ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.1—2017/IEC 61508-1:2010
代替 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

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

(IEC 61508-1:2010,IDT)

2017-12-29 发布　　2018-07-01 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《电气/电子/可编程电子安全相关系统的功能安全》分为七个部分：

——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。

本部分为GB/T 20438的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替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》，与GB/T 20438.1—2006相比，主要技术变化如下：

——增加了功能安全管理中，人员能力的要求(见第6章)；

——增加了整体安全生命周期中，E/E/PE系统安全要求规范阶段(见7.10)；

——修改了评估独立性的评价方法(见第8章)。

本部分使用翻译法等同采用IEC 61508-1:2010《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》。

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控制和自动化标准化技术委员会(SAC/TC 124)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、北京国电智深控制技术有限公司、中国安全生产科学研究院、上海工业自动化仪表研究院、杭州和利时自动化有限公司、欧姆龙自动化(中国)有限公司、西门子(中国)有限公司、上海中沪电子有限公司。

本部分主要起草人：冯晓升、熊文泽、潘钢、史学玲、吴宗之、罗安、周有铮、杨柳、方来华、李佳嘉、李佳、郑威、张龙、王海清、孟邹清、梅豪。

本部分所代替标准的历次版本发布情况为：

——GB/T 20438.1—2006。

引　言

由电气和电子器件构成的系统，多年来在许多应用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）在其应用领域中用于执行非安全功能，并且也越来越多地用于执行安全功能。如果要安全并有效地使用计算机技术，有关决策者在安全方面有充足的指导并据此做出决定是十分必要的。

GB/T 20438 针对由电气和/或电子和/或可编程电子（E/E/PE）组件构成的、用来执行安全功能的系统安全生命周期的所有活动，提出了一个通用的方法。采用统一的方法的目的是为了针对所有以电为基础的安全相关系统提出一种一致的、合理的技术方针。主要目标是促进基于 GB/T 20438 系列标准的产品和应用领域国家标准的制定。

注 1：在参考文献中给出了基于 GB/T 20438 系列标准的产品和应用领域标准的例子（见参考文献[1]，[2]，[3]）。

在许多情况下，可用多种基于不同技术（如机械的、液压的、气动的、电气的、电子的、可编程电子的等）的系统来保证安全。因而必须考虑各类安全策略，不仅要考虑单个系统中的所有组件的问题（如传感器、控制器、执行器等），还要考虑不同安全相关系统组合后的问题。因此当 GB/T 20438 在关注电气/电子/可编程电子（E/E/PE）安全相关系统的同时，也提供了一个框架，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/PE 安全相关系统。对每个特定的应用，将根据特定应用的许多因素来确定所需的安全措施。GB/T 20438 作为基本原则可在未来的产品和应用领域国家标准制定和已有标准的修订中规范这些措施。

GB/T 20438

——考虑了当使用 E/E/PE 系统执行安全功能时，所涉及的整体安全生命周期、E/E/PE 系统安全生命周期以及软件安全生命周期的各阶段（如初始概念、整体设计、实现、运行和维护到退役）；

——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；

——使涉及 E/E/PE 安全相关系统的产品和应用领域的国家标准得以制定；在 GB/T 20438 的框架下，产品和应用领域的国家标准的制定在应用领域和交叉应用领域宜具有高度一致性（如基本原理，术语等）；这将既具有安全性又具有经济效益；

——为实现 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；

——采用了一种可确定安全完整性要求的基于风险的方法；

——引入安全完整性等级，用于规定 E/E/PE 安全相关系统所要执行的安全功能的目标安全完整性等级；

注 2：GB/T 20438 没有规定每个安全功能的安全完整性等级的要求，也没有规定如何确定安全完整性等级。而是提供了一种基于风险概念的框架和技术范例。

——建立了 E/E/PE 安全相关系统执行安全功能的目标失效量，这些量都同安全完整性等级相联系；

——建立了单一 E/E/PE 安全相关系统执行安全功能时，目标失效量的一个下限值。这些 E/E/PE 安全相关系统运行在：

——低要求运行模式下，下限设定成要求时危险失效平均概率为 10^{-5}；

——高要求运行模式或者连续运行模式下，下限设定成危险失效平均频率为 10^{-9}/h。

注 3：单一 E/E/PE 安全相关系统不一定是单通道架构。

注 4：对于非复杂系统，通过安全相关系统的设计实现更优目标安全完整性是可能的。但对于相对复杂的系统（例如可编程电子安全相关系统），这些限值代表了目前能够达到的水平。

——基于工业实践中获取的经验和判断，设定了避免和控制系统性故障的要求。即使发生系统性故障的可能性一般不能量化，但 GB/T 20438 允许为一个特定的安全功能做出声明，即如果标准中的所有要求都满足，认为与安全功能相关的目标失效量已达到；

——引入了系统性能力，该能力表明一个组件为满足规定的安全完整性等级要求时，系统性安全完整性的置信度；

——采用多种原理、技术和措施以实现 E/E/PE 安全相关系统的功能安全，但没有明确地使用失效-安全的概念。然而，如果能够满足标准中相关条款的要求，则“失效-安全”的概念和“本质安全”原则可能被应用，并且采用这些概念是可接受的。

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的主要目的是促进负责产品或应用领域的技术委员会制定产品和应用领域国家标准。这将允许充分考虑与产品或应用相关的所有因素,从而满足产品和应用领域用户的特定需要。GB/T 20438第二个目的是,在产品或应用领域没有国家标准的情况下能够开发E/E/PE安全相关系统。

1.2 GB/T 20438尤其:

a) 适用于包含有一个或几个电气/电子/可编程电子组件的安全相关系统;

注1:对于低复杂的E/E/PE安全相关系统,GB/T 20438规定的有些要求不是必要的,可以不符合(见4.2和GB/T 20438.4—2017的3.4.3中低复杂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—2017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有关人为因素的要求。

b) 是一个一般基础并适用于所有E/E/PE安全相关系统而无需考虑其具体应用;

c) 包括通过应用E/E/PE安全相关系统达到可容忍风险,但不包含E/E/PE设备自身出现的危险(如电击);

d) 可应用于所有类型的E/E/PE安全相关系统,包括保护系统和控制系统;

e) 不包括在下列情况时的E/E/PE系统:

——能够靠其自身能力满足可容忍风险的单一E/E/PE系统,并且

——该单一E/E/PE系统安全功能要求的安全完整性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)。

f) 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可用来规范任何用于保护设备和产品的E/E/PE系统;

注3:见GB/T 20438.4—2017的3.1.1。

g) 考虑了E/E/PE安全相关系统和其他风险降低措施,以便能系统性的、以基于风险的方式确定E/E/PE安全相关系统的安全要求规范;

h) 用整体安全生命周期模型作为技术框架,以便系统性地处理为确保E/E/PE安全相关系统功能安全所必需的活动;

注4:尽管整体安全生命周期首先是针对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)。

i) 不对各领域应用规定要求的安全完整性等级(这需要以该领域应用的详细信息和知识为基础),适合的安全完整性等级由负责制定各应用领域标准的技术委员会在行业应用标准中规定;

j) 对于尚无标准的各产品和应用领域提供E/E/PE安全相关系统的通用要求;

k) 需要在风险和危险分析时考虑恶意的和非授权的行为。分析范围包括所有相关的安全生命周期阶段;

注5:其他IEC/ISO标准对本条款有更详细的描写:参见ISO/IEC/TR 19791和IEC 62443系列标准。

l) 不包括防止未经批准人员损害E/E/PE安全相关系统的安全功能和/或对其产生不利影响的

预防措施;[见 k)]

m) 不规定需要满足 E/E/PE 安全相关系统要求的安保策略或安保服务的开发、实现、维护和/或运行的要求;

n) 不适用符合 IEC 60601 系列的医疗设备。

1.3 GB/T 20438 的本部分包含的一般要求适用于 GB/T 20438 的所有部分。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、更具体的要求;

——第 4 部分规定 GB/T 20438 中使用的术语定义和缩略语;

——第 5 部分用示例的方法,提供了第 1 部分应用中确定安全完整性等级的指南;

——第 6 部分提供了第 2 部分和第 3 部分的应用指南;

——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 和 GB/T 20438.4 是基础的安全标准,虽然它不适用于低复杂的 E/E/PE 安全相关系统(见 GB/T 20438.4—2017 的 3.4.3),但作为基础安全标准,各技术委员会可以在 IEC 指南 104 和 ISO/IEC 指南 51 的指导下制定相关标准时使用。GB/T 20438.1、GB/T 20438.2、GB/T 20438.3 和 GB/T 20438.4 也可作为独立标准来使用。GB/T 20438 的横向安全功能不适用于在 IEC 60601 系列指导下的医疗设备。

注:各技术委员会的责任之一,是在其标准的起草工作中尽可能使用基础的安全标准。在本部分中,本基础安全标准中的要求、测试方法或测试条件只有在这些技术委员会起草的标准中已明确引用或包含时适用。

1.5 图 1 表示了 GB/T 20438 的整体框架,同时明确了本部分在实现 E/E/PE 安全相关系统功能安全过程中的作用。

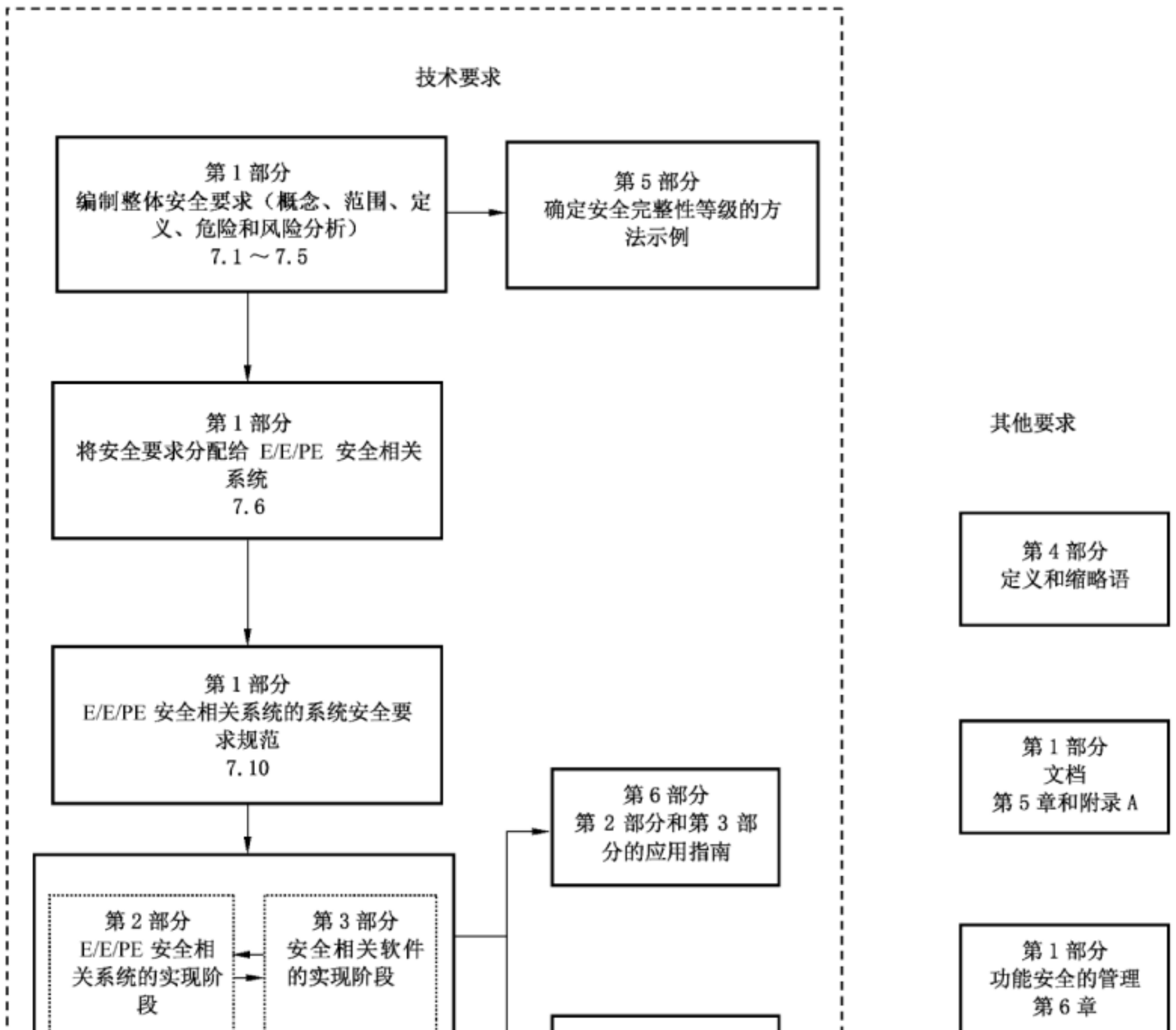


图 1　GB/T 20438 的整体框架

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20438.2—2017 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 61805-2:2010，IDT)

GB/T 20438.3—2017 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 61508-3:2010，IDT)

GB/T 20438.4—2017 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 61508-4:2010，IDT)

IEC Guide 104:1997 安全出版物的编写及基础安全出版物和多专业共用安全出版物的应用导则(The preparation of safety publications and the use of basic safety publications and group safety publications)

ISO/IEC Guide 51:1999 涉及安全的内容 将安全内容纳入标准的指南(Safety aspects—Guidelines for their inclusion in standards)

3 定义和缩略语

GB/T 20438.4—2017界定的定义和缩略语适用于本文件。

4 与GB/T 20438的符合性

4.1 要符合GB/T 20438，必须证明已满足了标准所有的相关要求(如安全完整性等级)，即已达到各章和各条的目的。

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。但对于低复杂的E/E/PE安全相关系统(见GB/T 20438.4—2017的3.4.3)，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：

——在有关应用和产品领域标准中实现GB/T 20438.1～GB/T 20438.7要求时，有些要求也许不必要，不符合这些要求是可接受的。

——如在有关产品或应用领域没有相应标准，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，不满足这些要求是可接受的。

4.3 按GB/T 20438框架制定的E/E/PE安全相关系统的产品或应用领域的国家标准，应考虑ISO/IEC指南51和IEC指南104的要求。

5 文档

5.1 目的

5.1.1 本章要求的第一个目的是规定必须进行归档的信息，这些信息是为了能够有效执行整体安全生命周期、E/E/PE系统安全生命周期和软件安全生命周期的各阶段。

5.1.2 本章要求的第二个目的是规定必须进行归档的信息，这些信息是为了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(见第 8 章)等活动。

注 1：本部分的归档要求从根本上讲是指信息，而不是实际的文档，这些信息不要求包括在实际的文档之中，除非在相关条款中有明确说明。

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：相关的文档结构见附录 A。

注 4：见参考文献中的引用文件[7]。

5.2 要求

5.2.1 对于整体以及 E/E/PE 系统和软件安全生命周期已完成的各个阶段，文档中应包括充分的信息。这些信息对于有效执行后续阶段和验证活动是必需的。

注：充分信息的构成取决于许多因素，包括 E/E/PE 安全相关系统的复杂程度和系统规模，以及具体应用的相关要求。

5.2.2 文档中应包括功能安全管理所需的足够信息(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充分信息，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 除非证明这些归档信息有效合理，或者在产品或应用领域标准中已规定，否则这些信息应同本部分各章中的规定相一致。

5.2.5 对于执行本部分相应条款的职责，文档应充分可用。

注：本部分要求的执行特定活动所需的信息，需要由各相关方掌握。

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；

——可使用和可维护。

5.2.7 文档或信息集应有指示内容范围的标题或名称，以及一些检索排列的形式，以便准确访问标准要求的信息。

5.2.8 文档的结构可根据公司规程和产品或应用领域的工作习惯来确定。

5.2.9 文档或信息集应有修订索引(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 所有相关文档应在适当的文档控制方案下进行修订、补充、复审、批准。

注：当用自动或半自动的工具生成文档时，在版本的管理或文档的其他控制方面，为了确保措施的有效性，专用规程也许是必要的。

6 功能安全管理

6.1 目的

6.1.1 本章要求的第一个目的是对 E/E/PE 安全相关系统或者对完整的 E/E/PE 系统和软件安全生命周期的一个或多个阶段的责任方确定功能安全管理的职责。

6.1.2 本章要求的第二个目的是在功能安全管理中确定由责任方执行的具体活动。

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实现和保持 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，将被规定作为 E/E/PE 安全相关系统及其元器件和组件的供货商提供信息的一部分。

6.2 要求

6.2.1 负责一个 E/E/PE 安全相关系统，或整体安全生命周期、E/E/PE 系统安全生命周期或软件安全生命周期一个或多个阶段的组织，应指派一个或多个人员承担下列全部责任：

——系统及其生命周期阶段；

——协调在这些阶段需执行的安全相关活动；

——这些阶段和由其他组织执行的其他阶段之间的接口；

——执行 6.2.2～6.2.11 和 6.2.13 的要求；

——协调功能安全评估[见 6.2.12b)和第 8 章]，尤其是在不同阶段，由不同的评估方执行功能安全评估的情况下，包括沟通、计划、集成文档、评价和建议；

——保证功能安全的实现和论证与本部分的目的和要求相一致。

注：对于安全相关活动或安全生命周期阶段的责任，可以委派他人，特别是那些相关的专家，使不同的人员对不同的活动和要求负责。然而，对协调的责任和对整体功能安全的责任，建议固定一个或少数人员，对其进行充分的管理授权。

6.2.2 应规定实现功能安全的方针和策略，包括评估它们实现的方法和在组织内交流的方法。

6.2.3 应识别出所有人员、部门和组织在适当的整体安全生命周期、E/E/PE 系统安全生命周期或软件安全生命周期阶段实施活动的责任(包括验证和功能安全评估的人员责任，以及应由相关的许可授权或法定的安全机构所负的责任)，并将这些责任完全的和清楚的告知责任方。

6.2.4 应制定规程以规定相关各方需交流何种信息以及如何交流。

注：见第 5 章的文档要求。

6.2.5 应制定规程以保证对 E/E/PE 安全相关系统的相关建议能迅速跟进和满意解决，建议包括来自：

a) 危险和风险分析(见 7.4)；

b) 功能安全评估(见第 8 章)；

c) 验证活动(见 7.18)；

d) 确认活动(见 7.8 和 7.14)；

e) 配置管理(见 6.2.10、7.16、GB/T 20438.2 和 GB/T 20438.3)；

f) 事故报告和分析(见 6.2.6)。

6.2.6 应制定规程以保证对所有检测到的危险事件开展分析，并提出建议以将其重复发生的可能性降到最低。

6.2.7 应规定周期性功能安全审核的要求，包括：

a) 功能安全审核的频率；

b) 执行这些审核的独立性水平；

c) 必要的文档和后续活动。

6.2.8 应在如下方面制定规程：

a) 发起对 E/E/PE 安全相关系统修改(见 7.16.2.2)；

b) 获得修改的批准和授权。

6.2.9 应制定规程以保持对危险和危险事件、安全功能和 E/E/PE 安全相关系统信息的准确性。

6.2.10 应在整体安全生命周期、E/E/PE 系统安全生命周期和软件安全生命周期阶段中制定 E/E/PE 安全相关系统配置管理的规程，特别是：

a) 对于特定的阶段，将执行正式配置的控制节点；

b) 用来唯一识别某项（硬件和软件）所有构成部分的规程；

c) 阻止非授权项进入服务的规程。

6.2.11 在特定的场合中，应提供应急服务的培训和信息。

6.2.12 那些负责一个或多个整体安全生命周期、E/E/PE 系统安全生命周期和软件安全生命周期阶段的责任方，应就那些他们负有责任的阶段和按照 6.2.1～6.2.11 所定义的规程，规定所有的管理和技术活动，这些活动对于保证 E/E/PE 安全相关系统功能安全的实现、证明和维护是必要的，包括：

a) 用来满足特定章条或条款要求而选择的措施和技术（见 GB/T 20438.2、GB/T 20438.3 和 GB/T 20438.6）；

b) 功能安全评估活动和将功能安全实现证明给那些执行功能安全评估人员的方法（见第 8 章）；

注：宜使用适当的功能安全评估规程来定义：

——适当的独立性水平下，对适当组织、角色和人员的选择；

——拟定和变更功能安全评估人员的职权范围；

——在系统安全生命周期的任一节点执行功能安全评估人员的变化；

——执行功能安全评估的人员之间存在的争议的解决方法。

c) 分析运行和维护性能的规程，特别是在：

——识别可能导致功能安全丧失的系统性故障，包括在例行维护中用来检测反复故障的规程；

——评估在运行和维护过程中，要求率和失效率是否符合系统设计过程中所做的假设。

6.2.13 应制定相应的规程，以保证 6.2.1 和 6.2.3 定义的所有负责人员（包括任何整体生命周期、E/E/PE 系统生命周期和软件生命周期活动的所有人员，包括验证、功能安全管理和功能安全评估的活动）有适当的能力（即培训、技术知识、经验和资质）执行其规定任务。这些规程应包括对能力的恢复、更新和持续评估的要求。

6.2.14 应根据特定的应用考虑能力的适宜性，需考虑的所有相关因素包括：

a) 人员的责任；

b) 要求的监督等级；

c) E/E/PE 安全相关系统失效事件的潜在后果——后果越严重，对能力（权限）的规范就越严格；

d) E/E/PE 安全相关系统的安全完整性等级——安全完整性越高，对能力的规范就越严格；

e) 设计、设计规程或应用的新颖性——越新颖或越未经使用，对能力的规范就越严格；

f) 之前的经验及其与待执行规定职责和采用技术的相关性——要求的能力越高，通过之前经验获得的能力和将实施特定活动的要求之间的符合性差距越小；

g) 适用于该环境的能力类型（例如：资质、经验、相关培训和后续实践，以及领导能力和决断能力）；

h) 适用于应用领域和该技术的工程知识；

i) 适用于该技术的安全工程知识；

j) 法律和安全规章框架的知识；

k) 对执行特定活动资格的相关性。

注：在参考文献[8]中包括了一个管理 E/E/PE 安全相关系统能力的示例方法。

6.2.15 根据 6.2.1 和 6.2.3 定义的所有负责人员的能力应文档化。

6.2.16 应执行并监视由 6.2.2～6.2.15 规定的活动。

6.2.17 对整体安全生命周期、E/E/PE 系统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责的组织提供产品或服务的供应商，应该提供该组织规定的产品或服务并有一个适当的质量

管理体系。

6.2.18 与功能安全管理相关的活动应适用于整体安全生命周期、E/E/PE 系统安全生命周期和软件安全生命周期的相关阶段(见 7.1.1.5)。

7 整体安全生命周期的要求

7.1 概述

7.1.1 简介

7.1.1.1 为了以系统性方式处理所有的活动,这些活动是为使 E/E/PE 安全相关系统执行的安全功能实现要求的安全完整性等级所必须的,本部分采用了一种整体安全生命周期的技术框架(见图 2)。

注:整体安全生命周期宜作为声明符合本部分的一个基础,但如果本部分各章的目的和要求都满足,也可使用不同于图 2 的整体安全生命周期。

7.1.1.2 整体安全生命周期包含下列达到可容忍风险的方法:

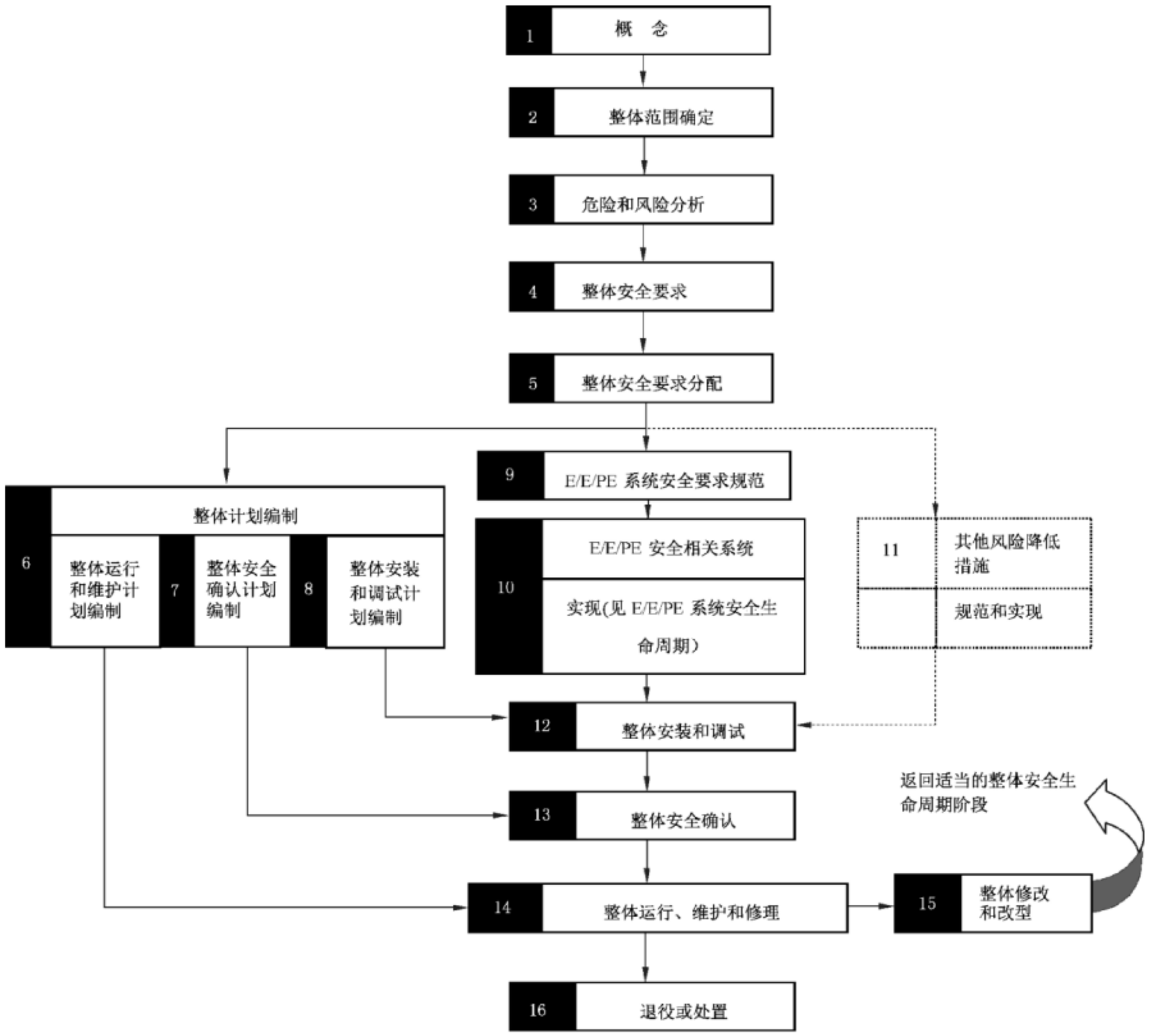
——E/E/PE 安全相关系统;

——其他风险降低措施。

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。E/E/PE 系统安全生命周期部分构成了 GB/T 20438.2 的技术框架。图 4 显示了软件安全生命周期部分并构成了 GB/T 20438.3 的技术框架。图 5 显示了安全相关系统的整体安全生命周期与 E/E/PE 系统安全生命周期和软件安全生命周期之间的关系。

7.1.1.4 整体的、E/E/PE 系统的和软件的安全生命周期图(图 2~图 4)仅是实际情况的一个简化图,并未显示特定阶段或阶段间的反复过程,然而通过整体的、E/E/PE 系统的和软件的安全生命周期进行开发,这种反复是必要的并且是至关重要的。

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



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/PE 系统的和软件的安全生命周期各阶段有关。

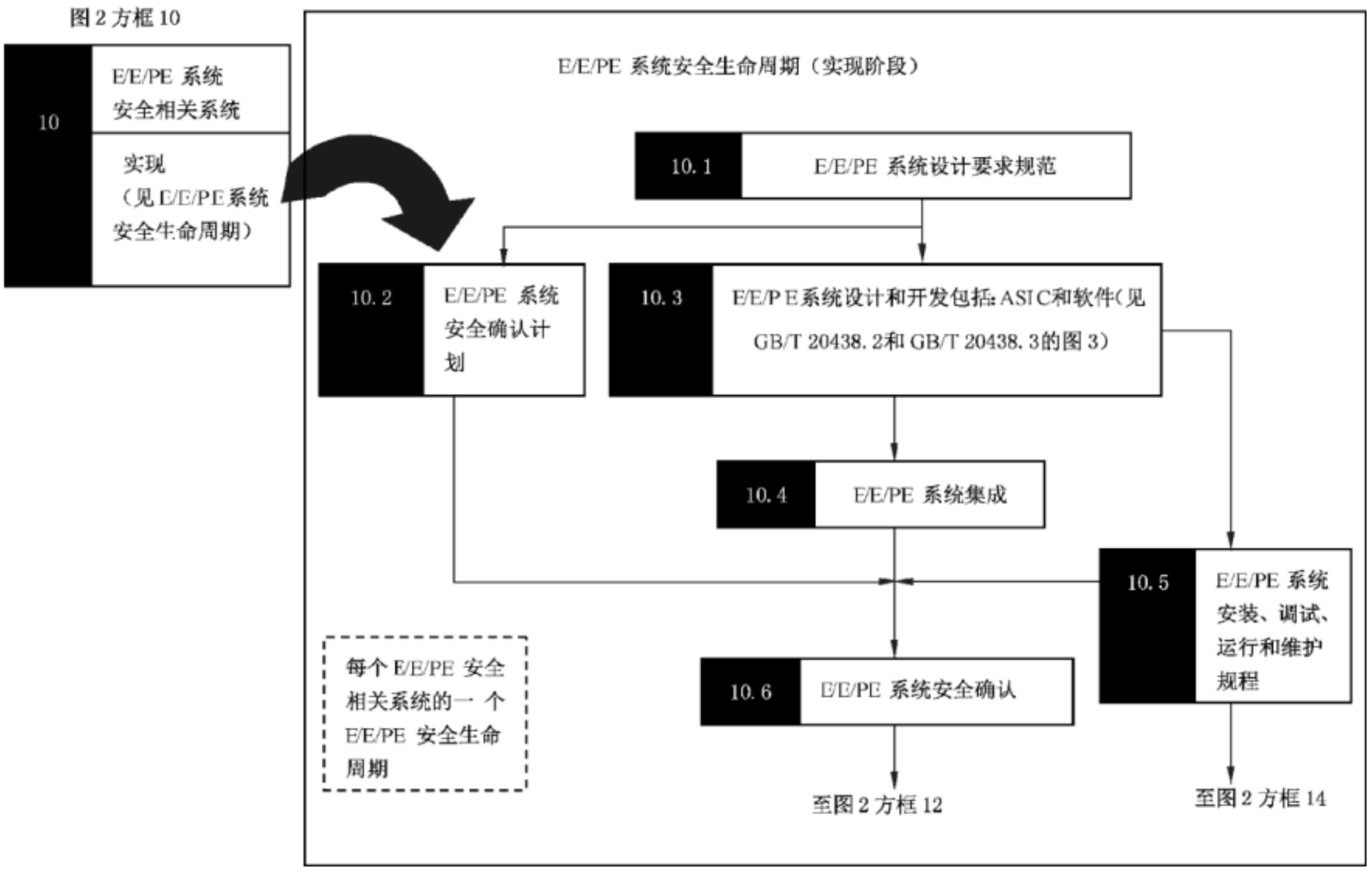
注 2：方框 11 所表示的阶段不在 GB/T 20438 范围之内。

注 3：GB/T 20438.2 和 GB/T 20438.3 涉及方框 10(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)。

注 4：各方框代表的每个阶段的目标和范围的描述见表 1。

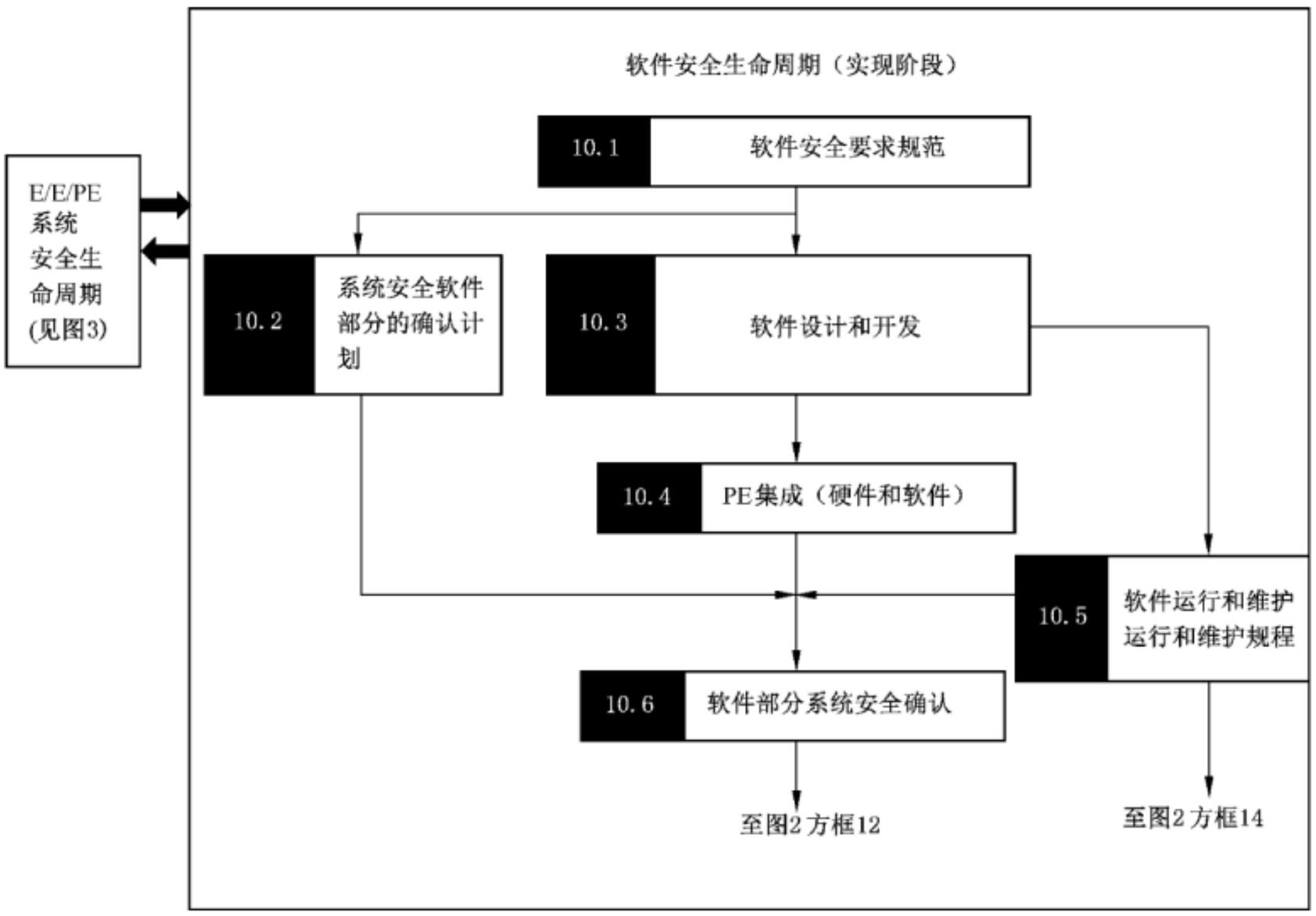
注 5：对整体运行、维护、修理、修改、改型和退役或处置所需的技术要求，将被规定作为 E/E/PE 安全相关系统和其组件和元器件供应商提供信息的一部分。

图 2　整体安全生命周期



注：本图仅表示在整体安全生命周期实现阶段中的E/E/PE系统安全生命周期部分。完整的E/E/PE系统安全生命周期，还包括整体安全生命周期后续阶段（见图2的方框12～方框16）中与E/E/PE安全相关系统相关的内容。

图3　E/E/PE系统安全生命周期（实现阶段）



注：本图仅表示在整体安全生命周期实现阶段中的软件安全生命周期部分。完整的软件安全生命周期，还包括整体安全生命周期后续阶段(见图 2 的方框 12～方框 16)中与 E/E/PE 安全相关系统软件相关的内容。

图 4　软件安全生命周期(实现阶段)

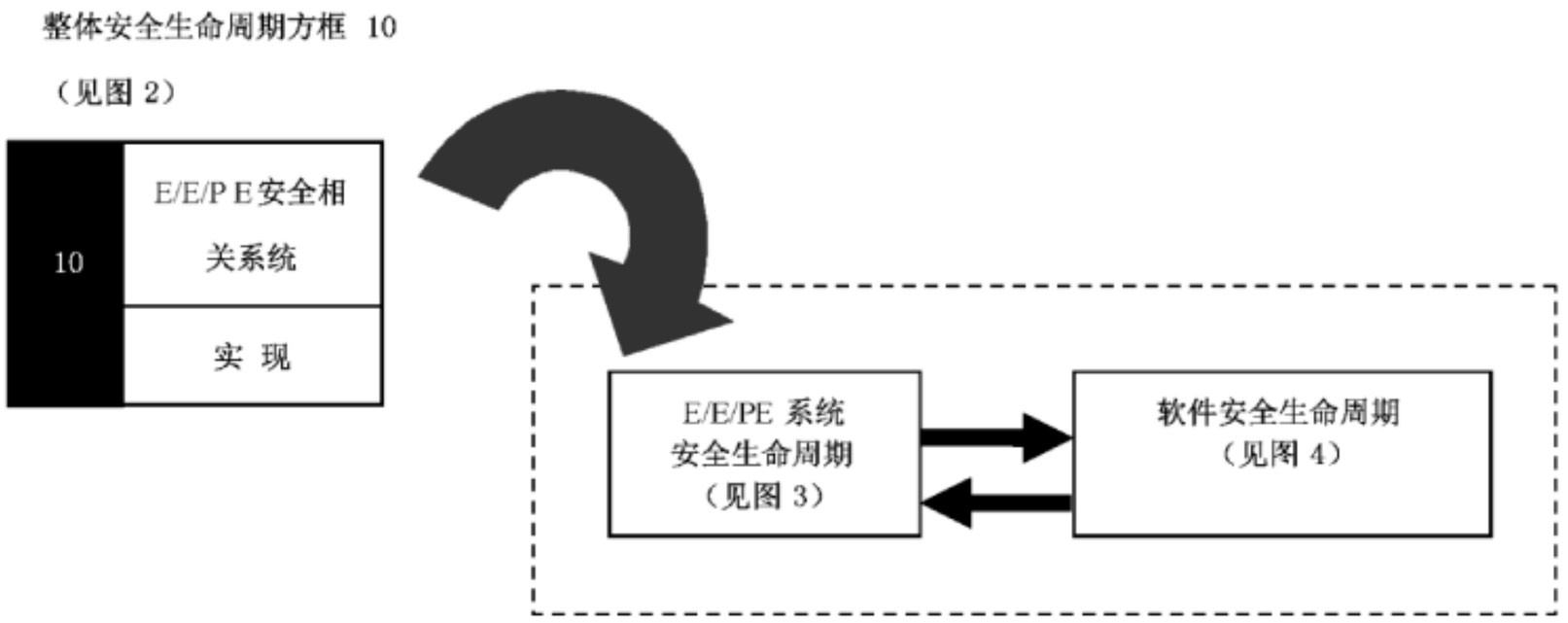


图 5　整体安全生命周期与 E/E/PE 系统安全生命周期和软件安全生命周期之间的关系

7.1.2　目的与要求:概述

7.1.2.1　从 7.2～7.17 规定了整体安全生命周期各阶段的目的与要求。在 GB/T 20438.2 和 GB/T 20438.3中分别给出了 E/E/PE 系统及软件安全生命周期阶段的目的和要求。

注：7.2～7.17 对应于图 2 的特定方框(阶段)，这些条的注中参考了这些特定的方框。

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相关信息	与 EUC 及其环境和危险相关的信息
2	整体范围确定	7.3.1： 确定 EUC 和 EUC 控制系统的范围； 规定危险与风险分析的范围（如过程危险、环境危险等）	EUC 及其环境	7.3.2	与 EUC、及其环境和危险相关的信息	已确定的危险和风险分析范围
3	危险和风险分析	7.4.1： 对包括故障状况和合理可预见的误用（见 GB/T 20438.4—2017 的 3.1.14）在内的所有合理的可预见的情况，确定 EUC 和 EUC 控制系统（所有运行模式下）的危险、危险事件和相关的危险状况； 确定导致危险事件的事件顺序； 确定伴随危险事件的 EUC 风险	范围与涉及的整体的、E/E/PE 系统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与风险分析）。 初始危险与风险分析的范围将由整体范围确定的输出决定	7.4.2	已确定的危险和风险分析范围	危险与风险分析的描述以及相关的信息
4	整体安全要求	7.5.1： 为实现所需的功能安全，根据安全功能要求和安全完整性要求为 E/E/PE 安全相关系统和其他风险降低措施编制整体安全要求规范	由整体范围确定的输出决定	7.5.2	危险与风险分析的描述及相关的信息	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

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					
5	整体安全要求分配	7.6.1： 为指定的 E/E/PE 安全相关系统和其他风险降低措施分配安全功能，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； 给每个由 E/E/PE 安全相关系统执行的安全功能分配安全完整性等级	由整体范围确定的输出决定	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	整体安全功能分配的信息，它们的目标失效量及相应安全完整性等级。 需要在 EUC 整个生命周期中管理的其他风险降低措施的假设（见 7.6.2.13）
6	整体运行和维护计划编制	7.7.1： 拟定 E/E/PE 安全相关系统的运行和维护计划，以确保在运行和维护过程中保持所需的功能安全	EUC、EUC 控制系统和人的因素； E/E/PE 安全相关系统	7.7.2	整体安全功能分配的信息，它们的目标失效量及相应安全完整性等级。 需要在 EUC 整个生命周期中管理的其他风险降低措施的假设（见 7.6.2.13）	E/E/PE 安全相关系统运行和维护计划
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	整体安全要求分配的信息和结果	E/E/PE 安全相关系统的整体安全确认计划
8	整体安装和调试计划编制	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，以保证实现所需的功能安全；拟定受控方式下的 E/E/PE 安全相关系统的调试计划，以保证实现所需的功能安全	EUC 和 EUC 控制系统； E/E/PE 安全相关系统	7.9.2	整体安全要求分配的信息和结果	E/E/PE 安全相关系统安装计划； E/E/PE 安全相关系统调试计划
9	E/E/PE 系统安全要求规范	7.10.1： 定义 E/E/PE 系统安全要求，包括 E/E/PE 系统安全功能要求和 E/E/PE 系统安全完整性要求，以实现所需的功能安全	E/E/PE 安全相关系统	7.10.2	整体安全要求分配的信息和结果	E/E/PE 系统安全要求规范

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					
10	E/E/PE 安全相关系统：实现	7.11.1 和第 2、第 3 部分：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	7.11.2 GB/T 20438.2 和 GB/T 20438.3	E/E/PE 系统安全要求规范	根据 E/E/PE 系统安全要求规范，实现每个 E/E/PE 安全相关系统
11	其他风险降低措施：规范和实现	7.12.1： 建立其他风险降低措施，满足为该系统规定的安全功能要求和安全完整性要求（此内容不在本部分范围之内）	其他风险降低措施	7.12.2	其他风险降低措施安全要求规范（不在本部分范围之内，并且本部分后续内容也不涉及此内容）	根据对其他措施的安全要求实现其他风险降低措施
12	整体安装和调试	7.13.1： 安装 E/E/PE 安全相关系统； 调试 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； 调试 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； 经充分调试过的 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； 整体安全要求分配的相关信息和结果	考虑 E/E/PE 安全相关系统的安全要求分配结果，确认所有 E/E/PE 安全相关系统满足整体安全要求规范
14	整体运行、维护和修理	7.15.1： 确保 E/E/PE 安全相关系统维持在规定的安全等级； 确保整体运行、维护和修理 E/E/PE 相关系统所需要的技术要求已规定，并提供给未来负责 E/E/PE 安全相关系统的运行和维护人员	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运行和维护计划	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 安全相关系统的运行、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： 规定必要的规程以确保在修改和改型阶段中和阶段后，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 安全相关系统的修改和改型文档
16	退役或处置	7.17.1： 在 EUC 的退役或处置活动中及活动后，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，对退役或处置的请求	在退役或处置活动中及活动后，均可实现 E/E/PE 安全相关系统要求的功能安全； 按时间排序的退役或处置活动的文档

7.1.3 目的

7.1.3.1 7.1 的首要目的是用一种系统性的方式构造整体安全生命周期中的各个阶段，以实现 E/E/PE 安全相关系统要求的功能安全。

7.1.3.2 7.1 的第二个目的是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归档的信息化。

注：文档要求和文档结构示例分别见第 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本部分的符合性。如使用其他的整体安全生命周期，应在功能安全计划编制（见第 6 章）过程中规定，并应满足本部分各章条的目的和要求。

注：形成整体安全生命周期实现阶段的 E/E/PE 系统安全生命周期和软件安全生命周期部分，分别由GB/T 20438.2 和 GB/T 20438.3 规定。

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同时进行。

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。除非作为功能安全活动管理（见第 6 章）的

一部分已做调整或在产品和应用领域标准中另有规定。

7.1.4.6 每个整体安全生命周期阶段的输出见表1。除非作为功能安全活动管理(见第6章)的一部分已做调整或在产品和应用领域标准中另有规定。

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7.18中规定的每个整体安全生命周期阶段的验证要求。

7.2 概念

注:这个阶段是图2的方框1。

7.2.1 目的

7.2的目的是提高对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 全面彻底熟悉EUC及其要求的控制功能和实际环境。

7.2.2.2 确定可能的危险源、危险状况和伤害事件。

7.2.2.3 获取已确定危险的信息(例如:持续时间、强度、毒性、暴露限度、机械力、爆炸条件、反应性、易燃性等)。

7.2.2.4 获取当前的安全法规(国际的和国内的)。

7.2.2.5 应同时考虑EUC与其他设备或系统(已安装的或将被安装的)以及与其他EUC(已安装的或将被安装的)之间相互作用所产生的危险、危险状况和伤害事件。

7.2.2.6 7.2.2.1～7.2.2.5所要求的信息和结果应归档。

7.3 整体范围确定

注:这个阶段是图2的方框2。

7.3.1 目的

7.3.1.1 7.3的首要目的是确定EUC和EUC控制系统的范围。

7.3.1.2 7.3的第二个目的是规定危险与风险分析的范围(如过程危险、环境危险等)。

7.3.2 要求

7.3.2.1 应确定EUC和EUC控制系统的范围,包括所有与危险和危险事件相关的设备和系统(包含所有相关人员)。

注:可能需要在整体范围确定与危险和风险分析间进行多次反复。

7.3.2.2 应确定危险与风险分析范围内所有的实际设备,包括EUC和EUC控制系统。

注:见参考文献[9]和[10]。

7.3.2.3 应确定在危险与风险分析中应考虑的外部事件。

7.3.2.4 应确定与危险、危险事件相关的设备及系统。

7.3.2.5 应确定需要考虑的引发事故的事件类型(如元器件失效、程序故障、人为错误,以及能导致危险事件发生的相关失效机制)。

7.3.2.6 7.3.2.1～7.3.2.5所需的信息和结果应归档。

7.4 危险与风险分析

注:这个阶段是图2的方框3。

7.4.1 目的

7.4.1.1 7.4 的第一个目的是对于所有合理可预见的情况(见 GB/T 20438.4—2017 的 3.1.14),包括故障状况和合理可预见的误用,确定与 EUC 和 EUC 控制系统相关的危险、危险状况和危险事件(在所有运行模式下)。

7.4.1.2 7.4 的第二个目的是确定导致 7.4.1.1 所确定的危险事件的事件顺序。

7.4.1.3 7.4 的第三个目的是确定与 7.4.1.1 确定的危险事件相关的 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性风险分析的基础上,7.4 是必需的。除非将 EUC 和 EUC 控制系统考虑在内,否则这些将无法完成。

注 2:在可对危险事件及其后果进行有效假设的应用领域中,7.4(和 7.5)中所需的分析可由 GB/T 20438 应用领域版本的编制者完成,并可把这些分析嵌入到简化的图解要求之中。示例见 GB/T 20438.5—2017 的附录 E 和附录 G。

7.4.2 要求

7.4.2.1 应进行危险与风险分析,分析时应考虑整体范围确定阶段中的信息(见 7.3)。如在整体安全生命周期、E/E/PE 系统安全生命周期和软件安全生命周期的后期做出的决定,可能改变前期所作决定的基础,此时应进行进一步的危险与风险分析。

注 1:指南见参考文献[9]和[10]。

注 2: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持续危害与风险分析的例子。危险与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,它将导致新的危险事件顺序。

7.4.2.2 应该考虑如何消除或降低危险。

注:尽管不包括在 GB/T 20438 范围内,但在源头消除 EUC 中已辨识的危险是非常重要的,如应用固有安全原则,以及应用优秀工程实践经验。

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、危险事件及危险状况(包括故障条件、合理可预见的误用和恶意或未经授权的行为)。还包括所有相关的人为因素引起的问题,尤其应注意那些不常见的、异常的 EUC 运行模式。如果危险分析识别到合理可预见的恶意的或未经批准的行动构成了安保威胁,应开展安保威胁分析。

注 1:对于合理可预见的误用,见 GB/T 20438.4—2017 的 3.1.14。

注 2:关于危险识别包括描述和分析人为因素事件的指导见参考文献[11]。

注 3:安保风险分析见 IEC 62443 系列。

注 4:恶意或未授权的行为包含了安保威胁。

注 5:危险与风险分析宜考虑因某个要求或误动作而启动一个安全功能是否会产生新的危险,若有,则可能需要开发一个新的安全功能来处理这个危险。

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 1:事件顺序宜参考安全方针和风险管理决策。

注 2:通常会考虑用修改过程设计或所用设备的方法消除事件顺序。

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。

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与风险分析技术满足 7.4.2.1～7.4.2.7 的要求(见 GB/T 20438.5)。

7.4.2.9 技术选用的合理性及其使用范围取决于很多因素,包括:

——特定的危险及后果;

——EUC 及 EUC 控制系统的复杂性;

——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；

——作为危险与风险分析依据的准确数据的可用性。

7.4.2.10 危险与风险分析应考虑的因素如下：

——每个确定的危险事件和产生危险的元器件；

——伴随每个危险事件的事件顺序的后果和可能性；

——每个危险事件的可容忍风险；

——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。应详细说明运行约束或人为介入的可信度。

7.4.2.11 构成危险与风险分析的信息和结果应归档。

7.4.2.12 对 EUC 和 EUC 控制系统而言，从危险与风险分析阶段至退役或处置阶段的整个整体安全生命周期全过程中，都应保存构成危险与风险分析的信息和结果。

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

7.5 整体安全要求

注：这个阶段是图 2 的方框 4。

7.5.1 目的

7.5 的目的是为实现所需的功能安全，根据整体安全功能要求和整体安全完整性要求，为 E/E/PE 安全相关系统和其他风险降低措施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 准应用领域版本的编制者按照 7.5(和 7.4)进行分析，并可把这些分析嵌入简化的图解要求之中，示例见 GB/T 20438.5—2017 的附录 E 和附录 F。

7.5.2 要求

7.5.2.1 基于危险与风险分析所得出的危险事件制定所需要的整体安全功能。这些安全功能构成了整体安全功能要求规范。

注 1：应该为每一个危险事件建立整体安全功能。

注 2：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。

示例：防止容器 X 温度超过 250 ℃和防止马达 Y 转速超过 3 000 r/min 是整体安全功能的实例。

7.5.2.2 如果已经识别出安保威胁，则为了详细确定安保要求应进行脆弱性分析。

注：在 IEC 62443 中已经给出指南。

7.5.2.3 对于每个安全功能，应确定其目标安全完整性要求以满足可容忍风险。要求可通过定量或定性的方法得到。这些将构成整体安全完整性要求规范。

注 1：整体安全完整性要求规范，是确定目标失效量和确定 E/E/PE 安全相关系统实施的安全功能的安全完整性等级的中间阶段。一些用于确定安全完整性等级的定性方法(见 GB/T 20438.5—2017 的附录 E 和附录 F)直接将风险参数转换为安全完整性等级。在这种情况下，安全完整性要求是隐含的而不是明确表述的，它们包含在方法本身之中。

注 2：可以通过减轻危险事件的后果(这是首选)或者减少 EUC 和 EUC 控制系统的危险事件发生率来降低 EUC 风险(见下文 7.5.2.4)。

注 3：可通过附加措施来减少危险事件发生的频率以达到要求，这些措施包括 E/E/PE 安全相关系统和/或其他风险降低措施。其他风险降低措施包括其他技术的安全相关系统或管理措施如逃生、阻隔或暴露时间。

注 4：为了达到可容忍风险，在确定每个安全功能的目标安全完整性时，考虑个体可能暴露于来自其他危险源的风

险，可能是有必要的。

注 5：对于某些应用领域，如果存在相关的国家标准，且标准中提供合适的方法能够直接确定安全完整性要求，可用这个标准来满足 7.5 的要求。

7.5.2.4 整体安全完整性要求应根据以下两者之一来确定：

——为达到可容忍风险所必须的风险降低；

——为达到可容忍风险所必须的可容忍危险事件发生率。

7.5.2.5 如果在评估 EUC 风险时，声明单个 EUC 控制系统功能的危险失效平均频率低于 10^{-5}/h，则此 EUC 控制系统就应被看作是安全相关控制系统，且需服从于 GB/T 20438 的相关要求。

注：例如，如果 EUC 控制系统声明的失效率在 10^{-6}/h 和 10^{-5}/h 之间，则该 EUC 控制系统被视为 E/E/PE 安全相关系统，且需满足安全完整性等级 1 的相关要求。

7.5.2.6 EUC 控制系统的失效对一个或多个 E/E/PE 安全相关系统和/或其他风险降低措施提出要求时，以及不想把 EUC 控制系统指定为一个安全相关系统时，应满足下列要求：

a) 对 EUC 控制系统声明的危险失效率应通过下列渠道获得数据的支持：

——在相似应用领域中，EUC 控制系统的实际运行经验；

——对认可的规程进行可靠性分析；

——同类设备的可靠性工业数据库。

b) EUC 控制系统声明的危险失效率应不低于 10^{-5}/h；

注 1：见 7.5.2.5。

c) 在制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 安全相关系统和其他风险降低措施。

注 2：如果安全相关系统已设计成具有足够安全完整性，并考虑了 EUC 控制系统的正常要求率，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，如声明的失效率小于安全完整性等级 1(见表 3)中的目标安全完整性上限时，控制系统将变成安全相关系统，并且将使用 GB/T 20438 中的要求。

注 3："独立"的含义见 7.6.2.7。

7.5.2.7 如果不能满足 7.5.2.6 a)～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 控制系统所声明的危险失效率，它与表 3 中的规定相符(见 7.6.2.9 注 3)。在这种情况下，本部分中与分配的安全完整性等级有关的要求适用于 EUC 控制系统。

注：另见 7.5.2.5 和 7.6.2.10。

7.6 整体安全要求分配

注：这个阶段是图 2 的方框 5。

7.6.1 目的

7.6.1.1 7.6 的第一个目的是为指定的 E/E/PE 安全相关系统和其他风险降低措施分配整体安全功能，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：有必要考虑其他风险降低措施，因为若不考虑其他风险降低措施，则对 E/E/PE 安全相关系统的分配就无法完成。

7.6.1.2 7.6 的第二个目的是对 E/E/PE 安全相关系统的每个安全功能分配目标失效量和安全完整性等级。

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，应通过以下途径达到可容忍风险：

——E/E/PE 安全相关系统；和/或

——其他风险降低措施。

注：本部分仅适用于至少部分可容忍风险的实现由 E/E/PE 安全相关系统完成的情况。

7.6.2.2 在给 E/E/PE 安全相关系统和其他风险降低措施分配整体安全功能时，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，从规范到维护和运行的所有阶段都要求高等级的能力。而用其他低复杂技术的解决方案可能有同等效果，还会因降低了复杂性而带来一些好处。

注 2：在实际运行中，运行、维护的可用技能和资源以及运行环境，对于所要实现的功能安全可能是关键的。

7.6.2.3 把按 7.5 建立的每个整体安全功能及其相应的整体安全完整性要求分配给一个或多个指定的 E/E/PE 安全相关系统和/或其他风险降低措施，以达到安全功能可容忍的风险。这种分配要重复进行，如果发现不能达到可容忍风险则应修改 EUC 控制系统规范、指定的 E/E/PE 安全相关系统和其他风险降低措施并进行重新分配。

注 1：分配一个具体的整体安全功能给一个或多个 E/E/PE 安全相关系统或其他风险降低措施取决于多种因素，但主要取决于整体安全完整性要求。安全完整性要求越高，这个功能越可能被多个 E/E/PE 安全相关系统和/或其他风险降低措施所承担。

注 2：图 6 给出了整体安全要求分配的方法。

7.6.2.4 7.6.2.3 所述的分配应分配所有的整体安全功能并为每一个安全功能定义目标失效量(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根据以下之一进行规定：

——低要求运行模式时，安全功能的危险失效平均概率，或

——高要求或连续运行模式时，安全功能的危险失效平均频率[h^{-1}]。

7.6.2.6 安全完整性要求的分配可使用适当的技术通过概率的组合来实现。

注 1：可用定量和/或定性的方法进行安全要求分配。

注 2：当需要多个 E/E/PE 安全相关系统和/或其他风险降低措施来达到可容忍风险时，实际的风险将取决于 E/E/PE 安全相关系统和/或其他风险降低措施之间的系统的相关性(见 GB/T 20438.5—2017 中 A.5.4 中相关性的详细说明以及分析方法)。

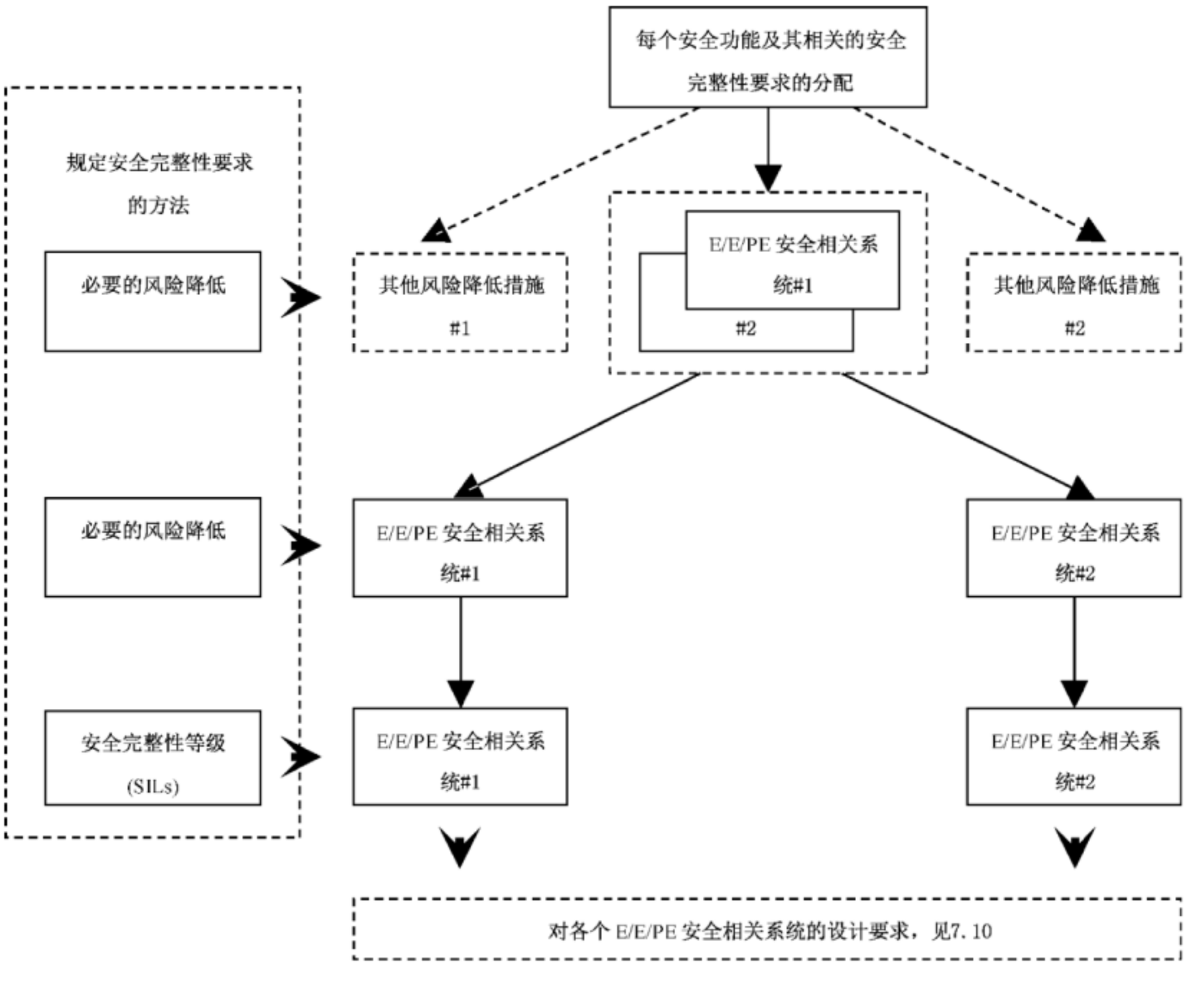


图 6　E/E/PE 安全相关系统和其他风险降低措施的整体安全要求分配图

7.6.2.7　进行分配时应考虑共因失效的概率。如果 EUC 控制系统、E/E/PE 安全相关系统和其他风险降低措施的(安全功能)分配实现了独立，则它们：

——是相互独立的，以致两个或两个以上这些不同系统或措施同时发生失效的可能性相对于要求的安全完整性足够低；

——是功能多样性的(即用完全不同的方法达到相同的结果)；

——是基于不同的技术的(即用不同类型的设备达到相同的结果)。

注 1：要认识到，尽管技术是多样性的，对失效发生时会产生严重后果的高安全完整性系统而言，应该采取特殊的预防措施来防止低概率的共同原因事件，例如飞机失事和地震。

——不能共用因其失效将引起所有系统产生危险失效模式的公共部件、服务或支持系统(如电源)；

——不能共用公共的运行、维护或测试规程。

注 2：本部分规定了如何实现分配给 E/E/PE 安全相关系统的安全要求，及规定的要求应如何完成。本部分没有详细规定如何实现分配给其他风险降低措施的安全要求。

在共因分析中，应当仔细检查 E/E/PE 安全相关系统实现中的限制和约束条件，例如 E/E/PE 系统、子系统或者组件不同通道间的必要隔离，如空间隔离。但这也许不能实现，如同一电路板上的双通道或双微处理器，或片上冗余(见 GB/T 20438.2—2017 的附录 E)。

7.6.2.8　如果不能全部满足 7.6.2.7 的所有要求，则 E/E/PE 安全相关系统和其他风险降低措施不能独立作为安全分配目标，分配应考虑 EUC 控制系统、E/E/PE 安全相关系统和其他风险降低措施之间的相关共因失效。

注 1：相关失效分析的更多信息见参考文献的[13]和[14]。

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。

注 3：如 7.6.2.3 所述，分配是重复进行的，如果当包含共因失效的分析表明基于最初假设无法满足可容忍风险时，设计需要改变(详细指导见 GB/T 20438.5—2017 的 A.5.4)。

7.6.2.9 当分配已充分进行后，分配给 E/E/PE 安全相关系统的每个安全功能的安全完整性要求应按表 2 或表 3 规定安全完整性等级，并且指明目标失效量是：

——低要求运行模式下(表 2)，安全功能的要求时危险失效平均概率，(PFD_{avg})，或

——高要求运行模式下(表 3)，安全功能的危险失效平均频率[h^{-1}]，(PFH)，或

——连续运行模式下(表 3)，安全功能的危险失效平均频率[h^{-1}]，(PFH)。

表 2 安全完整性等级：在低要求运行模式下安全功能的目标失效量

安全完整性等级 (SIL)	安全功能在要求时的危险失效平均概率 (PFD_{avg})
4	$\geqslant 10^{-5} \sim < 10^{-4}$
3	$\geqslant 10^{-4} \sim < 10^{-3}$
2	$\geqslant 10^{-3} \sim < 10^{-2}$
1	$\geqslant 10^{-2} \sim < 10^{-1}$

表 3 安全完整性等级：在高要求或连续运行模式下安全功能目标失效量

安全完整性等级 (SIL)	安全功能的每小时危险失效平均频率 (PFH)
4	$\geqslant 10^{-9} \sim < 10^{-8}$
3	$\geqslant 10^{-8} \sim < 10^{-7}$
2	$\geqslant 10^{-7} \sim < 10^{-6}$
1	$\geqslant 10^{-6} \sim < 10^{-5}$

注 1："低要求运行模式"、"高要求运行模式"和"连续运行模式"的具体含义见 GB/T 20438.4—2017 的 3.5.16。

注 2：目标失效量与危险和风险分析相关的运行模式的指导见 GB/T 20438.5。

注 3：表 2 与表 3 将分配给由 E/E/PE 安全相关系统执行的安全功能的目标失效量与安全完整性等级联系起来。普遍接受的事实是，不可能对 E/E/PE 安全相关系统所有方面的安全完整性都进行定量的预测。为保证目标失效量得以实现，必须考虑的预防措施不得不使用定性的技术、措施和判断。系统性安全完整性(见 GB/T 20438.4—2017 的 3.5.6)尤为如此，为达到规定的安全完整性等级所需的系统性安全完整性，在考虑必要的预防措施时，不得不采用相应的定性技术和判断[见 GB/T 20438.2—2017 中 7.4.2.2 c)、7.4.3、7.4.6、7.4.7 和 GB/T 20438.3]。

注 4：对于硬件安全完整性，为了评价由风险评估所确定的目标安全完整性是否已实现，有必要在考虑随机硬件失效(见 GB/T 20438.2—2017 的 7.4.5)的情况下，应用定量的可靠性评估技术。

注 5：当使用定性方法(如定性的风险图)确定安全完整性等级时，表 2 或表 3 可以给出合适的定量失效量为硬件安全完整性设定限值。

注 6：当使用两个或多个 E/E/PE 安全相关系统时，安全完整性可能优于表 2 提供的结果，前提是达到足够的独立等级，例如，当两个 E/E/PE 安全相关系统之间达到足够的独立性，指定的安全功能就能通过两个系统实现。

注 7：在规定的任务时间内不能进行维修的、按高要求或连续运行模式运行的 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，除以任务时间即得

到要求的每小时失效频率，然后从表 3 获得要求的安全完整性等级。

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—2017 的 7.4.2.4 和 GB/T 20438.3—2017 的 7.4.2.8。

7.6.2.11 一些情况下，分配过程出现了 E/E/PE 安全相关系统执行 SIL4 安全功能的要求，则应用以下措施：

a) 应对应用进行重新考虑，确定是否可以对任何风险参数进行调整，从而避免对 SIL4 安全功能的要求。复审应考虑是否：

——能够引入不基于 E/E/PE 安全相关系统的额外的安全相关系统和其他风险降低措施；

——能够降低后果的严重性；

——降低指定后果的可能性。

b) 如果对应用深入的研究，决定实施 SIL4 安全功能，那么应使用定量方法进行进一步的风险评估，同时考虑潜在的 E/E/PE 系统与下列系统之间的共因失效：

——其失效会导致对 E/E/PE 安全相关系统提出要求的任何其他系统；

——任何其他安全相关系统。

7.6.2.12 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。即安全相关系统运行在：

——低要求运行模式下，下限设为要求时安全功能的危险失效平均概率为 10^{-5}；

——高要求或连续运行模式，下限设为危险失效平均频率为 10^{-9}/h。

注：对于非复杂系统，通过安全相关系统的设计实现更优目标安全完整性是可能的。但对于相对复杂的系统（例如可编程电子安全相关系统），这些限值代表了目前能够达到的水平。

7.6.2.13 7.6.2.1～7.6.2.12 中获得的整体安全要求分配的信息和结果连同所作的任何假设和证明（包括 EUC 的整个生命周期中需要管理的关于其他风险降低措施的假设）都要归档。

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 7.10 中指定的 E/E/PE 安全相关系统安全要求的基础。

7.7 整体运行和维护计划编制

注 1：这一阶段是图 2 的方框 6。

注 2：以下图 7 所示为运行和维护活动模型的一个例子。

注 3：以下图 8 所示为运行和维护管理模型的一个例子。

注 4：7.7.2 的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 5：为实现功能安全，有必要对所有其他风险降低措施提出类似要求。

7.7.1 目的

7.7 要求的目的是制定 E/E/PE 安全相关系统的运行和维护计划，以保证在运行和维护期间保持所需的功能安全。

7.7.2 要求

7.7.2.1 应制定计划以规定以下内容：

a) 保持 E/E/PE 安全相关系统所需的功能安全，需要执行的日常行动；

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、正常运行、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：

1) 在 E/E/PE 安全相关系统发生故障期间对 EUC 运行的约束；

2) 在 E/E/PE 安全相关系统的维护期间对 EUC 运行的约束；

3) 当对 EUC 运行的约束可能被解除时；

4) 恢复到正常运行的规程；

5) 确认已达到正常运行的规程；

6) 在启动、特殊运行或测试时，E/E/PE 安全相关系统执行的安全功能可能被旁路的情况；

7) 在旁路 E/E/PE 安全相关系统之前、之后、之中需遵循的规程，包括工作规程许可和授权级别。

c) 显示功能安全审核和测试结果的文档，这些文档需被维护；

d) 危险事件和具有可能导致危险事件的所有意外事故的文档，这些文档需被维护；

e) 维护活动(不同于修改活动)的范围；

f) 危险事件发生时应采取的行动；

g) 按时间顺序编排运行和维护活动文档的内容(见 7.15)。

注 2：大多数 E/E/PE 安全相关系统具有一些失效模式，仅在日常维护的测试中才可发现。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。

注 3：本条适用于软件供应商，要求软件供应商提供软件产品的信息和运行规程，以使用户在运行和维护安全相关系统时能保证所需的安全功能。其中包括作为运行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—2017 的 7.6)，这些规程的实现包括在 GB/T 20438.3—2017 的 7.8 中。作为修改一个安全相关系统的某条要求的后果而产生的进一步软件修改的准备规程详见 GB/T 20438.3—2017 的7.6。这些规程的实现包括在 GB/T 20438.2—2017 中的 7.8 中。

注 4：在运行和维护规程编制过程中宜考虑满足 GB/T 20438.2 和 GB/T 20438.3 的要求。

7.7.2.2 如果 E/E/PE 安全相关系统的任何硬件故障裕度为零的子系统处于离线测试，计划应当确保通过附加措施和约束以维持 EUC 的安全。附加措施和约束提供的安全完整性应至少等于 E/E/PE 安全相关系统正常运行时提供的安全完整性。如果 E/E/PE 安全相关系统的任何子系统的硬件故障裕度大于零，则在测试过程中，至少保留 E/E/PE 安全相关系统的一条通道在运行，并且测试应当在 MTTR 内完成，该 MTTR 是在确定符合目标失效量的计算时设定的值。

注：硬件故障裕度见 GB/T 20438.2—2017 的 7.4.4.1。

7.7.2.3 用来检测未揭露的故障的定期维护活动应当通过系统性分析确定。

注：如果未揭露的故障没有被检测到，则：

a) 如果是 E/E/PE 安全相关系统或其他风险降低措施，导致要求时运行失效；

b) 如果是非安全相关系统，导致对 E/E/PE 安全相关系统或其他风险降低措施产生要求。

7.7.2.4 维护 E/E/PE 安全相关系统的计划应当得到负责运行和维护以下系统的相关人员的同意：

——E/E/PE 安全相关系统；

——其他风险降低措施；和

——有可能对 E/E/PE 安全相关系统或其他风险降低措施产生要求的非安全相关系统。

7.8 整体安全确认计划编制

注 1：这一阶段是图 2 的方框 7。

注 2：此条款的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 3：为实现功能安全，有必要对其他风险降低措施提出类似要求。

7.8.1 目的

7.8 的目的是制定一个对 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 制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 运行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；

——示教；

——自动；

——手动；

——半自动；

——运行的稳定状态；

——重新启动；

——关机；

——维护；

——合理可预见的异常状况。

d) 针对开始调试之前的每种 EUC 运行模式，需要进行确认的 E/E/PE 安全相关系统的规范；

e) 确认的技术策略(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 中输出的每个要素的具体引用；

h) 开展确认活动所需的环境(如进行测试所需的经过校准的工具和设备等)；

i) 通过和不通过的准则；

j) 评价结果有效性的方针和规程，特别是不通过时的方针和规程。

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/PE 系统安全确认和软件安全确认计划的工作。重要的是，保证考虑了两个或多个 E/E/PE 安全相关系统和/或其他风险降低措施之间的相互作用，并实现了所有的安全功能(如 7.5 输出中的规定)。

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

7.9 整体安装和调试计划编制

注 1：这一阶段是图 2 的方框 8。

注 2：此条款的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 3：为实现功能安全，有必要对其他风险降低措施提出类似要求。

7.9.1 目的

7.9.1.1 7.9 的第一个目的是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 7.9 的第二个目的是拟定在受控方式下的 E/E/PE 安全相关系统的调试计划，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：

a) 安装日程表；

b) 不同安装部分的负责人员；

c) 安装规程；

d) 各组件集成的顺序；

e) 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；

f) 失效和不兼容性的解决规程。

7.9.2.2 E/E/PE 安全相关系统的调试计划应规定：

a) 调试日程表；

b) 调试不同部分的负责人员；

c) 调试操作规程；

d) 与不同安装阶段的关系；

e) 与确认的关系。

7.9.2.3 整体安装和调试计划应归档。

7.10 E/E/PE 系统安全要求规范

注：这一阶段是图 2 的方框 9。

7.10.1 目的

7.10 的目的是依据 E/E/PE 系统安全功能要求和 E/E/PE 系统安全完整性要求，定义 E/E/PE 系统安全要求以实现所需的功能安全。

7.10.2 要求

7.10.2.1 E/E/PE 系统安全要求规范应来自 7.6 中指定的安全要求的分配，并结合应用的相关信息。这些信息应提供给 E/E/PE 安全相关系统的开发者。

7.10.2.2 E/E/PE 系统安全要求规范应当包括安全功能的要求以及它们相应的安全完整性等级。

注：目的是描述安全功能和它们所需的功能安全性能，而并不特指设备。此规范可以依据整体安全要求和整体安全要求分配阶段的输出进行验证，并可作为 E/E/PE 系统实现(见 GB/T 20438.2—2017 的 7.2)的基础。设备设计者可将规范作为选择设备和架构的基础。

7.10.2.3 E/E/PE 系统安全要求规范应当提供给 E/E/PE 安全相关系统的开发者。

7.10.2.4 E/E/PE 系统安全要求规范的结构和表达应当按如下方式：

a) 清晰、准确、不含糊、可验证、可测试、可维护且切实可行；

b) 便于在 E/E/PE 系统安全生命周期任何阶段使用此信息的工作人员理解；

c) 安全功能的要求可以通过自然语言或正式语言和/或逻辑图、顺序图或因果图表述，每个安全功能应单独定义。

7.10.2.5 E/E/PE 系统安全要求规范应当包含 E/E/PE 系统安全功能要求(见 7.10.2.6)和 E/E/PE 系统安全完整性要求(见 7.10.2.7)。

7.10.2.6 E/E/PE 系统安全功能要求规范应当包含：

a) 为实现所需的功能安全所需的所有安全功能的描述，每一个安全功能的描述应当：

——提供综合详细的具体要求以满足 E/E/PE 安全相关系统的设计与开发；

——包含 E/E/PE 安全相关系统实现或保持 EUC 系统安全状态的行为方式；

——规定为实现或保持 EUC 系统安全状态，是否要求连续控制以及控制周期，和

——规定安全功能是否适用于 E/E/PE 安全相关系统的低要求、高要求或连续运行模式。

b) 响应时间性能(即安全功能必须在要求的时间内完成)。

c) 实现所需的功能安全所必需的 E/E/PE 安全相关系统和操作员接口。

d) 所有功能安全相关的可能会对 E/E/PE 安全相关系统设计产生影响的信息。

e) 实现所需的功能安全所必需的 E/E/PE 安全相关系统和其他系统(EUC 内部或外部的)之间的接口。

f) 所有 EUC 的相关运行模式，包括：

——使用准备包括设置和调整；

——启动、示教、自动、手动、半自动、稳态运行；

——非运行的稳定状态、复位、关机、维护；

——合理可预见的不正常状态。

注：运行的特定模式(例如设置、调整或维护)可能要求额外的安全功能以确保安全运行。

g) 应规定所有 E/E/PE 安全相关系统所需的行为模式。特别是 E/E/PE 安全相关系统的失效行为和失效事件要求的响应(例如报警、自动停车等)。

7.10.2.7 E/E/PE 系统安全完整性要求规范应当包含：

a) 每一个安全功能的安全完整性等级和要求时目标失效量的规定值；

注 1：目标失效量的规定值可来自定量方法计算(见 7.5.2.3)。或者，当安全完整性以定性方式确定并以安全完整性等级表述时，目标失效量可参照表 2 或表 3。这样，指定的目标失效量是安全完整性等级的最小平均失效概率或失效率，除非已经用了另外的数值校准此方法。

注 2：安全功能运行在低要求运行模式的情况下，目标失效量将以要求时的危险失效平均概率表示，其由安全功能的安全完整性等级决定(见表 2)，除非 E/E/PE 系统安全完整性要求规范中对安全功能的要求满足特定目标失效量，而非指定的安全完整性等级。例如，为达到要求的可容忍风险，目标失效量被指定为 1.5×10^{-2}(要求时的危险失效平均概率)，则由随机硬件失效引起的安全功能在要求时的危险失效平均概率需小于等于 1.5×10^{-2}。

注 3：安全功能运行于高要求运行模式或连续运行模式的情况下，目标失效量将以每小时危险失效平均频率表示，其由安全功能的安全完整性等级决定(见表 3)，除非 E/E/PE 系统安全完整性要求规范中对安全功能的要求满足特定目标失效量，而非指定的安全完整性等级。例如，为达到要求的可容忍风险，目标失效量被指定为 $1.5\times10^{-6}[h^{-1}]$(每小时危险失效平均频率)，则由随机硬件失效引起的安全功能的每小时危险失效平均频率需小于或等于 $1.5\times10^{-6}[h^{-1}]$。

b) 每个安全功能的运行模式(低要求、高要求或连续)；

c) 要求的负荷率和寿命；

d) 保证 E/E/PE 硬件检验测试的要求、约束、功能和设施；

注 4：制定 E/E/PE 系统安全要求规范时，宜考虑 E/E/PE 安全相关系统的具体应用。这对维护至关重要，规定的检验测试时间间隔不宜小于特定应用的合理期望值。例如，为公共使用的大批量生产的产品的现实可实现的服务间隔时间可能比受控较多的应用的时间要长。

e) E/E/PE 系统的整个安全生命周期中可能发生的所有极端环境条件，包括生产、存储、运输、测试、安装、调试、运行和维护；

f) 为实现功能安全应设置电磁干扰限制。限制应当充分考虑电磁环境和要求的安全完整性等级

(见 GB /Z 17624.2)；

注 5：由于电磁现象的本质和物理现象很复杂，对于所有电磁现象在要求的抗干扰水平和安全完整性水平下，能建立明显的且可证明的相关信息。因此，在这些情况下，只根据 SIL 规定有效地抗干扰水平是不可能也是不合理的。在某种程度上，作为替代方法可根据要求的 SIL 和特定的测试安排或者测试执行标准(见 GB /Z 17624.2)来规定要求的抗干扰水平。

注 6：见参考文献[15]。

g) 由于共因失效的可能性，对 E/E/PE 安全相关系统实现的限制和约束条件(见 7.6.2.7)。

7.11 E/E/PE 安全相关系统-实现

注：这一阶段是图 2 的方框 10 和图 3、图 4 的方框 10.1～10.6。

7.11.1 目的

7.11 的目的是建立符合 E/E/PE 系统的安全要求规范(包括 E/E/PE 系统的安全功能要求规范和 E/E/PE 系统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)。

7.11.2 要求

应满足的要求包含在 GB/T 20438.2 和 GB/T 20438.3 中。

7.12 其他风险降低措施-规范和实现

注：这一阶段是图 2 的方框 11。

7.12.1 目的

7.12 的目的是建立其他风险降低措施，以满足为该系统规定的安全功能要求和安全完整性要求。

7.12.2 要求

本部分不包括用其他风险降低措施满足安全功能要求和安全完整性要求的规范。

注：其他风险降低措施是基于电气/电子/可编程电子以外的技术(例如液压，气动等)或者是物理结构(例如一个排水系统，防火墙或一个堤坝)。这些已被纳入整体安全生命周期，以确保通过 E/E/PE 安全相关系统获得的风险降低是在结合通过其他风险降低措施获得的风险降低的情况下确定的。

7.13 整体安装和调试

注 1：这一阶段是图 2 的方框 12。

注 2：7.13 的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 3：为了实现功能安全，有必要对所有其他的风险降低措施提出类似的要求。

7.13.1 目的

7.13.1.1 7.13 的第一个目的是安装 E/E/PE 安全相关系统。

7.13.1.2 7.13 的第二个目的是调试 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(见 7.9)。

7.13.2.2 安装过程中归档的信息应包括：

——安装活动文档；

——失效和不兼容的分析。

7.13.2.3 调试活动应按照 E/E/PE 安全相关系统的调试计划执行。

7.13.2.4 调试过程中归档的信息应包括：

——调试活动文档；

——涉及的失效报告；

——失效和不兼容的分析。

7.14 整体安全确认

注 1：这一阶段是图 2 的方框 13。

注 2：7.14 的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 3：为实现功能安全，有必要对其他风险降低措施提出类似要求。

7.14.1 目的

7.14 的目的是确认 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 作为确认活动的一部分，所用的所有定量测量设备应按国家标准或供方的规范进行校准。

7.14.2.3 确认过程中归档的信息应包括：

——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；

——测试项目的配置标识、适用的规程和测试环境；

——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，要进行分析决定是继续进行确认还是发布一个变更请求，返回到确认的早期阶段，并将上述内容归档。

7.15 整体运行、维护和修理

注 1：这一阶段是图 2 的方框 14。

注 2：7.15 中涉及的组织措施是为有效实现技术要求创造条件，并以完全实现和保持 E/E/PE 安全相关系统的功能安全为目的。维护功能安全所需的技术要求，将被规定为 E/E/PE 安全相关系统及其组件和元件的供应商提供信息的一部分。

注 3：在维护和修理活动中的功能安全要求，可能与在运行中的要求不同。

注 4：如果没有检查为初始安装和调试而制定的测试规程的有效性和实用性，就不宜假设 EUC 在线运行的情况下可以使用这些规程。

注 5：7.15 的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 6：为实现功能安全，有必要对其他风险降低措施提出类似要求。

7.15.1 目的

7.15.1.1 7.15 的第一个目的是确保 E/E/PE 安全相关系统的功能安全维持在规定的水平。

7.15.1.2 7.15 的第二个目的是确保 E/E/PE 安全相关系统的整体运行、维护和修理所需的技术要求已被规定，并提供给未来负责 E/E/PE 安全相关系统运行和维护的人员。

7.15.2 要求

7.15.2.1 应遵从下列要求：

——E/E/PE 安全相关系统运行和维护计划(见 7.7)；

——E/E/PE 安全相关系统运行、维护和修理规程。

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：

——规程的执行；

——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 6.2.7)；

——对 E/E/PE 安全相关系统所作的修改建立文档。

注 1：运行和维护活动模型的例子见图 7。

注 2：运行和维护管理模型的例子见图 8。

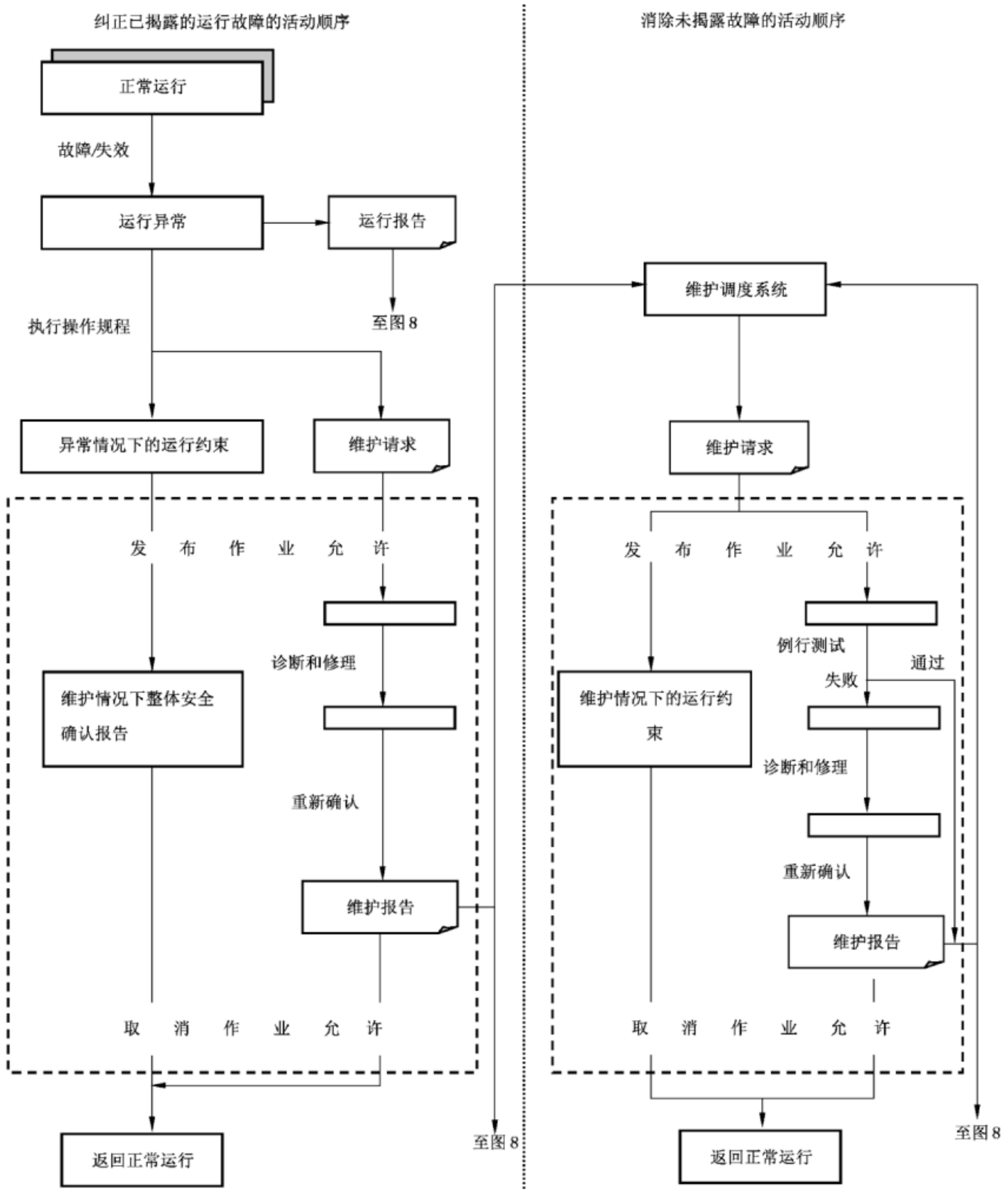
7.15.2.3 按时间编制的 E/E/PE 安全相关系统的运行、修理和维护文档应妥善保存并包括下列信息：

——功能安全审核和测试的结果；

——向 E/E/PE 安全相关系统(在实际运行中)发出要求的原因和时间，连同收到那些要求时 E/E/PE 安全相关系统的性能，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 按时间编排的文档的确切要求取决于具体的产品或应用，并应在产品和应用领域相关标准中详细说明。



注解：

运行异常 状态（命名的）

状态（未命名的）

维护请求 文档

重新确认 行动/事件

图 7 运行和维护活动模型示例

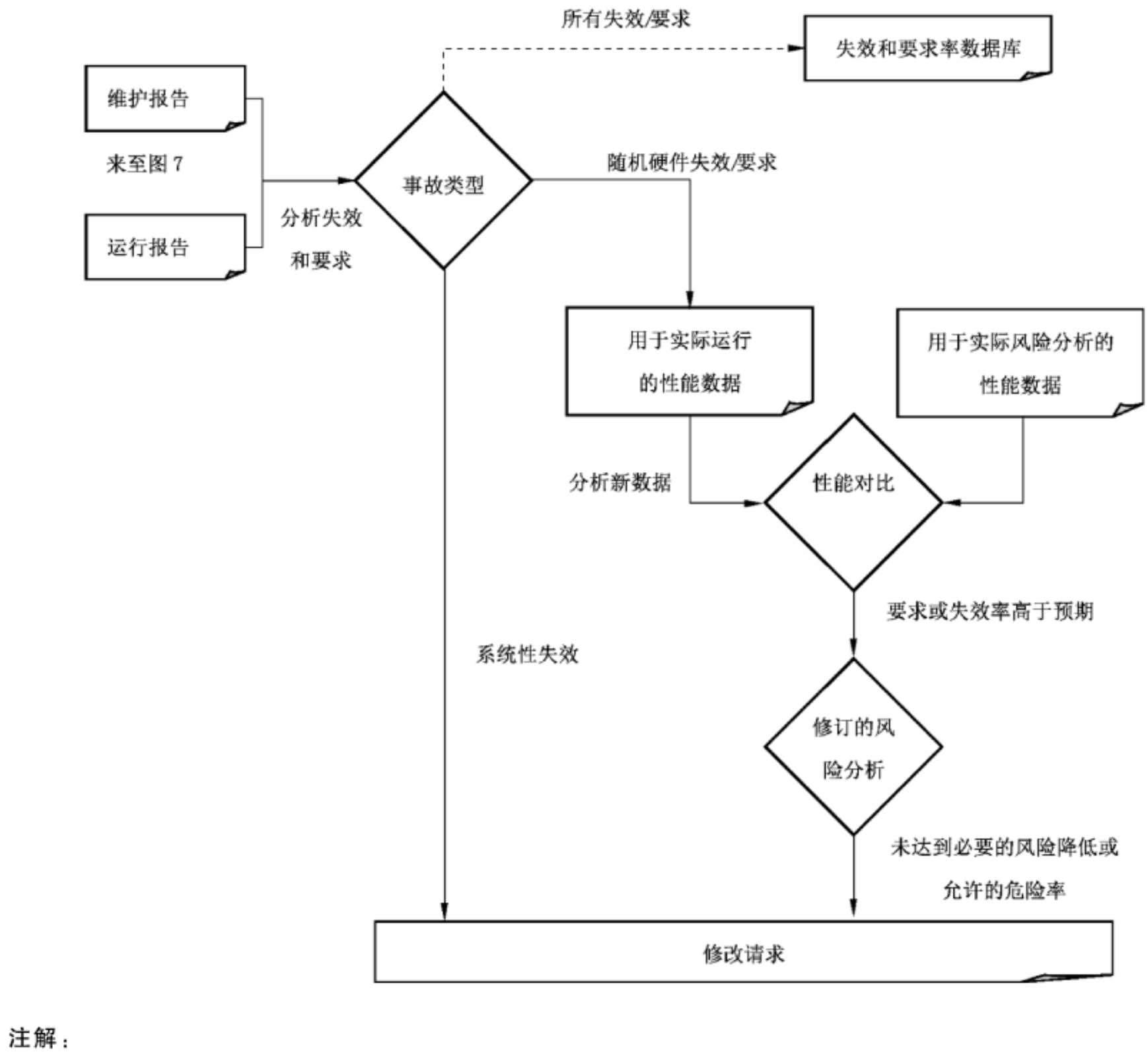


图 8　运行和维修管理模型示例

7.16　整体修改和改型

注 1：这一阶段是图 2 的方框 15。

注 2：7.16 中涉及的组织措施是为有效实现技术要求创造条件，并以完全实现和保持 E/E/PE 安全相关系统的功能

安全为目的。维护功能安全所需的技术要求，将被规定为 E/E/PE 安全相关系统及其组件和元件的供应商提供信息的一部分。

注 3：7.16 的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 4：为实现功能安全，有必要对其他风险降低措施提出类似要求。

7.16.1 目的

7.16 的目的是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，需计划好有关规程（见 6.2.8）。

注：修改规程模型的例子见图 9。

7.16.2.2 只有根据功能安全管理规程（见 6.2.8）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) 系统性故障的经验；

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) 运行和维护性能的分析，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/PE 系统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和深度。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 中所述的结果应归档。

7.16.2.5 执行所需修改或改型活动的批准应取决于影响分析的结果。

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应启动执行活动返回到整体安全生命周期、E/E/PE 系统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应按照为特定阶段规定的规程执行，该规程应符合本部分的要求。

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：如果没有检查为初始安装和调试而制定的测试规程的有效性和实用性，就不宜假设 EUC 在线运行的情况下可以使用这些规程。

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，其内容包括：

——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；

——被修改和改型活动影响的所有文档。

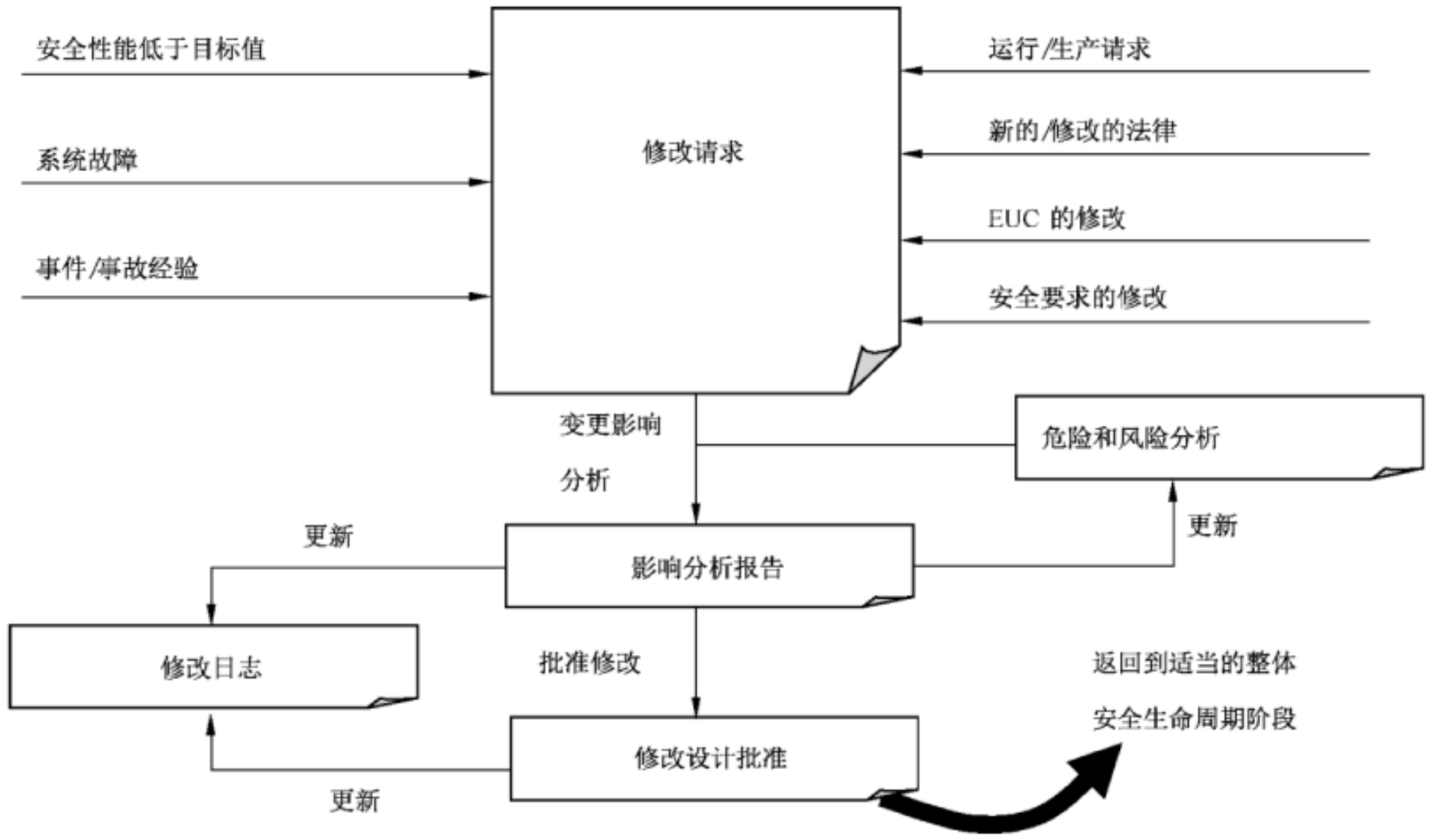


图 9　修改规程模型示例

7.17　退役或处置

注 1：这一阶段是图 2 的方框 16。

注 2：7.17 的要求是针对 E/E/PE 安全相关系统的。建议结合其他风险降低措施进行考虑，特别是假设已经考虑了需要在 EUC 的整个生命周期中加以管理的其他风险降低措施。

注 3：为实现功能安全，有必要对其他风险降低措施提出类似要求。

7.17.1　目的

7.17 的目的是定义必要的规程以确保在 EUC 退役或处置活动中或活动后，E/E/PE 安全相关系统具有适当的功能安全。

7.17.2　要求

7.17.2.1　在进行退役或处置活动之前应进行影响分析，影响分析包括建议的退役或处置活动对任何 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。评估应包括危险和风险分析，此分析应足以确定其后整体安全生命周期、E/E/PE 系统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和深度。

7.17.2.2　7.17.2.1 所述之结果应归档。

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，才可启动退役和处理阶段（见第 6

章)。

7.17.2.4 执行所需退役或处置的批准应取决于影响分析的结果。

7.17.2.5 在退役或处置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 如果退役或处置活动会对 E/E/PE 安全相关系统的功能安全产生影响,则应启动执行活动返回到整体安全生命周期、E/E/PE 系统安全生命周期或软件安全生命周期的适当阶段。然后,应按照本部分中为 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,这种分析可能对 E/E/PE 安全相关系统执行的安全功能产生不同的安全完整性等级要求。

注 2:退役或处置阶段中的功能安全要求可能与运行阶段中的不同。

7.17.2.7 应建立和保存按时间编排的包括退役或处置活动细节的文档,其内容包括:

——用于退役或处置活动的计划;

——影响分析。

7.18 验证

7.18.1 目的

7.18 的目的是为了(通过复审、分析和/或测试)证明在整体安全生命周期、E/E/PE 系统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/PE 系统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、技术和工具。

7.18.2.3 验证应按验证计划进行。

注:验证技术和措施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归档,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

本章的目的是规定必要的活动,以调查和判断基于 GB/T 20438 相关条款的 E/E/PE 安全相关系统或符合项(例如,组件/子系统)是否充分实现功能安全。

8.2 要求

8.2.1 应指定一人或多人进行一个或多个功能安全评估,以达到充分判断:

——E/E/PE 安全相关系统在特定的环境下实现的功能安全,符合本 GB/T 20438 的相关条款;

——组件和子系统实现的功能安全，符合 GB/T 20438 的相关条款。

8.2.2 进行功能安全评估时应对整体安全生命周期、E/E/PE 系统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。

注：访问曾参与安全生命周期阶段的人员可能无法实现，在这种情况下，应该依赖当前具有相关职责的人员。

8.2.3 应对整体安全生命周期、E/E/PE 系统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，包括文档、验证和功能安全管理。

8.2.4 进行功能安全评估时应考虑在整体、E/E/PE 系统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，并判断满足 GB/T 20438 的目的和要求的程度。

8.2.5 所有由负责实现功能安全的供应商和其他方制定的相关符合性声明，都应包括在功能安全评估中。

注：这类声明可以是为了一个运行着的系统制定，也可以是在整体安全生命周期、E/E/PE 系统安全生命周期和软件安全生命周期的各个阶段中为了保证活动和/或设备的功能安全而制定的。

8.2.6 功能安全评估可以在整体的、E/E/PE 系统的和软件安全生命周期的每个阶段后，或在几个安全生命周期阶段之后开展，最重要的是，功能安全评估必须在真正的危险出现之前进行。

8.2.7 功能安全评估应包含对已(全部或部分)执行的，与其范围有关的功能安全审核证据的评估。

8.2.8 每个功能安全评估应至少考虑如下内容：

——先前所做的功能安全评估工作；

——对整体安全生命周期、E/E/PE 系统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策略；

——对先前的功能安全评估的建议以及已作更改与建议的符合程度。

8.2.9 每个功能安全评估应有计划。计划应规定所有必要的信息，以便有效的评估，包括：

——功能安全评估的范围；

——参与的组织；

——要求的资源；

——承担功能安全评估的各方；

——承担功能安全评估各方的独立等级；

——每个参与功能安全评估人员的能力；

——功能安全评估的输出；

——功能安全评估应如何关联其他适合的功能安全评估，并与之集成(见 6.2.1)。

注 1：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版本状态；

注 2：计划可以由功能安全评估负责方或功能安全管理负责方制定，或由他们共同制定。

8.2.10 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功能安全管理的各方的批准。

8.2.11 对功能安全评估做结论时，应由执行评估的各方按评估的计划和参考条款建立文档，内容如下：

——进行的活动；

——产生的结果；

——得到的结论；

——按照标准的要求判断功能安全的充分性；

——评估产生的建议，包括接受、有条件的接受或不接受。

8.2.12 符合项的功能安全评估的相关输出应提供给包括 E/E/PE 安全相关系统设计方和评估方在内的任何对整体的、E/E/PE 系统的或软件的安全生命周期负责的各方。对 E/E/PE 安全相关系统评估

的输出应提供给 E/E/PE 系统集成商。

注：符合项是满足 GB/T 20438 条款的任何项(如，一个组件)。

8.2.13 符合项的功能安全评估的输出应包括以下的信息，以便在更大系统的情况下评估结果的复用(见 GB/T 20438.2—2017 的附录 D、GB/T 20438.3—2017 附录 D 和 GB/T 20438.4—2017 的 3.8.17)。

a) 符合项的准确识别，包括硬件和软件版本；

注：如果符合项作为一个更大系统或设备家族的一部分进行评估，系统或设备家族的准确识别也建议归档。

b) 评估中假设的条件(如使用 E/E/PE 安全相关系统的条件)；

c) 评估结论所依据的文档证据；

d) 评估系统性能力和判断有效性所使用的规程、方法和工具；

e) 评估硬件安全完整性和判断采用方法的合理性以及数据质量(例如，失效率/分布数据源)的规程、方法和工具；

f) 根据 GB/T 20438 的要求和符合项安全手册中的安全特征规范，获得的评估结果；

g) 对 GB/T 20438 要求已接受的差异，在文档中有对应解释和/或参考依据。

8.2.14 执行功能安全评估的各方应有能力按照 6.2.13～6.2.15 的要求开展活动。

8.2.15 执行功能安全评估的各方的最低独立等级应按照表 4 和表 5 规定。产品和应用领域的国家标准可按照其自身的标准，规定与表 4 和表 5 不同的独立等级。对表的解释如下：

——X：规定的独立等级，是在规定的后果(表 4)或安全完整性等级/系统性能力(表 5)情况下的最小值。如果采用一个更低的独立等级，应详细说明使用它的理由。

——X1 和 X2：见 8.2.16。

——Y：规定的独立等级，相对于规定的后果(表 4)或安全完整性等级/系统性能力(表 5)被认为是不充分的。

8.2.16 在表 4 和表 5 中，只有标记为 X，X1，X2 或 Y 的单元应被作为确定独立等级的基础。

对标记为 X1 和 X2 的单元，用 X1 还是 X2(不是同时)，取决于特定应用的一些因素。应详细说明选择 X1 或 X2 的理由。X2 比 X1 更合适的因素是：

——缺乏以往类似设计的经验；

——更复杂；

——设计更新颖；

——技术更新颖。

注 1：根据公司的组织和公司内部的专业知识，独立个人和部门的需求可能要通过外部组织达到。相反，公司有对安全相关系统的风险评估和应用非常熟悉的内部组织机构，并从负责主要开发的组织中独立和分离出来(用管理和其他资源的方式)，可能能够利用自己的资源来满足一个独立组织的需求。

注 2：对独立人员、独立部门和独立组织的定义见 GB/T 20438.4—2017 中 3.8.11、3.8.12 和 3.8.13。

注 3：功能安全评估方宜对评估范围的任何事情谨慎提出建议，因为这可能会损害他们的独立性。对可能导致判定安全不充分的情况，往往适合给出建议，例如证据不足，但通常不宜对这些问题或其他问题的具体补救措施提供咨询意见或给予建议。

8.2.17 在表 4 中，规定的独立等级的后果值为：

——后果 A：轻微的伤害(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：致很多人死亡。

表 4 中规定的后果是由包括 E/E/PE 安全相关系统在内的所有风险降低措施的失效事件中产生的。

8.2.18 在表5中，最低独立等级应基于由E/E/PE安全相关系统实现的具有最高的安全完整性等级的安全功能，或对于组件/子系统来说，应基于由安全完整性等级所规定的最高系统性能力。

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

最低独立等级	后果(见8.2.17)			
	A	B	C	D
独立人员	X	X1	Y	Y
独立部门		X2	X1	Y
独立组织			X2	X
注：本表的详细说明见8.2.15、8.2.16和8.2.17				

表5 进行功能安全评估各方的最低独立等级[整体安全生命周期阶段9和10，包括E/E/PE系统安全生命周期、软件安全生命周期的所有阶段(见图2，图3和图4)]

最低独立等级	安全完整性等级/系统性能力			
	1	2	3	4
独立人员	X	X1	Y	Y
独立部门		X2	X1	Y
独立组织			X2	X
注：本表的详细说明见8.2.15、8.2.16和8.2.18				

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，以及为结构化信息建立文档的方法。文档应包括为有效执行下列各项工作所需的足够信息：

——整体的、E/E/PE系统的和软件的安全生命周期的各个阶段；

——功能安全管理（第6章）；

——功能安全评估（第8章）。

足够信息的构成取决于一系列因素，包括E/E/PE安全相关系统的大小、复杂程度以及特定应用的相关要求。在特定的产品和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的文档中，也可能分开放在几个实际的文档中。同样，实际的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和命名文档的方法示例，更详细的说明见参考文献[7]。

文档是一种旨在让人理解的结构化的信息，可作为用户和/或系统之间进行交换的一个单元（见参考文献[16]）。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，除非在提及的条款中有清楚地说明或能从中清楚地理解，否则文档这个术语一般是指信息而不是指实际的文档。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。

参考文献[16]定义了文档种类，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（符号和符号间用来表示信号的线）的方式规定功能；

——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给出了结构化信息的文档结构示例。表中指出

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),表中的文档根据 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,其他值则在调试和维护中设定。

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)
整体范围确定	描述(整体范围确定)
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:整体安全功能要求和整体安全完整性要求)
整体安全要求分配	描述(安全要求分配)
整体运行和维护计划编制	计划(整体运行和维护)
整体安全确认计划编制	计划(整体安全确认)
整体安装和调试计划编制	计划(整体安装);计划(整体调试)
E/E/PE 系统安全要求	规范(E/E/PE 系统的安全要求,包括 E/E/PE 系统的安全功能要求和 E/E/PE 系统安全完整性的要求)
E/E/PE 安全相关系统的实现	见表 A.2 和表 A.3
整体安装和调试	报告(整体安装);报告(整体调试)
整体安全确认	报告(整体安全确认)
整体运行和维护	日志(整体运行和维护)
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)
退役或处置	报告(整体退役或处置影响分析);计划(整体退役或处置);日志(整体退役或处置)
针对所有阶段	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/PE 系统安全生命周期有关信息的文档结构示例

E/E/PE 系统安全生命周期阶段	信 息
E/E/PE 系统确认计划编制	计划(E/E/PE 系统安全确认)
E/E/PE 系统设计和开发 E/E/PE 系统架构	描述(E/E/PE 系统架构设计,包括硬件架构和软件架构)
	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)
硬件架构	描述(硬件架构设计)
	规范(硬件架构集成测试)
硬件模块设计	规范(硬件模块设计)
	规范(硬件模块测试)

表 A.2（续）

E/E/PE 系统安全生命周期阶段	信　息
元件制造和/或采购	硬件模块； 报告(硬件模块测试)
可编程电子集成	报告(可编程电子硬件和软件集成测试)(见表 A.3)
E/E/PE 系统集成	报告(可编程电子和其他硬件集成测试)
E/E/PE 系统运行和维护规程	说明书(用户)； 说明书(运行和维护)
E/E/PE 系统安全确认	报告(E/E/PE 系统安全确认)
E/E/PE 系统修改	说明书(E/E/PE 系统修改规程)； 请求(E/E/PE 系统修改)； 报告(E/E/PE 系统修改影响分析)； 日志(E/E/PE 系统修改)
针对所有阶段	计划(E/E/PE 系统安全)； 计划(E/E/PE 系统验证)； 报告(E/E/PE 系统验证)； 计划(E/E/PE 系统功能安全评估)； 报告(E/E/PE 系统功能安全评估)
针对所有相关阶段	符合项的安全手册

表 A.3　与软件安全生命周期有关信息的文档结构示例

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：软件安全功能要求和软件安全完整性要求)
软件确认计划编制	计划(软件安全确认)
软件设计和开发 软件架构	描述(软件架构设计)(硬件架构设计描述见表 A.2)； 规范(软件架构集成测试)； 规范(可编程电子硬件和软件集合测试)； 说明书(开发工具和编码手册)；
软件系统设计	描述(软件系统设计)； 规范(软件系统集成测试)；
软件模块设计	规范(软件模块设计)； 规范(软件模块测试)；
编码	表(源代码)； 报告(软件模块测试)； 报告(代码复审)；
软件模块测试	报告(软件模块测试)；
软件集成	报告(软件模块集成测试)； 报告(软件系统集成测试)； 报告(软件架构集成测试)

表 A.3（续）

软件安全生命周期阶段	信　息
可编程电子集成	报告(可编程电子硬件和软件集成测试)
软件运行和维护规程	说明书(用户)； 说明书(运行和维护)
软件安全确认	报告(软件安全确认)
软件修改	说明书(软件修改规程)； 请求(软件修改)； 报告(软件修改影响分析)； 日志(软件修改)
针对所有阶段	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)
针对所有相关阶段	符合项的安全手册

A.3　实际的文档结构

文档的实际结构是将不同资料组合为文档、文档集、文档夹和文档夹组的形式。一个文档可能出现在不同集中。

对于大型复杂系统，许多实际的文档可能分成多个文档夹，对于小型低复杂系统，实际的文档数量有限，可把带有不同检索标签的不同文档集组合成一个文档夹。图 A.1 是根据用户组构建的文档夹的示例。

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，因此一些实际的文档可能出现于几个文档夹组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 所示的不同的文档集中。例如，工程集会包含危险和风险分析描述和整体安全要求规范。

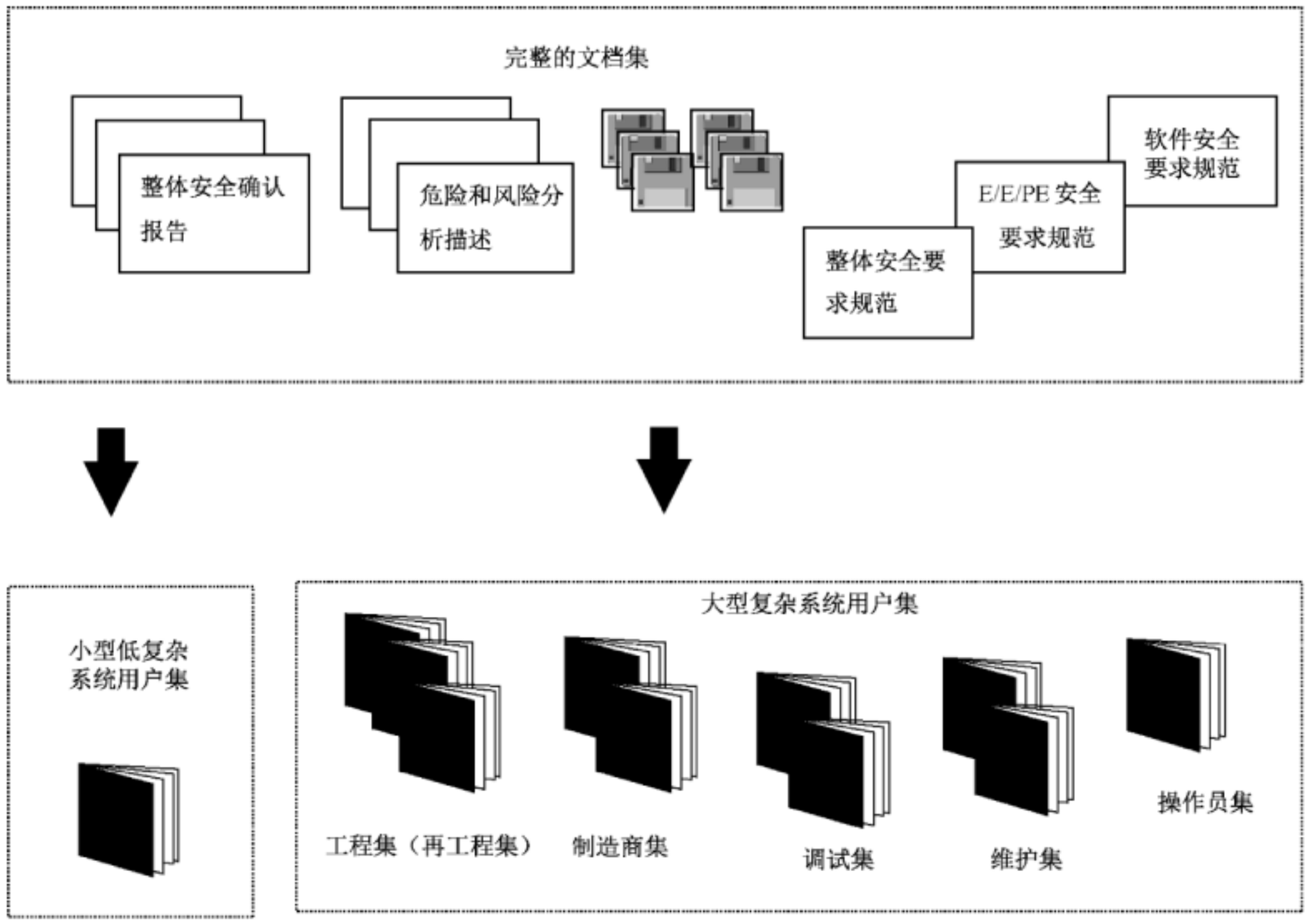


图 A.1　把信息构建成用户组的文档集

A.4　文档清单

文档清单典型地包括下列信息：

——图样或文档编号；

——修订索引；

——文档命名代码；

——标题；

——修订日期；

——数据载体。

该清单可以不同形式出现，如可按图样、文档编号或文档命名代码分类的数据库。文档命名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。

参 考 文 献

[1] GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

[2] GB 28526 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

[3] GB/T 12668.502 调速电气传动系统 第5-2部分:安全要求 功能

[4] GB/Z 29638—2013 电气/电子/可编程电子安全相关系统的功能安全 功能安全概念及GB/T 20438系列概况

[5] GB/T 20438.6—2017 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

[6] GB/T 20438.7—2017 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

[7] GB/T 19898—2005 工业过程测量和控制 应用软件文档集

[8] Managing Competence for Safety—Related Systems, IET/BCS/HSE, 2007; (Part 1: Key guidance; Part 2 Supplementary material). HSE. 2007

[9] Competence criteria for safety-related system practitioners. IET. 2006

[10] IEC 60300-3-1:2003 Dependability management—Part 3-1: Application guide—Analysis techniques for dependability—Guide on methodology

[11] IEC 60300-3-9:1995 Dependability management—Part 3: Application guide—Section 9: Risk analysis of technological systems

[12] IEC 61882:2001 Hazard and operability studies (HAZOP studies)—Application guide

[13] NUREG/CR-4780, Volume 1, January 1988 Procedures for treating common cause failures in safety and reliability studies—Procedural framework and examples

[14] NUREG/CR-4780, Volume 2, January 1989 Procedures for treating common cause failures in safety and reliability studies—Analytical background and techniques

[15] IEC 61326-3-1 Electrical equipment for measurement, control and laboratory use—EMC requirements—Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)—General industrial applications

[16] ISO 8613-1:1994 Information techno logy—Open Document Architecture (ODA) and Interchange Format: Introduction and general principles

[17] IEC 61355 (all parts) Classification and designation of documents for plants, systems and equipment

[18] IEC 60601 (all parts) Medical electrical equipment

[19] GB /Z 17624.2 电磁兼容 综述 与电磁现象相关设备的电气和电子系统实现功能安全的方法

[20] GB/T 20438.5—2017 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

[21] IEC 62443(all parts) Industrial communication networks—Network and system security

[22] ISO/IEC/TR 19791 Information technology—Security techniques—Security assessment of operational systems

GB/T 20438.1—2017/IEC 61508-1:2010

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—2017/IEC 61508-1:2010
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2017年12月第一版
*
书号:155066·1-57378

GB/T 20438.1-2017