 安全) 计划(E/E/PES 验证) 报告(E/E/PES 验证) 计划(E/E/PES 功能安全评估) 报告(E/E/PES 功能安全评估)

表 A.3　与软件安全生命周期有关的信息文档结构示例

软件安全生命周期阶段	信　　息
软件安全要求	规范(软件安全要求,包括:软件安全功能和软件安全完整性)
软件确认计划编制	计划(软件安全确认)
软件设计和开发 软件结构 软件系统设计 软件模块设计 编码 软件模块测试 软件集成	描述(软件结构设计)(见表 A.2 中的硬件结构设计描述) 规范(软件结构集成测试) 规范(可编程电子和软件集合测试) 说明书(开发工具和编码手册) 描述(软件系统设计) 规范(软件系统集成测试) 规范(软件模块设计) 规范(软件模块测试) 表(源代码) 报告(软件模块测试) 报告(代码复审) 报告(软件模块测试) 报告(软件系统集成测试) 报告(软件结构集成测试)
可编程电子集成	报告(可编程电子和软件集成测试)
软件操作和维护规程	说明书(用户) 说明书(操作和维护)

表 A.3（续）

软件安全生命周期阶段	信　　息
软件安全确认	报告（软件安全确认）
软件修改	说明书（软件更新程序） 要求（软件更新） 报告（软件更新影响分析） 日志（软件更新）
所有有关阶段	计划（软件安全） 计划（软件验证） 报告（软件验证） 计划（软件功能安全评估） 报告（软件功能安全评估）

A.3　实际文档结构

文档的实际结构是这样的形式，即不同的文档可以组合成文档、文档集、文档包或文档包组，图 A.1 是根据用户组构建的文档包集的示例，同一个文档可能出现在不同的文档包集中。

对于大型复杂系统，许多实际文档可能被分裂成多个文档包，对于实际文档数有限的小型简单系统，可把带有不同检索标签的不同文档集组合成一个文档包（见图 A.2）。

实际结构为执行活动的人或人群选择特定活动所需文档提供了方法，因此一些实际文档可能出现于几个文档包中或出现于其他媒体上（如计算机磁盘）。

注：表 A.1 中文档所要求的信息可能被包括在图 A.1 和图 A.2 所示的不同的文档集中。例如在工程集中会包含危险和风险分析描述和/或整体安全要求规范的文档。

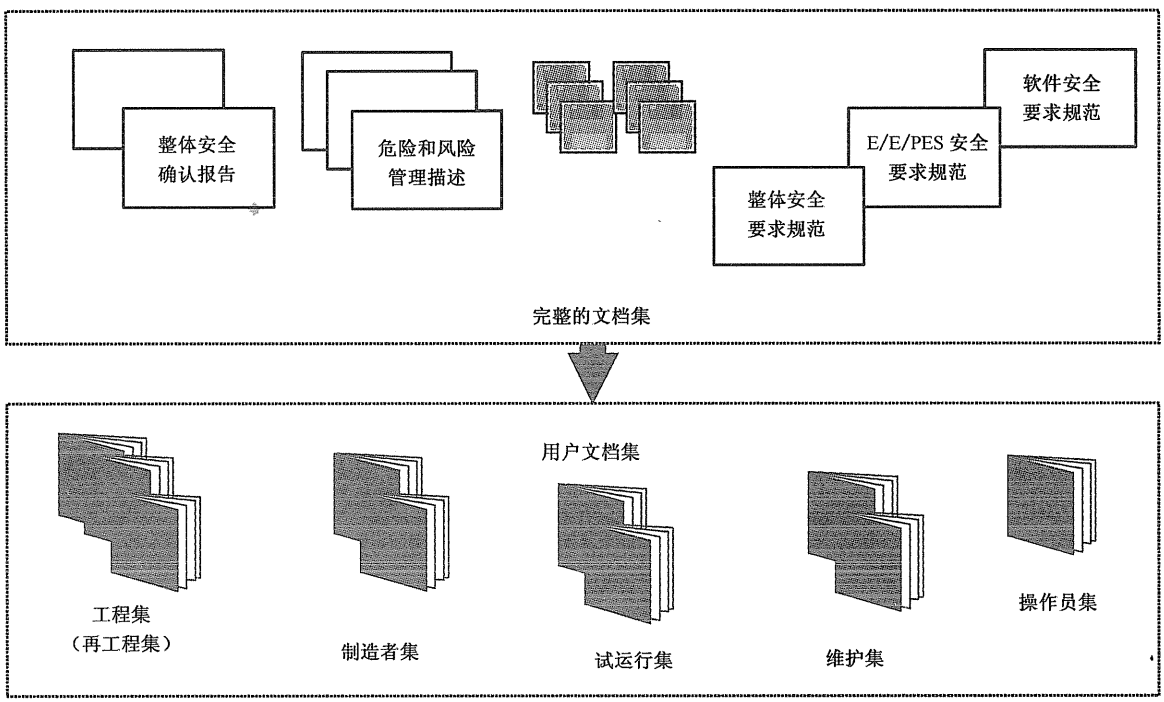


图 A.1　把信息构建成用户群的文档集

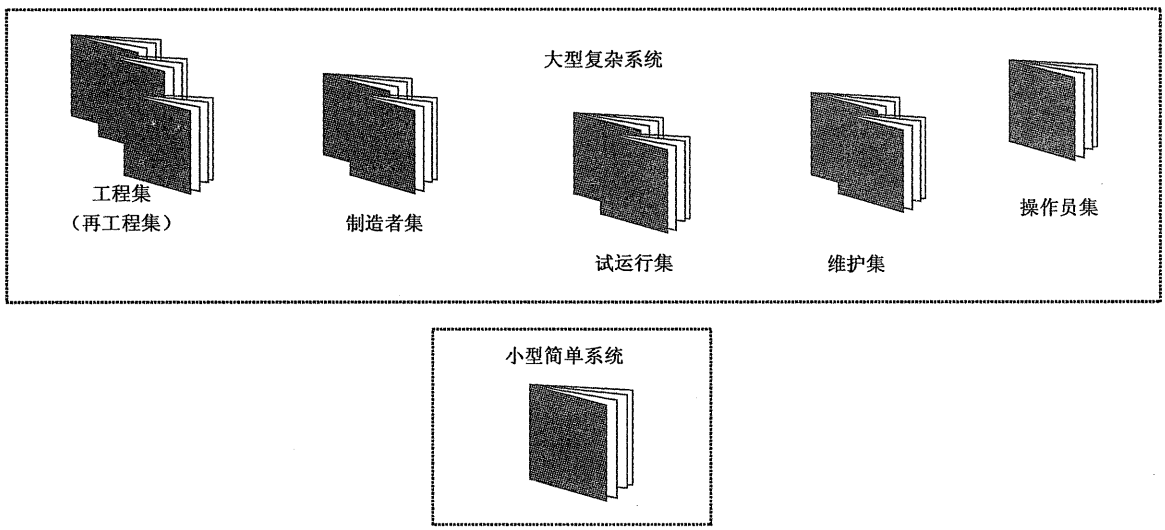


图 A.2 大型复杂系统和小型简单系统的结构化信息

A.4 文档清单

文档清单典型地包括下列内容：

——图样或文档号码；

——修订索引；

——文档指定代码；

——标题；

——修订日期；

——数据载体。

该清单可以不同形式出现，如可按文档或图的号码和指定代码储存的数据库。文档指定代码可能包含文档中描述的功能、位置或产品的参考命名，使其成为信息查询的有效工具。

附 录 B
（资料性附录）
人 员 能 力

B.1 目的

本附录所考虑的是保证对于整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期的任何活动负责的人具有履行其责任的能力。

B.2 一般考虑

涉及整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期的任何活动，包括管理活动的所有人员，应受过相关的培训、具有从事相关工作的技术知识、经验和资格。

应对涉及整体安全生命周期、E/E/PES 安全生命周期或软件安全生命周期的任何活动，包括任何功能安全管理活动的所有人员，在相关应用领域的培训、经验和资格进行评估。

当进行人员能力评估时应考虑下列因素：

a) 相关应用领域的工程知识。

b) 相关技术的工程知识（如电气、电子、可编程电子、软件工程）。

c) 相关技术的安全工程知识。

d) 法律和安全法规范围的知识。

e) E/E/PE 安全相关系统失效事件的后果。后果越严重，对资格的评估和规范就越严格。

f) E/E/PE 安全相关系统的安全完整性等级，安全完整性等级越高，对资格的评估和规范就越严格。

g) 设计、设计规程和应用的新颖程度。设计、设计规程和应用越是新颖，越是未经过试验，对资格的评估和规范就越严格。

h) 以往的经验和它与要履行的特定任务和使用的技术的关系。要求的资格水平越高，从以往经验中获得的能力就越接近适合承担特定任务所需的能力。

i) 资格与将履行的特定任务的关系。

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的任何活动有关的人员的培训、经验和资格都应文档化。

参 考 文 献

[1] IEC 60300-3-1:1991 可靠性管理 第3部分:应用指南 第1章:可靠性分析技术:方法论指南.

[2] IEC 60300-3-9:1995 可靠性管理 第3部分:应用指南 第9章:技术系统的风险分析.

[3] IEC 61355:1997 工厂、系统和设备文档的分类和命名.

[4] IEC 61506:1997 工业过程测量和控制 应用软件文档.

[5] ISO 8613-1:1994 信息技术 开放式文档体系结构(ODA)和交换格式:介绍和基本原理.

[6] ISO 10007:1995 质量管理 配置管理指南.

[7] ISO/IEC TR 15846 信息技术 软件生命周期过程 软件配置管理.

[8] ANSI/ISA S84:1996 对过程工业装有安全仪表的系统的应用.

[9] 在安全和可靠性研究中,处理共同原因失效的规程 规程框架和示例.NUREG/CR-4780,1988-01,1.

[10] 在安全和可靠性研究中,处理共同原因失效的规程 分析背景和技术.NUREG/CR-4780,1989-01,2.

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

GB/T 20438.1—2006/IEC 61508-1:1998