ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.2—2006/IEC 61508-2:2000

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

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2:Requirements for electrical/electronic/programmable electronic safety-related systems

(IEC 61508-2:2000,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2部分:电气/电子/可编程电子安全相关系统的要求
GB/T 20438.2—2006/IEC 61508-2:2000
*
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 3.5 字数 99 千字
2007年2月第一版 2007年2月第一次印刷
*
书号:155066·1-28707 定价 22.00 元

GB/T 20438.2-2006

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 2 部分。

本部分等同采用国际标准 IEC 61508-2:2000《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》(英文版)。

本部分的附录 A、附录 B、附录 C 为规范性附录。

本部分与 IEC 61508-2:2000 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 中的注 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：梅恪、冯晓升、王莉、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2部分:电气/电子/可编程电子安全相关系统的要求

1 范围

1.1 GB/T 20438.2

a) 在使用前,应充分理解GB/T 20438.1,GB/T 20438.1提供了实现功能安全的总体结构框架。

b) 适用于GB/T 20438.1定义的安全相关系统,安全相关系统至少包含一种电气、电子或可编程电子基本部件。

c) 适用于E/E/PE安全相关系统中的所有子系统及其部件(包括传感器、执行器、操作员界面)。

d) 规定了如何按照GB/T 20438.1从整体安全要求中提取开发信息并将其分配到E/E/PE安全相关系统;规定了如何从整体安全要求中提取E/E/PES的安全功能要求和E/E/PES安全完整性要求。

e) 规定了在E/E/PE安全相关系统的设计和制造过程中所进行的活动的要求(例如:建立E/E/PES安全生命周期模型),软件除外;软件要求在GB/T 20438.3(见图2、图3)中给出;这些要求包含了用以避免和控制故障和失效发生的技术和措施的应用,并被划分成与安全完整性等级相对应的不同等级。

f) 规定了执行E/E/PE安全相关系统的安装、试运行以及最终安全确认所需的信息。

g) 不适用于E/E/PE安全相关系统的操作和维护阶段,这方面内容在GB/T 20438.1中给出。但是,本部分为用户提供了有关E/E/PE安全相关系统的操作和维护所需的信息和规程的准备要求。

h) 对E/E/PE安全相关系统进行各种修改的各方应满足的要求进行了规定。

注1:本部分直接面向供方和/或公司内部的工程部门,因此包含了对修改的要求。

注2:本部分与GB/T 20438.3的关系见图3。

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的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使用。

在适用的情况下,技术委员会在制定其标准时都应使用基础安全标准。也就是说,本基础安全标准涉及的要求、测试方法或测试条件,只有在相关技术委员会制定标准时加以引用或包含时,才能得到应用。

注:仅当所有相关要求得到满足时,才能达到E/E/PE安全相关系统的功能安全。因此,认真考虑和充分参照所有相关要求是十分重要的。

1.3 图1表示了GB/T 20438的总体框架,同时指出了本部分在达到E/E/PE安全相关系统的功能安全时所起的作用。GB/T 20438.6—2006的附录A详述了GB/T 20438.2和GB/T 20438.3的应用。

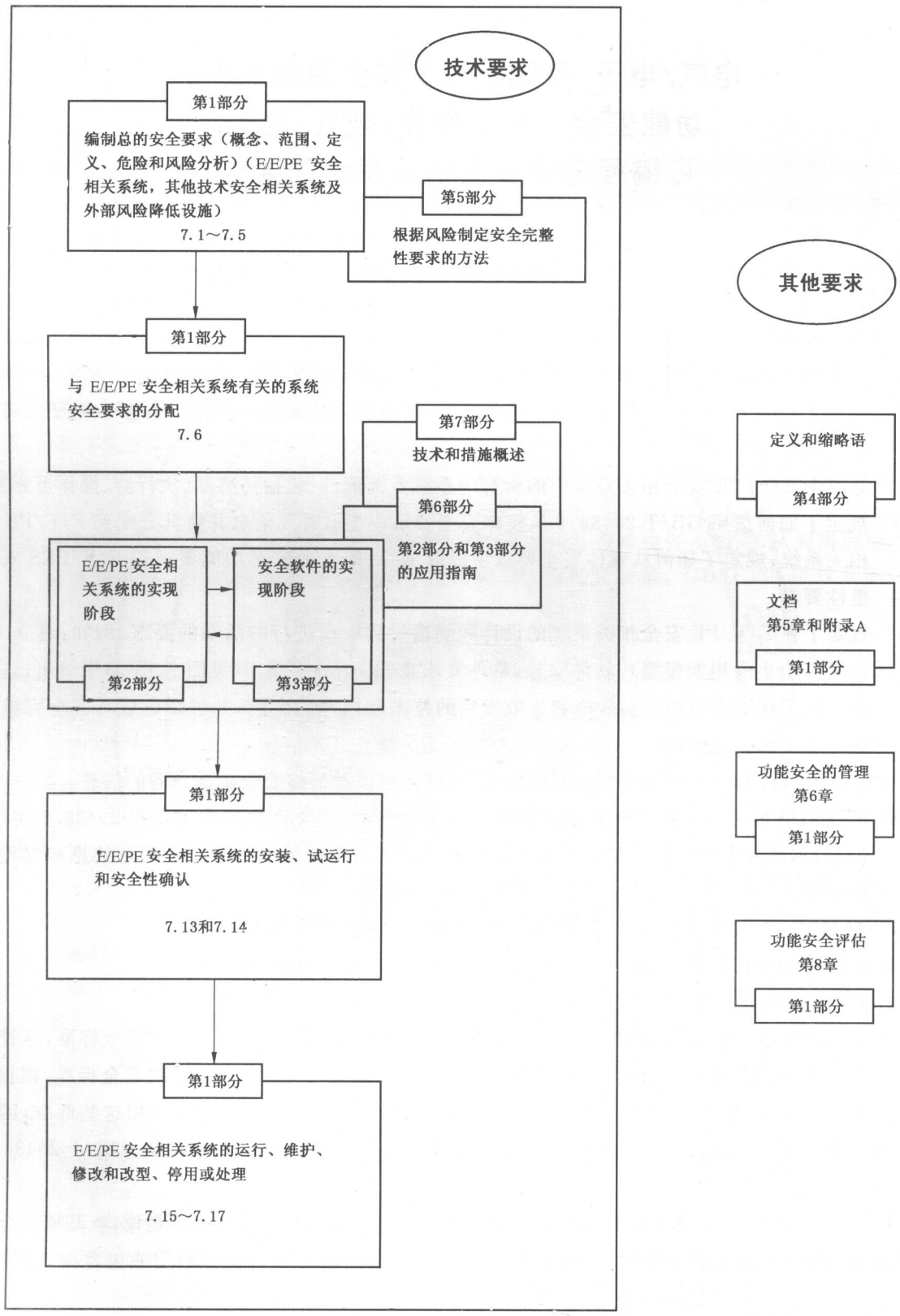


图 1　GB/T 20438 的总体框架

2 规范性引用文件

下列文件中的条款通过 GB/T 20438.2 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 20438.1—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 20438.3—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)

IEC 60050(371):1984 国际电气词汇 371章：遥控

IEC 60300-3-2:1993 可靠性管理 第3部分：应用指南 第2篇：现场可靠性数据的采集

IEC 61000-1-1:1992 电磁兼容性(EMC) 第1部分：概述 第1篇：基本定义、术语的应用和说明

IEC 61000-2-5:1995 电磁兼容性(EMC) 第2部分：环境 第5篇：电磁环境的分类 基本电磁兼容性出版物

IEEE 352:1987 核电站安全相关系统可靠性分析一般原理的指南

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

见 GB/T 20438.4。

4 与 GB/T 20438 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 功能安全管理

见 GB/T 20438.1—2006 的第6章。

7 E/E/PES 安全生命周期要求

7.1 一般要求

7.1.1 目的和要求：一般要求

7.1.1.1 本条阐述 E/E/PES 安全生命周期各阶段的目的和要求。

注：整体安全生命周期的目的和要求以及标准结构的简述在 GB/T 20438.1 中给出。

7.1.1.2 对于 E/E/PES 安全生命周期的所有阶段，表 1 给出了：

——需要达到的目的；

——各阶段的范围；

——要求所在的条款；

——各阶段所要求的输入；

——符合条款要求的输出。

7.1.2 **目的**

7.1.2.1 以系统化的方式构造应考虑的 E/E/PES 安全生命周期的各阶段，以达到 E/E/PE 安全相关系统所需的功能安全。

7.1.2.2 将贯穿于 E/E/PES 安全生命周期的有关 E/E/PE 安全相关系统功能安全的所有信息文档化。

7.1.3 **要求**

7.1.3.1 符合 GB/T 20438 的 E/E/PES 安全生命周期如图 2 所示。若应用其他安全生命周期，应在功能安全计划编制(见 GB/T 20438.1—2006 的第 6 章)时加以说明，并应满足本部分所有条款的目的和要求。

注：本部分和 GB/T 20438.3 的关系和范围见图 3。

7.1.3.2 功能安全的管理规程(见 GB/T 20438.1—2006 的第 6 章)应与 E/E/PES 安全生命周期的各阶段并行。

7.1.3.3 E/E/PES 安全生命周期的每个阶段都应根据各阶段规定的范围、输入、输出(见表 1)划分成相应的基本活动。

7.1.3.4 除非在功能安全的计划编制过程中有正当理由，否则 E/E/PES 安全生命周期的每个阶段的输出都应文档化(见 GB/T 20438.1—2006 的第 5 章)。

7.1.3.5 E/E/PES 安全生命周期的每个阶段的输出都应符合各阶段规定的目的和要求(见 7.2～7.9)。

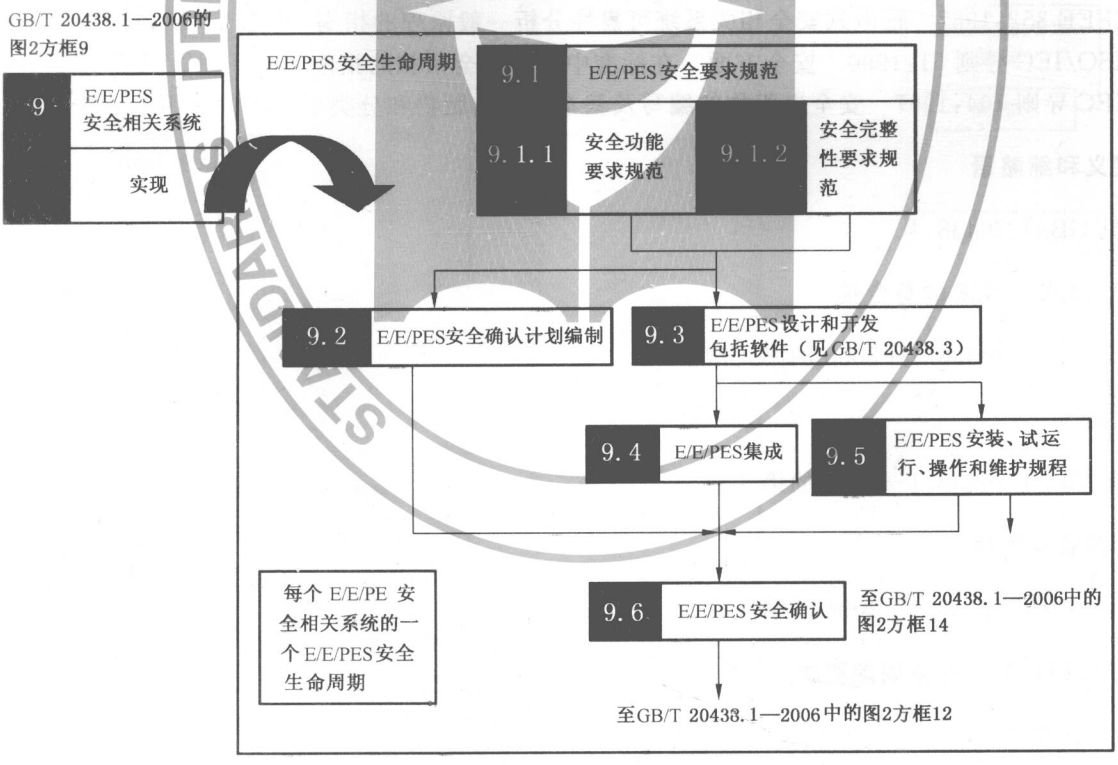


图 2 E/E/PES 安全生命周期(实现阶段)

注：另见 GB/T 20438.6—2006 附录 A 中的 A.2 b)。

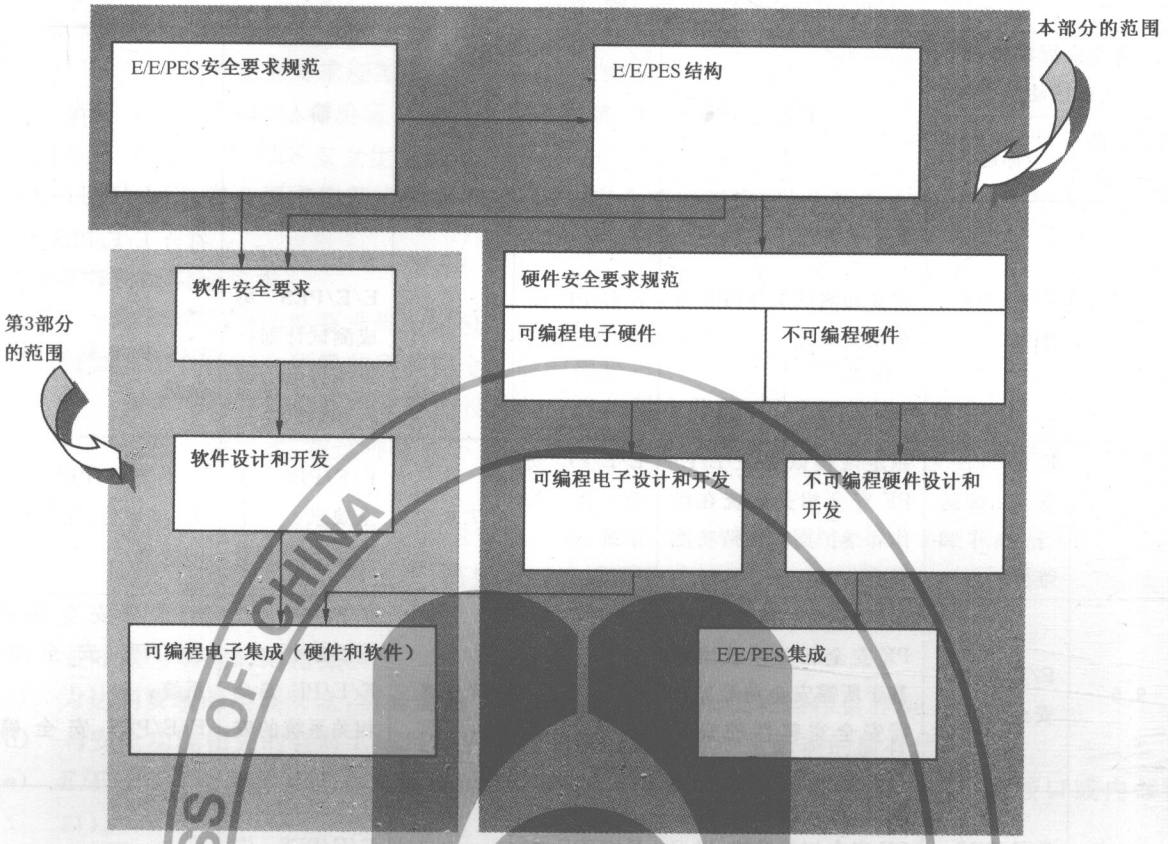


图 3　GB/T 20438.2 和 GB/T 20438.3 的范围和关系

表 1　E/E/PES 安全生命周期实现阶段概述

安全生命周期阶段或活动		目的	范围	要求所在的条款	输入	输出
图 2 中的方框号	标题					
9.1	E/E/PES 安全要求规范	为达到所需的功能安全，根据所需的安全功能和所需的安全完整性规定每个 E/E/PE 安全相关系统的要求	E/E/PE 安全相关系统	7.2.2	安全要求分配的描述（见 GB/T 20438.1—2006 的 7.6）	E/E/PES 安全要求； 软件安全要求（作为软件安全要求规范的输入）
9.2	E/E/PES 安全确认计划编制	编制 E/E/PE 安全相关系统的安全确认计划	E/E/PE 安全相关系统	7.3.2	E/E/PES 安全要求	E/E/PE 安全相关系统的安全确认计划
9.3	E/E/PES 设计和开发	设计满足安全功能要求和安全完整性要求的 E/E/PE 安全相关系统	E/E/PE 安全相关系统	7.4.2～7.4.8	E/E/PES 安全要求	符合 E/E/PES 安全要求的 E/E/PE 安全相关系统设计； E/E/PES 集成测试计划； PES 结构化信息（作为软件要求规范的输入）

表 1(续)

安全生命周期阶段或活动		目的	范围	要求所在的条款	输入	输出
图 2 中的方框号	标题					
9.4	E/E/PES 集成	集成和测试 E/E/PE 安全相关系统	E/E/PE 安全相关系统	7.5.2	E/E/PES 设计； E/E/PES 集成测试计划； 可编程电子硬件和软件	符合 E/E/PES 设计的全功能的 E/E/PE 安全相关系统； E/E/PES 集成测试的结果
9.5	E/E/PES 安装、试运行、操作和维护规程	制定规程以保证 E/E/PE 安全相关系统在操作和维护期间保持功能安全	E/E/PE 安全相关系统； EUC	7.6.2	E/E/PES 安全要求； E/E/PES 设计	各个 E/E/PES 单独安装、试运行、操作和维护的规程
9.6	E/E/PES 安全确认	在所有方面，确认 E/E/PE 安全相关系统满足基于所需安全功能和所需安全完整性的安全要求	E/E/PE 安全相关系统	7.7.2	E/E/PES 安全要求； E/E/PE 安全相关系统的安全确认计划	经充分安全确认的 E/E/PE 安全相关系统； E/E/PES 安全确认结果
—	E/E/PES 修改	改正、加固或适应 E/E/PE 安全相关系统，以保证达到和维持所需的安全完整性等级	E/E/PE 安全相关系统	7.8.2	E/E/PES 安全要求	E/E/PES 修改结果
—	E/E/PES 验证	就某阶段输入的产品和标准而言，测试和评价该阶段的输出，以保证正确性和一致性	E/E/PE 安全相关系统	7.9.2	同上，依赖于某阶段； 每个阶段 E/E/PE 安全相关系统的验证计划	同上，依赖于某阶段； 每个阶段 E/E/PE 安全相关系统的验证结果
—	E/E/PES 功能安全评估	调查和判断 E/E/PE 安全相关系统所达到的功能安全	E/E/PE 安全相关系统	8	E/E/PES 功能安全评估计划	E/E/PES 功能安全评估结果

7.2 E/E/PES 安全要求规范

注：这一阶段是图 2 的方框 9.1。

7.2.1 目的

为达到所需的功能安全，根据所需的安全功能和所需的安全完整性规定每个 E/E/PE 安全相关系统的要求。

注：例如，要使 EUC 进入安全状态或保持安全状态要对安全功能提出要求。

7.2.2 一般要求

7.2.2.1 E/E/PES 安全要求规范应来源于 GB/T 20438.1—2006 的 7.6 规定的安全要求的分配，以及功能安全计划编制中规定的要求(见 GB/T 20438.1—2006 的第 6 章)。E/E/PES 的开发者应可获得这些信息。

注：如果同一 E/E/PE 安全相关系统即执行非安全功能又执行安全功能，要加倍谨慎。虽然，这是标准所允许的，

但这将会导致执行 E/E/PE 安全生命周期活动(例如设计、确认、功能安全评估和维护)的过程更加复杂并使难度增加。

7.2.2.2 E/E/PES 的安全要求应按以下要求表述和组织

a) 清晰、准确、无歧义、可验证、可测试、可维护并切实可行;和

b) 便于采用 E/E/PES 安全生命周期任一阶段信息的各方理解。

7.2.2.3 E/E/PES 安全要求规范应包含 E/E/PES 安全功能要求(见 7.2.3.1)和 E/E/PES 安全完整性要求(见 7.2.3.2)。

7.2.3 E/E/PES 安全要求

7.2.3.1 E/E/PES 安全功能要求规范应包括:

a) 达到要求功能安全所需的所有安全功能的描述,针对每一安全功能应:

——为 E/E/PE 安全相关系统的设计与开发提供充分的、可理解的详细要求;

——包括一种方式,在这种方式下,E/E/PE 安全相关系统被用来达到或保持 EUC 的某种安全状态;

——规定在达到或保持 EUC 安全状态时是否要求连续控制,以及在什么时期控制;

——规定在低要求操作模式下,高要求或连续操作模式下,安全功能是否适用于 E/E/PE 安全相关系统。

b) 吞吐量与响应时间指标。

c) 为达到要求的功能安全,所必需的 E/E/PE 安全相关系统和操作员界面。

d) 与安全功能相关的会对 E/E/PE 安全相关系统的设计产生影响的所有信息。

e) E/E/PE 安全相关系统与其他系统之间的所有接口(与 EUC 直接关联的外部接口或内部接口)。

f) EUC 操作的所有相关模式,包括:

——使用准备,包括设置与调整;

——启动、教学、全自动、手动、半自动、稳定的工作状态;

——非工作时的稳定状态,重设置,关机,维护;

——合理的、可预见的异常工况。

注 1:合理的、可预见的异常工况是指开发者与用户所能合理预见到的异常工况。

注 2:特殊的操作模式(例如设置、调整、维护)可能要求附加的安全功能,以使这些操作能安全执行。

g) E/E/PE 安全相关系统行为的所有要求模式——尤其是 E/E/PE 安全相关系统的失效行为和要求的响应(例如报警、自动关机等)应当详细说明。

h) 所有硬件或软件相互作用的重要性——当相关时,硬件或软件之间要求的约束应加以标识和文档化。

注 3:在完成设计之前不知道相互作用的情况下,只能对一般约束加以说明。

i) E/E/PE 安全相关系统和相关子系统的限制与约束条件,例如:定时约束。

j) 启动和再启动 E/E/PE 安全相关系统的有关规程的任何特殊要求。

7.2.3.2 E/E/PES 安全完整性要求规范应包括:

a) 每一安全功能的安全完整性等级,以及需要时(见注 2)安全功能要求的目标失效量。

注 1:依照 GB/T 20438.1—2006 的表 2 和表 3,某个安全功能的安全完整性等级确定了该安全功能的目标失效量。

注 2:在使用定量方法推导安全功能所需的风险降低时,需要规定该安全功能的目标失效量(见 GB/T 20438.1—2006 的 7.5.2.2)。

b) 每一安全功能的操作模式(低要求、高要求或连续)。

c) 使 E/E/PE 的硬件检验测试得以实施的要求、约束、功能与设备。

d) 在 E/E/PES 的安全生命周期中,包括制造、贮存、运输、检测、安装、试运行、操作和维护中可

能遇到的极端环境条件。

e) 达到的电磁兼容性要求的抗电磁干扰极限(见 IEC 61000-1-1) ——抗电磁干扰极限,应依据电磁环境(见 IEC 61000-2-5)和所需的安全完整性等级得出。

注 1:认识到安全完整性等级是决定抗电磁干扰极限的一个因素是很重要的,特别是由于环境的电磁干扰水平服从统计分布的原因。在很多现实情况下,不可能规定一个绝对的干扰水平。实际上,只能预计不超过某一水平(就是电磁兼容水平)。但是操作中的困难使得这种预计的概率难以确定。因此,抗干扰极限并不能保证 E/E/PE 安全相关系统不会由于电磁干扰而失效,它仅为在某种程度上提供某种置信度水平。实际达到的置信度水平是在操作环境下与干扰水平的统计分布有关的抗干扰极限功能。安全完整性等级越高就需要更高的置信度水平,这意味着对于越高的安全完整性等级,抗干扰极限超过电磁兼容水平的容限应当越大。

注 2:同时,在 EMC 产品标准中可以找到相应的指导,但重要的是要认识到如果设备要在严酷的电磁环境下使用或装在某些特殊的位置时,抗干扰水平要高于这些标准中规定的水平。

注 3:在拟定 E/E/PES 安全要求规范时,要考虑 E/E/PE 安全相关系统的应用领域。这对维护尤其重要,规定的检验测试间隔要不小于对特殊应用的合理预期值。例如,公众使用的批量生产项目中实际得到的服务间隔时间要比在有更多控制的应用中的服务间隔时间大得多。

7.2.3.3 为避免 E/E/PES 安全要求规范中的失误,应当使用表 B.1 中的一组合适的技术和措施。

7.3 E/E/PES 安全确认计划编制

注:这一阶段是图 2 的方框 9.2。它通常与 E/E/PES 设计和开发并行(见 7.4)。

7.3.1 目的

编制 E/E/PE 安全相关系统的安全确认计划。

7.3.2 要求

7.3.2.1 编制计划以便规定用于证明 E/E/PE 安全相关系统满足 E/E/PES 安全要求规范(见 7.2)的步骤(包括规程的和技术的)。

注:见 GB/T 20438.3 的软件确认计划。

7.3.2.2 编制 E/E/PE 安全相关系统的确认计划应考虑:

a) E/E/PES 安全要求规范定义的所有要求;

b) 用于确认每一安全功能正确实现的规程和在完成测试时的通过或未通过的准则;

c) 用于确认每一安全功能所需的安全完整性的规程和在完成测试时通过或未通过的准则;

d) 测试所需的环境,包括所有所需的工具和设备(还包括工具与设备的校准计划);

e) 测试评价规程(带合理性证明);

f) 应用于确认规定的抗电磁干扰极限的测试规程和性能准则;

注:抗干扰测试极限规范的指南由 IEC 61000-2-5 和 IEC 61000-4 给出。

g) 解决确认失效的方针。

7.4 E/E/PES 的设计与开发

注:这一阶段是图 2 的方框 9.3,它通常与 E/E/PES 安全确认计划编制并行(见 7.3)。

7.4.1 目的

确保 E/E/PE 安全相关系统的设计和实现满足规定的安全功能和安全完整性要求(见 7.2)。

7.4.2 一般要求

7.4.2.1 考虑 7.4 的所有要求,并根据 E/E/PES 安全要求规范(见 7.2)设计 E/E/PE 安全相关系统。

7.4.2.2 E/E/PE 安全相关系统的设计(包括硬、软件的整体结构、传感器、执行器、可编程电子、嵌入式软件和应用软件等,见图 4),应当符合以下 a)~c)的全部要求:

a) 硬件安全完整性要求包括:

——硬件安全完整性的结构约束(见 7.4.3.1);和

——危险随机硬件失效概率的要求(见 7.4.3.2)。

b) 系统安全完整性要求包括：

——避免失效的要求(见 7.4.4)和系统故障控制的要求(见 7.4.5)；或

——设备“经使用证实”的证据(见 7.4.7.6～7.4.7.12)。

c) 故障检测时对系统行为的要求(见 7.4.6)。

注 1：E/E/PES 安全完整性整体框架：为证明达到 E/E/PE 安全相关系统中的某个安全完整性等级(硬件的和系统的)，选择一种设计方案的总体方法如下：

——确定安全功能所要求的安全完整性等级(SIL)(见 GB/T 20438.1 和 GB/T 20438.5)；

——设置：硬件安全完整性＝系统安全完整性＝SIL(见 7.4.3.2.1)；

——对于硬件安全完整性，确定能够满足结构约束条件的结构(见 7.4.3.1)，并且证明由于随机硬件失效引起的安全功能失效的概率能够满足要求的目标失效量(见 7.4.3.2)；

——对于系统安全完整性，选择实际操作中控制(容许)系统故障(见 7.4.5)的设计特性或是证明“经使用证实”的要求已经得到满足(见 7.4.7.6～7.4.7.12)；

——对于系统安全完整性，选择在设计与开发中避免(防止引入)系统故障(见 7.4.4)的技术和措施或是证明“经使用证实”的要求已经得到满足(见 7.4.7.6～7.4.7.12)。

注 2：GB/T 20438.3 包括软件结构要求(见 7.4.2.2)；产生可编程电子和软件集成测试规范的要求(见 7.5)；依据该规范(见 7.5)集成可编程电子和软件的要求。在所有情况下，E/E/PE 安全相关系统的开发者与软件开发者之间的密切合作都是必需的。

结构示例，可以是：

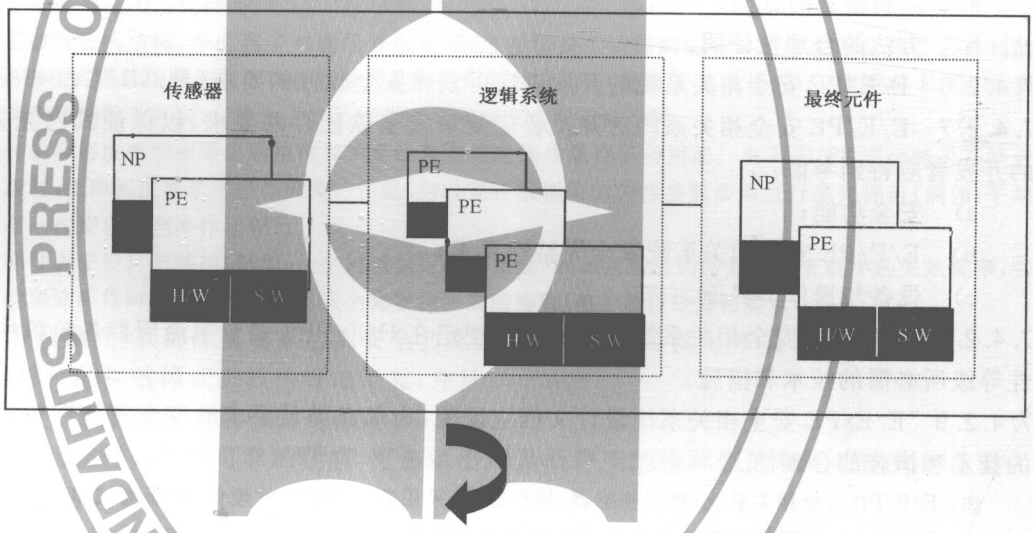
——单通道；

——双通道；

——1oo2，

1oo3，

2oo2 等



可编程电子结构		
PE 硬件结构	**PE 软件结构(S/W 结构包括嵌入式 S/W 和应用 S/W)**	
PE 硬件中通用的和应用时的具体特性： 例如包括： ——诊断测试； ——冗余处理器； ——双 I/O 卡	PE 嵌入式软件	PE 应用软件
	例如包括： ——通信驱动器； ——故障处理； ——可执行软件	例如包括： ——输入/输出功能； ——派生功能(例如，未提供嵌入式软件服务时的传感器检验)

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 4 可编程电子中软件结构和硬件结构的关系

7.4.2.3 在E/E/PE安全相关系统既执行安全功能又执行非安全功能的地方，除非能够表明实现安全功能和非安全功能是充分独立的(也就是说，非安全功能的失效不会引起安全功能的危险失效)，否则所有的软硬件都应被视为与安全相关的。只要可行，安全功能应与非安全功能分开。

注1：非安全和安全部件之间相关失效概率与安全功能包含的最高安全完整性等级相比足够低，即意味着实现的充分独立。

注2：当在同一E/E/PE安全相关系统中实现非安全功能和安全功能时，要谨慎操作。虽然，这是标准所允许的，但这将会导致执行E/E/PE安全生命周期活动(例如设计、确认、功能安全评估和维护)的过程更加复杂并使难度增加。

7.4.2.4 软硬件的要求由拥有最高安全完整性等级的安全功能的安全完整性等级来决定，除非能够表明不同安全完整性等级的安全功能的实现是充分独立的。

注1：实现不同安全完整性等级的安全功能的各部分之间的相关失效概率与安全功能包含的最高安全完整性等级相比足够低，即意味着实现的充分独立。

注2：在一个E/E/PE安全相关系统实现几个安全功能时，需要考虑单一故障会引起几个安全功能失效的概率。在这种情况下，恰当的作法是根据这类失效的风险，按照比任何一个安全功能相关的安全完整性等级更高的安全完整性等级确定软硬件的要求。

7.4.2.5 在要求安全功能之间相互独立(见7.4.2.3和7.4.2.4)时，在设计时以下几条应文档化：

a) 达到独立的方法；

b) 方法的合理性证明。

7.4.2.6 E/E/PE安全相关系统的开发者应可获得安全软件的要求(见GB/T 20438.3)。

7.4.2.7 E/E/PE安全相关系统的开发者应复审安全软硬件的要求，以保证其已充分规定。E/E/PE的开发者应特别考虑：

a) 安全功能；

b) E/E/PE安全相关系统安全完整性要求；

c) 设备与操作员界面。

7.4.2.8 E/E/PE安全相关系统设计文档应规定在E/E/PES安全生命周期各阶段中为达到安全完整性等级所必需的技术和措施。

7.4.2.9 E/E/PE安全相关系统设计文档应证明，为形成满足要求的安全完整性等级的集成集所选择的技术和措施的合理性。

注：E/E/PE安全相关系统(包括传感器、执行器等)采用独立类型的软硬件、诊断测试和编程工具，并利用适当的软件语言，都有可以降低E/E/PES应用工程的复杂性的潜力。

7.4.2.10 在设计与开发活动中，应认识、评估和文档化所有软硬件相互作用的重要意义(如相关)。

7.4.2.11 设计应基于子系统分解的方法，每一个子系统有规定的设计和系列集成测试(见7.4.7)。

注1：一个部件或任意部件组都可以认为是一个子系统。一个完整的E/E/PE安全相关系统是由一系列一起执行安全功能的、可识别并分开的子系统构成。子系统可以拥有一个以上的通道，见7.4.7.3。

注2：只要可行，在实现中要尽量使用现有的经验证过的子系统。本陈述一般仅在下述两种情况下有效：如果现有子系统的功能、能力、性能几乎能够100%地映射于新要求上；或是已验证过的子系统由这样一种方式组成，即用户仅能选择特殊应用所需的功能、能力和性能。如果现有子系统被做得太复杂或是有未被使用的特性，并且不能防止不期望的功能，过多的功能、能力或性能会有损于系统安全。

7.4.2.12 带多路输出的子系统，有必要确定由E/E/PE安全相关系统失效引起的一些输出状态的组合是否能够直接引发危险事件(如用危险与风险分析来确定，见GB/T 20438.1—2006的7.4.2.10)。本条建立后，对输出状态的组合的预防措施应被视为在高要求或连续操作模式下工作的一个安全功能(见7.4.6.3和7.4.3.2.5)。

7.4.2.13 所有的部件应尽可能降额(见GB/T 20438.7—2006附录A的A.2.8)使用。在其极限值下使用任意部件的合理性证明应文档化(见GB/T 20438.1—2006的第5章)。

注：降额系数至少为0.67才合适。

7.4.3 硬件安全完整性要求

注：GB/T 20438.6—2006 附录 A 的 A.2 提供了达到要求的硬件安全完整性所需步骤的概述，并说明了本条与 GB/T 20438 的其他要求之间的关系。

7.4.3.1 硬件安全完整性的结构约束

7.4.3.1.1 硬件安全完整性的安全功能所声明的最高安全完整性等级，受限于硬件故障裕度和执行该安全功能的子系统的安全失效分数(见附录 C)。表 2 和表 3 规定了安全功能所声明的最高安全完整性等级，该安全功能使用了一个考虑了该子系统的硬件故障裕度和安全失效分数的子系统(见附录 C)。表 2 与表 3 的要求应适用于执行安全功能的每一子系统和 E/E/PE 安全相关系统的每一部分。7.4.3.1.2～7.4.3.1.4 规定了表 2 与表 3 中的哪一个适用于任一特定子系统。7.4.3.1.5 和 7.4.3.1.6 规定了如何导出安全功能所声明的最高安全完整性等级。对于这些要求：

a) 硬件故障裕度 N 意味着 $N+1$ 个故障会导致全功能的丧失，在确定硬件故障裕度时不考虑其他可能控制故障影响的措施，如诊断。

b) 若一个故障可直接引起一个或几个后续故障的发生，这些故障可视为单个故障。

c) 在确定硬件故障裕度时，如果相对于子系统安全完整性而言某些故障出现的可能性很小，这些故障可不考虑。不考虑这类故障的合理性应被证明和文档化(见注 3)。

d) 子系统安全失效分数的定义为子系统的平均安全失效率加检测到的平均危险失效率与子系统总平均失效率之比(见附录 C)。

注 1：为了达到足够健壮的结构，考虑到子系统的复杂水平，已经包括了结构的约束。通过应用这些要求得到的 E/E/PE 安全相关系统的硬件安全完整性等级是允许声明的最高值。尽管在某些情况下，如果对 E/E/PE 安全相关系统采用纯数学方法，在理论上也可以导出更高的安全完整性等级。

注 2：为满足硬件故障裕度要求而导出的结构和子系统是在正常操作条件下使用的。当 E/E/PE 安全相关系统进行在线修理时，故障裕度要求可适当放宽。但是，与放宽要求相关的关键参数必须进行事先评价(例如：平均恢复时间与一次要求的概率作比较)。

注 3：如果一个部件由于设计与结构(例如，一个机械执行器连接器)的固有属性的特点仅具有极小的失效概率，将不必考虑使用该部件时任何安全功能的安全完整性所需的约束(基于硬件故障裕度)。

7.4.3.1.2 满足下列条件，其部件被要求达到安全功能的一个子系统可视为 A 类：

a) 所有组成部件的失效模式都被很好地定义；并且

b) 故障状况下子系统的行为能够完全确定；并且

c) 通过现场经验获得充足而可靠的数据，可显示出满足所声明的检测到的和未检测到的危险失效的失效率(见 7.4.7.3 和 7.4.7.4)。

7.4.3.1.3 满足下列条件，其部件被要求达到安全功能的一个子系统可视为 B 类：

a) 至少一个组成部件的失效模式未被很好地定义；或

b) 故障状况下子系统的行为不能完全确定；或

c) 通过现场经验获得的可靠的数据不够充分，不足以显示出满足所声明的检测到的和未检测到的危险失效的失效率(见 7.4.7.3 和 7.4.7.4)。

注：这就是说，如果子系统中只要有一个组成部件满足 B 类的条件，那么这个子系统应被视为 B 类，而不是 A 类。参见 7.4.2.11 的注 1。

7.4.3.1.4 表 2 或表 3 的结构约束应适用于每一个执行安全功能的子系统，所以：

a) 应达到整个 E/E/PE 安全相关系统的硬件故障裕度的要求；

b) 表 2 用于 E/E/PE 安全相关系统构成中的每一个 A 类子系统；

注 1：如果 E/E/PE 安全相关系统仅包括 A 类子系统，那么在表 2 中的要求将适用于整个 E/E/PE 安全相关系统。

c) 表 3 用于 E/E/PE 安全相关系统构成中的每一个 B 类子系统；

注 2：如果 E/E/PE 安全相关系统仅包括 B 类子系统，那么在表 3 中的要求将适用于整个 E/E/PE 安全相关系统。

d) 表 2 与表 3 适用于由 A 类和 B 类子系统组成的 E/E/PE 安全相关系统，表 2 的要求适用于 A 类子系统，表 3 的要求适用于 B 类子系统。