ICS 25.040
N 10

中华人民共和国国家标准

GB/T 21109.1—2007/IEC 61511-1:2003

过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和软件要求

Functional safety—Safety instrumented systems for the process industry sector—Part 1:Framework,definitions,system,hardware and software requirements

(IEC 61511-1:2003,IDT)

2007-10-11 发布　　2007-12-01 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 21109《过程工业领域安全仪表系统的功能安全》分为三个部分：

——第1部分：框架、定义、系统、硬件和软件要求；

——第2部分：GB/T 21109.1的应用指南；

——第3部分：确定要求的安全完整性等级的指南。

本部分为GB/T 21109的第1部分，等同采用IEC 61511-1:2003《过程工业领域安全仪表系统的功能安全　第1部分：框架、定义、系统、硬件和软件要求》(英文版)。为便于使用，对IEC 61511-1:2003做了下列编辑性修改：

——删除国际标准的前言，按GB/T 1.1—2000重新编写了本部分的前言；

——凡是出现“IEC 61511”之处均改为“GB/T 21109”，“IEC 61511-1”均改为“GB/T 21109.1”，“IEC 61511-2”均改为“GB/T 21109.2”，“IEC 61511-3”均改为“GB/T 21109.3”；

——凡是出现“本国际标准”之处均改为“GB/T 21109”；

——用小数点“.”代替作小数点的逗号“,”；

——根据GB/T 1.1—2000进行编辑性修改。

本部分的附录A为资料性附录。

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归口。

本部分主要起草单位：机械工业仪器仪表综合技术经济研究所、上海自动化仪表股份有限公司技术中心、北京华控技术有限责任公司、中科院沈阳自动化研究所、浙江中控技术有限公司、上海工业自动化仪表研究所、国营759厂。

本部分主要起草人：王春喜、梅恪、包伟华、王麟琨、刘丹、陈小枫、魏剑嵬、史学玲、谭平、李佳嘉、欧阳劲松、蔡廷安、马光武。

本部分为首次制定。

引　言

在过程工业(process industry sector)中,用来执行仪表安全功能的安全仪表系统已使用了多年。如要使仪表能有效地用于仪表安全功能,最重要的是该仪表应达到某些最低标准和性能水平。

GB/T 21109 阐述了过程工业安全仪表系统的应用。GB/T 21109 还要求执行一次过程危险和风险评估,使之能导出安全仪表系统的规范。当考虑安全仪表系统的性能要求时,才考虑其他安全系统,从而把其他安全系统的贡献计算在内。安全仪表系统包括从传感器到最终元件之内的所有部件和子系统,它们都是执行仪表安全功能所必要的。

GB/T 21109 包含了作为应用基础的两个概念:安全生命周期和安全完整性等级。

GB/T 21109 针对基于使用电气(E)/电子(E)/可编程电子(PE)技术的安全仪表系统。在逻辑解算器使用其他技术的情况下,须应用 GB/T 21109 的基本原则。GB/T 21109 还涉及安全仪表系统的传感器和最终元件,而不管它们所使用的技术。GB/T 21109 在 GB/T 20438—2006 的框架范围内专用于过程领域(见附录 A)。

GB/T 21109 提出了达到这些最低标准的安全生命周期活动的方法。为了使用合理和一致的技术策略,已采纳了此方法。

在大多数情况下,固有(inherently)安全过程设计就能很好地实现安全性。必要时,还可结合一个或一些保护系统,以便处理任何已发现的残余风险。保护系统可依靠不同的技术(化学的、机械的、液压的、气动的、电气的、电子的、可编程电子的)。为促成该方法,GB/T 21109 要求:

——执行一次危险和风险评估以便确定整体安全要求;

——给安全仪表系统分配安全要求;

——应在一个适用于所有用仪表实现功能安全的方法的框架内进行工作;

——详述了适用于实现功能安全的所有方法的某些活动(如安全管理)的使用。

关于过程工业的安全仪表系统的 GB/T 21109:

——涉及从初始概念、设计、实现、运行和维护直到停用的所有安全生命周期阶段;

——能使现有的或新的国家专用的过程工业标准同本标准协调一致。

GB/T 21109 致力于在过程工业领域内导致高度一致(如基本原则、术语、信息等)。这将带来安全和经济两方面的好处。

在权限方面,在管理当局(如国家的、省的、自治区的等)已建立过程安全设计、过程安全管理或其他要求的情况下,这些要求应比本标准中定义的要求优先考虑。

GB/T 21109 的整体框架见图 1。

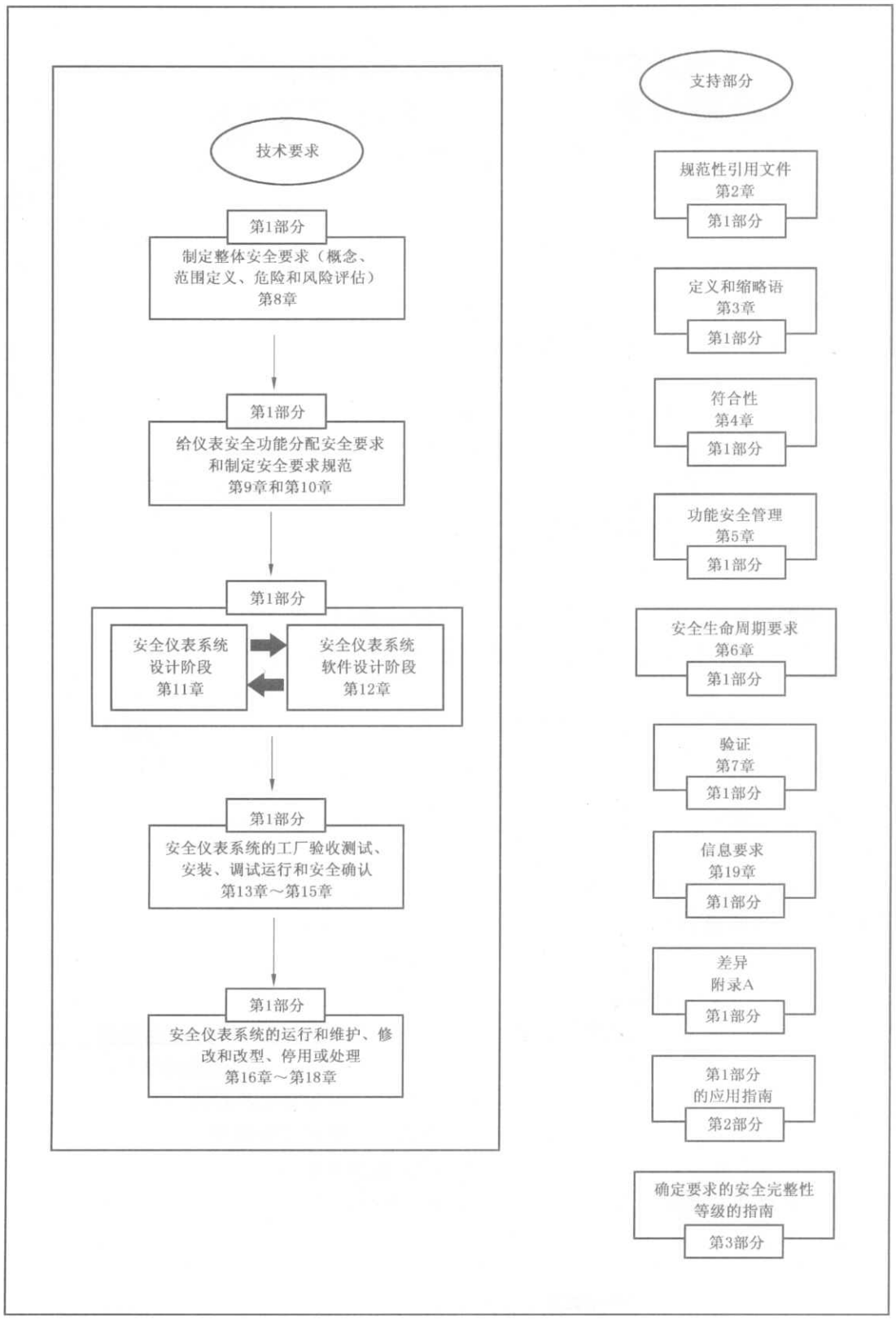


图 1　GB/T 21109 的整体框架

过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和软件要求

1 范围

GB/T 21109的本部分给出了安全仪表系统的规范、设计、安装、运行和维护要求,这确保该系统能把过程置于或保持在某个安全状态。GB/T 21109已作为GB/T 20438—2006在过程领域的实现而制定。

尤其是,本部分:

a) 规定了实现功能安全的要求但未规定谁负责实现这些要求(如设计师、供应商、所有权公司/运营公司、承包商);根据安全计划编制和国家法规的情况,责任可能指派到不同的责任方。

b) 适用于把满足GB/T 20438—2006或本部分中11.5要求的设备集成到可用于过程领域应用的整体系统中,但并不适用于希望申明装置适用于过程领域的安全仪表系统的制造商(见GB/T 20438.2—2006和GB/T 20438.3—2006)。

c) 定义了GB/T 21109和GB/T 20438—2006之间的关系(图2和图3)。

d) 适用于开发使用有限可变语言或固定程序语言的系统的应用软件,而不适用于开发嵌入式软件(系统软件)或使用全可变语言的制造商、安全仪表系统设计师、集成商和用户(见GB/T 20438.3—2006)。

e) 适用于包括化学、炼油、油气生产、纸浆和造纸、非核电生产在内的过程领域的广泛工业领域。

注:在某些过程领域应用中(如海上),可能还需满足一些附加要求。

f) 绘制了仪表安全功能和其他功能之间的关系(图4)。

g) 在考虑到其他方法所达到的风险降低的情况下,辨识仪表安全功能的功能要求和安全完整性要求。

h) 规定了系统结构、硬件配置、应用软件和系统集成的要求。

i) 规定了安全仪表系统用户和集成商的应用软件要求(第12章),特别规定了对以下内容的要求:

——在应用软件设计和开发过程中将使用的各个安全生命周期阶段和活动(软件安全生命周期模型)。这些要求包括措施和技术的应用,它们致力于避免软件中的故障,并控制可能发生的失效。

——被传递给执行SIS集成的组织的与软件安全确认相关的信息。

——用于SIS运行和维护的用户所需软件有关的信息和规程的准备。

——执行修改安全软件的组织应满足的规程和规范。

j) 可在为了人员保护、公众保护或环境保护而使用一个或多个仪表安全功能来实现功能安全时使用。

k) 也适用于非安全应用(如资产保护)。

l) 确定了实现仪表安全功能的要求,这些要求被用作实现功能安全的整体安排的一部分。

m) 使用了安全生命周期(图8),并定义了确定安全仪表系统功能要求和安全完整性要求所必需的活动清单。

n) 要求执行危险和风险评估,来确定每个仪表安全功能的安全功能要求和安全完整性等级。

注:风险降低方法的总览见图9。

o) 为安全完整性等级确立了在要求时的平均失效概率和每小时的危险失效频率的数值目标。

p) 规定了硬件故障裕度的最低要求。

q) 规定了实现要求的完整性等级所要求的技术/措施。

r) 确定了根据 GB/T 21109 实现的仪表安全功能所能达到的最高性能水平(SIL 4)。

s) 确定了低于此水平时 GB/T 21109 就不适用的最低性能水平(SIL 1)。

t) 提供了用来确定安全完整性等级的一个框架,但并不规定特定应用要求的安全完整性等级(它应根据特定应用的知识来确定)。

u) 规定了安全仪表系统各部分(从传感器到最终元件)的要求。

v) 定义了安全生命周期内所需的信息。

w) 要求仪表安全功能的设计应考虑人为因素。

x) 不对个别操作员或维护人员提任何直接的要求。

本部分的系统、硬件和软件的关系见图 5。

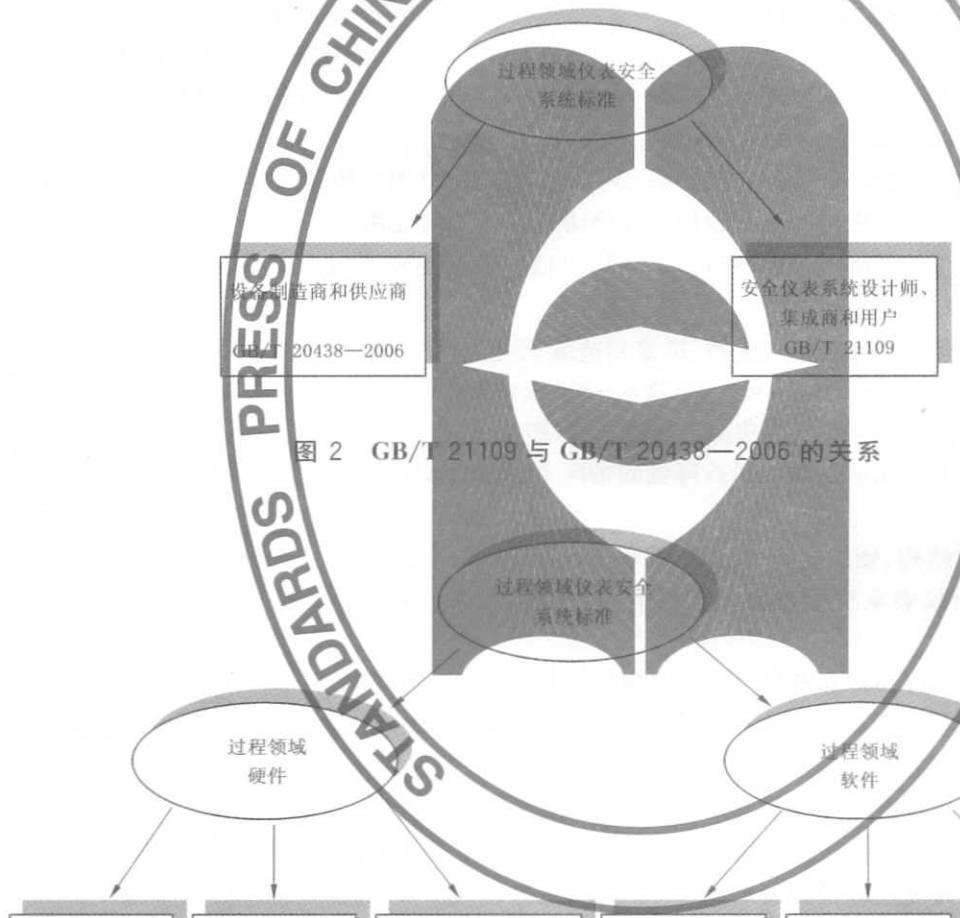


图 2 GB/T 21109 与 GB/T 20438—2006 的关系

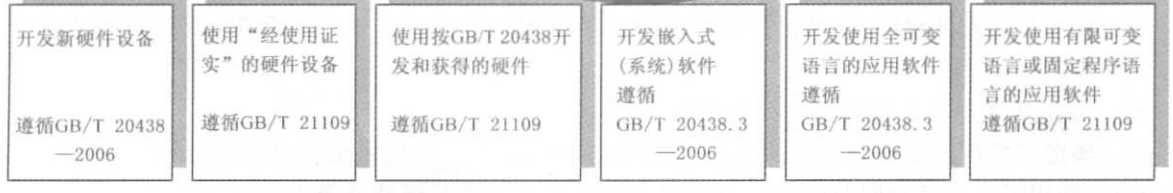


图 3 GB/T 21109 与 GB/T 20438—2006 的关系(见第 1 章)

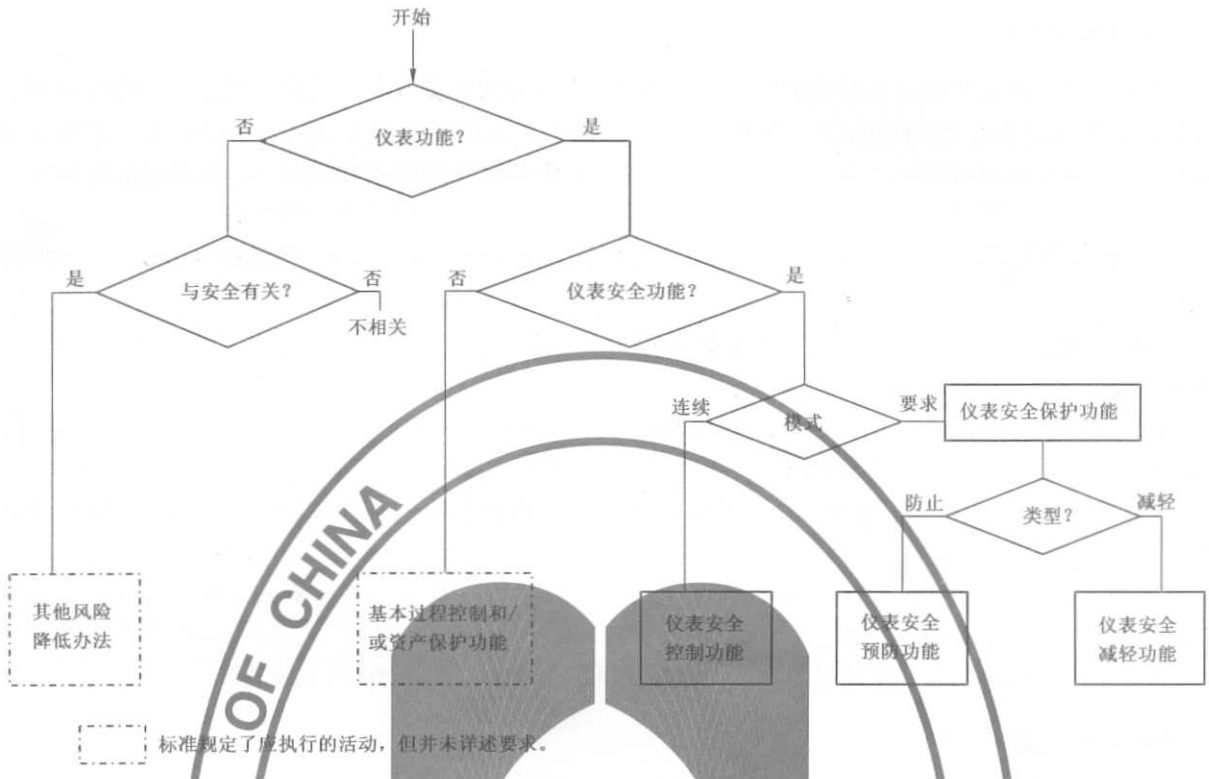


图 4　仪表安全功能和其他功能的关系

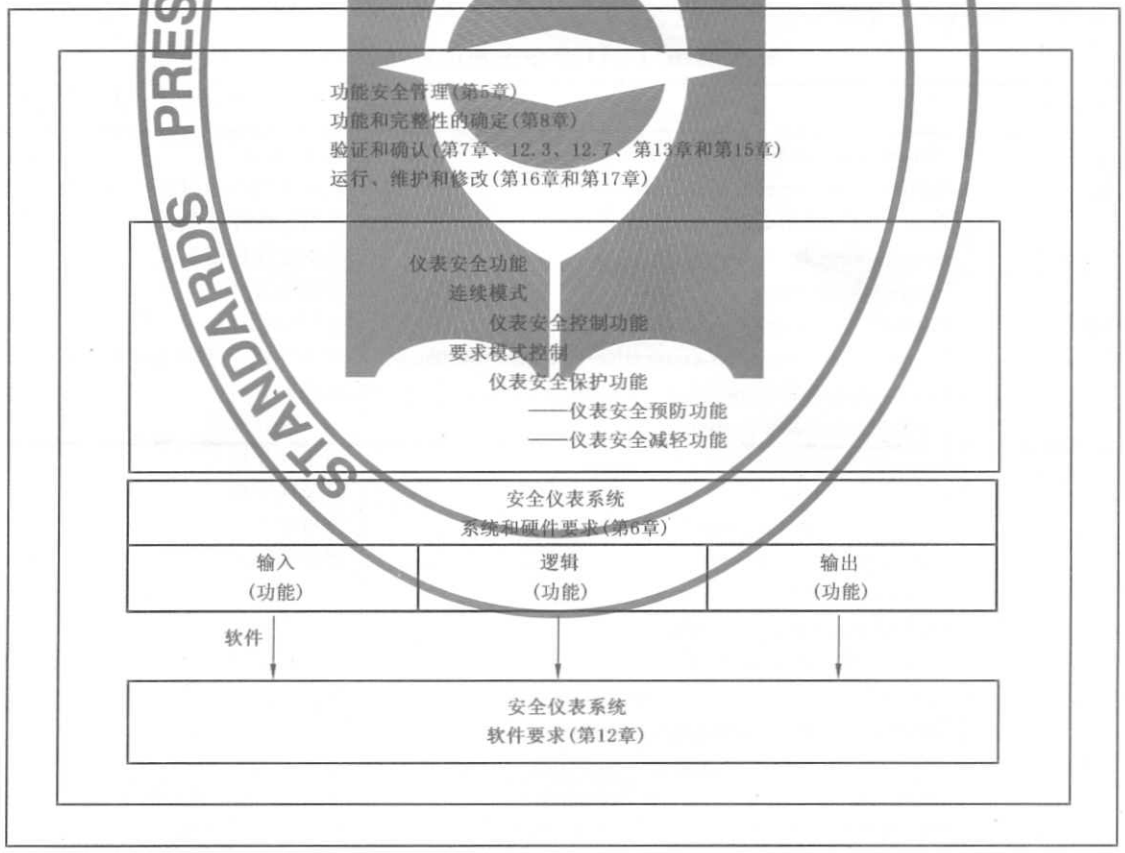


图 5　本部分的系统、硬件和软件的关系

2 规范性引用文件

下列文件中的条款通过GB/T 21109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 17214.1—1998 工业过程测量和控制装置工作条件 第1部分：气候条件(idt IEC 60654-1:1993)

GB/T 18268—2000 测量、控制和实验室用的电设备 电磁兼容性要求(idt IEC 61326-1:1997, Amd.1:1998)

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

GB/T 20438.3—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 21109.2—2007 过程工业领域安全仪表系统的功能安全 第2部分：GB/T 21109.1的应用指南(IEC 61511-2:2003,IDT)

IEC 60654-3:1998 工业过程测量和控制设备的运行条件 第3部分：机械影响

3 缩略语和定义

3.1 缩略语

GB/T 21109使用的缩略语见表1。

表1 GB/T 21109中使用的缩略语

缩略语	全 称	解 释
AC/DC	Alternating current/direct current	交流/直流
ALARP	As low as reasonably practicable	在合理可行的前提下尽可能低
ANSI	American National Standards Institute	美国国家标准学会
BPCS	Basic process control system	基本过程控制系统
DC	Diagnostic coverage	诊断覆盖率
E/E/PE	Electrical/electronic/programmable electronic	电气/电子/可编程电子
E/E/PES	Electrical/electronic/programmable electronic system	电气/电子/可编程电子系统
EMC	Electro-magnetic compatibility	电磁兼容性
FAT	Factory acceptance testing	工厂验收测试
FPL	Fixed program language	固定程序语言
FTA	Fault tree analysis	故障树分析
FVL	Full Variability language	全可变语言
HFT	Hardware fault tolerance	硬件故障裕度
HMI	Human manchine interface	人-机接口
H&RA	Hazard and risk assessment	危险和风险评估
HRA	Human reliability analysis	人员可靠性分析
H/W	Hardware	硬件
IEC	International Electrotechnical Commission	国际电工委员会
IEV	International Electrotechnical Vocabulary	国际电工词汇
ISA	Instrumentation, systems and Automation Society	仪表、系统和自动化学会
ISO	International Organization for Standardization	国际标准化组织
LVL	Limited variability language	有限可变语言
MooN	"M"out of "N"(see 3.2.45)	从"N"中取"M"(见3.2.45)
NP	Non-programmable	非可编程

表 1(续)

缩略语	全　称	解　释
PE	Programmable electronics	可编程电子
PES	Programmable electronic system	可编程电子系统
PFD	Probability of failure on demand	要求时的失效概率
PFD_{avg}	Average probability of failure on demand	要求时的平均失效概率
PLC	Programmable logic controller	可编程逻辑控制器
SAT	Site acceptance test	现场验收测试
SFF	Safe failure fraction	安全失效分数
SIF	Safety instrumented function	仪表安全功能
SIL	Safety integrity level	安全完整性等级
SIS	Safety instrumented system	安全仪表系统
SRS	Safety requirement specification	安全要求规范
S/W	Software	软件

3.2　术语和定义

下列术语和定义适用于本部分。

3.2.1

结构　architecture

系统中硬件和/或软件元素的安排，如：

a)　安全仪表系统(SIS)子系统的安排；

b)　SIS 子系统的内部结构；

c)　软件程序的安排。

注：本术语的定义同 GB/T 20438.4—2006 中的定义有差别，从而反映出过程领域术语中的差异。

3.2.2

资产保护　asset protection

为防止资产损失分配给系统设计的功能。

3.2.3

基本过程控制系统　basic process control system;BPCS

对来自过程的、系统相关设备的、其他可编程系统的和/或某个操作员的输入信号进行响应，并产生使过程和系统相关设备按要求方式运行的系统，但它并不执行任何具有被声明的 SIL≥1 的仪表安全功能。

注：见 A.2。

3.2.4

通道　channel

独立执行一个功能的一个或一组元素。

注 1：一个通道中的元素可能包括输入/输出(I/O)模块、逻辑系统(见 3.2.40)、传感器、最终元件。

注 2：一个双通道配置是指一个具有两个能独立执行相同功能的通道配置。

注 3：本术语可用来描述整个系统或者系统的一部分(如传感器或者最终元件)。

3.2.5

编码　coding

见 3.2.57。

3.2.6 **共同失效**

3.2.6.1

共同原因失效 common cause failure

由一个或多个事件引起一个多通道系统中的两个或多个分离通道失效，从而导致系统失效的一种失效。

3.2.6.2

共同模式失效 common mode failure

两个或多个通道以同样的方式引起相同的误差结果的失效。

3.2.7

部件 component

执行某一特定功能的系统、子系统或装置的一个组成部分。

3.2.8

配置 configuration

见3.2.1。

3.2.9

配置管理 configuration management

为了在生命周期全过程中控制组件的变化(硬件和软件)和保持连续性和可追溯性，对进化系统(硬件和软件)中组件的识别规则。

3.2.10

控制系统 control system

对来自过程和/或操作员的输入信号进行响应，并产生使过程按要求方式运行的输出信号的系统。

注：控制系统包括输入装置和最终元件，它可以是一个BPCS，也可以是一个SIS，或者二者的组合。

3.2.11

危险失效 dangerous failure

可能使安全仪表系统潜在地处于某种危险或功能丧失状态的失效。

注：这种可能性是否变为现实可能取决于系统的通道结构，在用来提高安全性的多通道系统中，一个危险硬件失效很少能导致整体危险或功能丧失状态。

3.2.12

相关失效 dependent failure

其概率不能表示为引起失效的独立事件的无条件概率的简单乘积的失效。

注1：仅当$P(A\text{ 和 }B)>P(A)\times P(B)$时，两个事件A和B才是相关的。$P(Z)$是事件Z的概率。

注2：考虑保护层当中相关失效的例子见9.5。

注3：相关失效包括共同原因失效(见3.2.6)。

3.2.13

检测到的 detected

揭露的 revealed

明显的 overt

在与硬件失效和软件故障有关时，通过诊断测试或正常操作发现的。

3.2.14

装置 device

能实现某个规定目的的硬件或软件或者二者结合的功能单元(如现场装置，同SIS I/O端的现场侧面连接的设备，这些设备包括现场接线、传感器、最终元件、逻辑解算器和硬接线到SIS I/O端的操作员接口装置)。

3.2.15

诊断覆盖率 diagnostic coverage:DC

诊断测试检测到的部件或子系统的失效率与总失效率之比。诊断覆盖率不包含由检验测试检测到的任何故障。

注1：诊断覆盖率用于从总失效率($\lambda_{总失效率}$)计算检测到的失效率($\lambda_{检测到的}$)和未检测到的失效率($\lambda_{未检测到的}$)：$\lambda_{检测到的}=DC\times\lambda_{总失效率}$ 和 $\lambda_{未检测到的}=(1-DC)\times\lambda_{总失效率}$。

注2：诊断覆盖率适用于安全仪表系统的部件或子系统。如：典型地对于传感器、最终元件或逻辑解算器需确定其诊断覆盖率。

注3：对安全应用，典型的诊断覆盖率可适用于一个部件或子系统的安全失效和危险失效。如：一个部件或子系统的危险失效的诊断覆盖率为 $DC=\lambda_{DD}/\lambda_{DT}$，式中 λ_{DD} 是检测到的危险失效率，λ_{DT} 是总的危险失效率。

3.2.16

多样性 diversity

执行一个要求功能存在不同方法。

注：可用不同的物理方法或不同的设计途径来实现多样性。

3.2.17

电气/电子/可编程电子 electrical/electronic/programmable electronic:E/E/PE

基于电气(E)和/或电子(E)和/或可编程电子(PE)技术。

注：打算用本术语来覆盖以电原理工作的任一和所有装置或系统，它包括：

——机电装置(电气)；

——固态电子或可编程电子装置(电子)；

——基于计算机技术的电子装置(可编程电子)(见3.2.55)。

3.2.18

误差 error

计算出的、观测到的和测量到的值或条件，和真实的、规定的或理论上正确的值或条件之间的差异。

注：采用IEV 191-05-24中的定义但不包括注。

3.2.19

外部风险降低设施 external risk reduction facilities

与SIS分离且性质不同的降低或减少风险的措施。

注1：如排放系统、防火墙、堤(坝)。

注2：本术语的定义同GB/T 20438.4—2006中的定义有差别，从而反映出过程领域术语中的差异。

3.2.20

失效 failure

功能单元执行一个要求功能的能力的终止。

注1：本定义(除注外)同ISO/IEC 2382-14-01-09:1997相符。

注2：另外的信息见GB/T 20438.4—2006。

注3：要求的功能特性必需排除某些行为，并根据应避免的行为来规定某些功能。这些行为的出现就是失效。

注4：失效或是随机的或是系统的(见3.2.62和3.2.85)。

3.2.21

故障 fault

可能引起功能单元执行要求功能的能力降低或丧失的异常状况。

注：IEV 191-05-01定义"故障"是一种无能力执行要求功能的状态，不包括预防性维护、或其他计划行动的期间的无能力，或外部资源缺少产生的无能力[ISO/IEC 2382-14-01-09]。

3.2.22

故障避免 fault avoidance

在安全仪表系统安全生命周期的任何阶段中为避免引入故障而使用的技术和程序。

3.2.23

故障裕度　fault tolerance

在出现故障或误差的情况下，功能单元继续执行要求功能的能力。

注：IEV 191-15-05 中的定义仅指子项目故障。见 3.2.21 的注[ISO/IEC 2382-14-04-06]。

3.2.24

最终元件　final element

执行实现某种安全状态所必需的实际动作的安全仪表系统的组成部分。

注：例如阀门、开关装置、电机及其附属元件，如仪表安全功能中的电磁阀和执行机构。

3.2.25

功能安全　functional safety

与过程和 BPCS 有关的整体安全的组成部分，它取决于 SIS 和其他保护层的正确功能执行。

注：本术语的定义同 GB/T 20438.4—2006 中的定义有差别，从而反映出过程领域术语中的差异。

3.2.26

功能安全评估　functional safety assessment

基于证据的调查，以判定由一个或多个保护层所实现的功能安全。

注：本术语的定义同 GB/T 20438.4—2006 中的定义有差别，从而反映出过程领域术语中的差异。

3.2.27

功能安全审核　functional safety audit

对于按计划安排的功能安全要求专用的规范是否有效地执行并满意地达到规定目的进行系统地、独立的检查。

注：功能安全审核可以作为功能安全评估的一部分。

3.2.28

功能单元　functional unit

能够完成规定目的的软件、硬件或两者相结合的实体。

注 1：在 IEV 191-01-01 中，常用“项目(item)”一词代替功能单元，一个项目有时可能包括人员在内。

注 2：本定义是在 ISO/IEC 2382-14-01-01 中给出的定义。

3.2.29

硬件安全完整性　hardware safety integrity

在危险失效模式中，与硬件随机失效有关的仪表安全功能的安全完整性的一部分。

注 1：此术语与危险模式中的失效有关，即有损于安全完整性的仪表安全功能的那些失效。与本术语中有关的两个参数是总危险失效率和要求时操作失效率。

注 2：见 3.2.86。

注 3：本术语的定义同 GB/T 20438.4—2006 中的定义有差别，从而反映出过程领域术语中的差异。

3.2.30

伤害　harm

由财产或环境的破坏而直接或间接导致的人身伤害或人体健康的损害。

注：此定义同 ISO/IEC 指南 51 相符。

3.2.31

危险　hazard

伤害的潜在根源。

注 1：此定义同 ISO/IEC 指南 51 的 3.4 相符。

注 2：本术语包括短时内发生的对人员的威胁(如着火或爆炸)，以及对人体健康长时间有影响的那些威胁(如有毒物质的释放)。

3.2.32

人为误差　human error

失误　mistake

引发非期望结果的人的动作或不动作。

注：本定义是以 ISO/IEC 2382-14-02-03 为基础，并与 IEV 191-05-25 给出的不同，它增加了“或不动作”。

3.2.33

影响分析　impact analysis

确定一个系统中的一个功能或部件的改变，对该系统和其他系统中其他功能或部件影响的活动。

3.2.34

独立部门　independent department

在进行安全评估或确认的安全生命周期的特定阶段中，同负责所发生活动的部门分开且不同的部门。

3.2.35

独立组织　independent organization

在进行安全评估或确认的安全生命周期的特定阶段中，通过管理和其他资源同负责所发生活动的组织分开且不同的组织。

3.2.36

独立人员　independent person

在进行安全评估或确认的安全生命周期的特定阶段中，同所发生活动分开且不同的人员，这些人员并不直接负责那些活动。

3.2.37

输入功能　input function

为了给逻辑解算器提供输入信息，监视过程及其相关设备的功能。

注：输入功能可以是手动功能。

3.2.38

仪表　instrument

在执行某个动作中使用的仪器（典型的可见仪表系统）。

注：过程领域中，仪表系统典型地由传感器（如压力、流量、温度变送器）、逻辑解算器或控制系统（如可编程控制器、分散型控制系统）和最终元件（如控制阀）组成。在特殊情况下，仪表系统可能是安全仪表系统（见 3.2.72）。

3.2.39

逻辑功能　logic function

在输入信息（由一个或几个输入功能提供）和输出信息（由一个或几个输出功能使用）之间执行变换的功能；逻辑功能提供从一个或几个输入功能到一个或几个输出功能的转换。

注：另见 GB/T 15969.3 和 IEC 60617-12。

3.2.40

逻辑解算器　logic solver

既可以是一个 BPCS 的一部分，也可以是 SIS 的一部分，它执行一个或几个逻辑功能。

注 1：在 GB/T 21109 中，逻辑系统使用了以下术语：

——机电技术的电气逻辑系统；

——电子技术的电子逻辑系统；

——可编程电子系统的可编程逻辑系统。

注 2：例如：电气系统、电子系统、可编程电子系统、气动系统、液压系统。传感器和最终元件不是逻辑解算器的组成部分。

3.2.40.1

安全配置的逻辑解算器 safety configured logic solver

根据11.5为在安全应用中使用专门配置的工业级通用型PE逻辑解算器。

3.2.41

维护/工程接口 maintenance/engineering interface

为能正确维护或修改SIS所提供的硬件和软件。包括:在软件中可能含有的指令和诊断程序、具有适当通信协议的编程终端、诊断工具、指示器、旁路装置、试验装置和校正装置。

3.2.42

减轻 mitigation

减小危险事件后果的动作。

注:例如,根据已证实的着火或气体泄漏的检测所采取的紧急减压。

3.2.43

操作模式 mode of operation

仪表安全功能运行方式。

3.2.43.1

要求模式下的仪表安全功能 demand mode safety instrumented function

响应过程条件或其他要求而采取一个规定动作(如关闭一个阀门)的场合,在仪表安全功能的危险失效事件中,仅当发生过程或BPCS的失效事件时,才发生潜在危险。

3.2.43.2

连续模式下的仪表安全功能 continuous mode safety instrumented function

在仪表安全功能的危险失效事件中,如果不采取预防动作,即使没有进一步的失效,潜在危险也会发生。

注1:连续模式覆盖了实现连续控制以保持功能安全的那些仪表安全功能。

注2:要求模式应用中,在要求率的频率大于每年1次的情况下,危险率不高于仪表安全功能的危险失效率。在这种情况下,通常适宜使用连续模式准则。

注3:表3和表4定义了运行在要求模式和连续模式下的仪表安全功能的目标失效量。

注4:本术语的定义同GB/T 20438.4—2006中的定义有差别,从而反映出过程领域术语中的差异。

3.2.44

模块 module

执行某个特定硬件功能的硬件部件的自含式组件(即数字输入模块、模拟输出模块),或支持某一特定功能的可重用应用程序(可能是一个或一组内固程序)。如执行特定功能的计算机程序的一部分。

注1:在GB/T 15969.3中,软件模块是一个功能或功能块。

注2:本术语的定义同GB/T 20438.4—2006中的定义有差别,从而反映出过程领域术语中的差异。

3.2.45

从N中取M MooN

"N"个独立通道构成的安全仪表系统或其部分,它被连接成其中"M"个通道足以执行仪表安全功能。

3.2.46

必要的风险降低 necessary risk reduction

为保证把风险降低到允许水平所需的风险降低。

3.2.47

非可编程(NP)系统 non-programmable (NP) system

基于非计算机技术的系统(即不基于可编程电子[PE]或软件的系统)。

注:例如,硬接线电气或电子系统,机械、液压或气动系统。

3.2.48

操作员接口 operator interface

在操作人员和SIS之间进行信息交换的手段(如阴极射线管CRT、指示灯、按钮、操纵杆、报警器);操作员接口有时又叫人机接口(HMI)。

3.2.49

其他技术安全相关系统 other technology safety related system

不基于电气、电子或可编程电子技术的安全相关系统。

注:安全阀就是"另一种技术的安全相关系统"。"其他技术安全相关系统"可以包括液压和气动系统。

3.2.50

输出功能 output function

根据来自逻辑功能的终端执行机构的信息,控制过程及其相关设备的功能。

3.2.51

阶段 phase

发生GB/T 21109中描述活动的安全生命周期中的某个时段。

3.2.52

预防 prevention

降低危险事件发生频率的动作。

3.2.53

以往使用 prior use

见3.2.36。

3.2.54

过程风险 process risk

因异常事件(包括BPCS功能失常)引起过程条件产生的风险。

注1:本文中的风险与使用SIS提供必要的风险降低的特定危险事件有关(即与功能安全相关的风险)。

注2:GB/T 21109.3中描述了过程风险分析。确定过程风险的主要目的是给予考虑保护层的风险确立一个参考点。

注3:过程风险的评估应包括相关人为因素问题。

注4:本术语相当于GB/T 20438.4—2006中的"受控设备(EUC)风险"。

3.2.55

可编程电子 programmable electronics;PE

基于计算机技术构成PES一部分的电子部件或装置。本术语包括硬件和软件及输入和输出单元。

注1:本术语覆盖基于一个或几个中央处理单元(CPU)及相关的存储器的微电子设备。过程领域可编程电子的例子包括:

——智能传感器和最终元件。

——可编程电子逻辑解算器,包括:

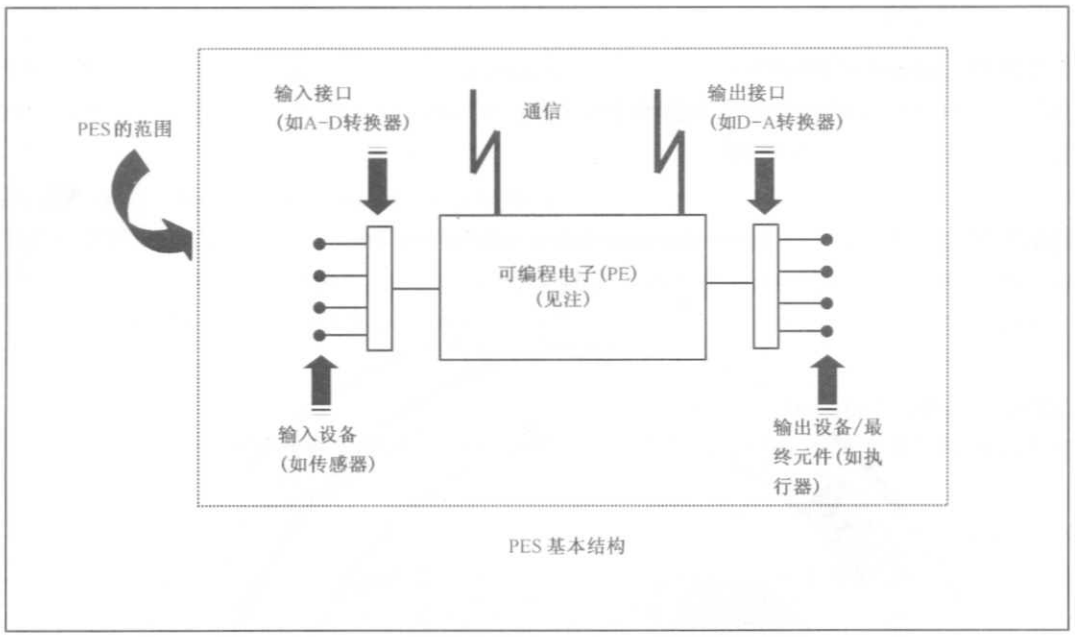
- 可编程控制器;
- 可编程逻辑控制器;
- 回路控制器。

注2:本术语的定义同GB/T 20438.4—2006中的定义有差别,从而反映出过程领域术语中的差异。

3.2.56

可编程电子系统 programmable electronic system;PES

基于一个或多个可编程电子装置的,用于控制、防护或监视的系统,包括系统中所有的元素,如电源、传感器和其他输入装置、数据高速公路和其他通信途径以及执行器和其他输出装置(见图6)。



注：可编程电子位于图中心位置，但在PES中可位于几个不同的位置。

图6 可编程电子系统(PES)：结构和术语

3.2.57

编程 programming

为解决问题或处理数据而设计、编写和测试一组指令的过程。

注：GB/T 21109中，编程典型地同可编程电子(PE)相关。

3.2.58

检验测试 proof test

为揭露安全仪表系统中未检测到的故障而执行的测试，以便在必要时把系统修复到所设计的功能。

3.2.59

保护层 protection layer

借助控制、预防或减轻以降低风险的任何独立机制。

注：它可能是装危险化学物品的压力容器的容量这样的一个过程工程机制，也可能是一个安全阀这样的机械工程机制，或者一个安全仪表系统，或者是应对紧急危险的一个应急计划这样的管理规程。可以自动启动或手动启动这些响应机制(见图9)。

3.2.60

经使用验证的 proven-in-use

当文档化的评估显示有适当证据表明：基于部件以往使用的情况，该部件适用于安全仪表系统时(见11.5中的“以往使用”)。

注：本术语的定义同GB/T 20438有差别，从而反映出过程领域技术的差异。

3.2.61

质量 quality

一个实体满足指明的和隐含需要的性能总和。

注：更多的情况见ISO 9000。

3.2.62

硬件随机失效 random hardware failure

在硬件中，由各种退化机制引起，以随机时间发生的失效。

注1：在不同部件中存在以不同速率发生的许多退化机制。因为在工作不同的时间之后，由于这些机制，制造公差

会引起部件故障;所以包含许多部件的整个设备的失效将以可预见的速率发生,而发生的时间却是不可预见的(即是随机的)。

注2:硬件随机失效和系统失效(见3.2.85)特征之间的主要差别在于硬件随机失效引起的系统失效率(或其他相应的量)能被预测,而由固有特性产生的系统失效则不可预测。即硬件随机失效引起的系统失效率可被量化,而由系统失效引起的系统失效率则因导致系统失效的事件不易被预测而不能进行统计量化。

3.2.63

冗余 redundancy

使用多个元素或系统来执行同一种功能;冗余可以使用同种元素实现(同型冗余),或使用不同元素实现(异型冗余)。

注1:例如,使用重复功能部件和附加奇偶校验位。

注2:冗余主要用来提高可靠性或可用性。

注3:IEV 191-15-01中的定义不太完全[ISO/IEC 2382-14-01-11]。

注4:本术语的定义同GB/T 20438.4—2006中的定义有差别,从而反映出过程领域术语中的差异。

3.2.64

风险 risk

出现伤害的概率及该伤害严重性的组合。

注:有关本概念的其他讨论见第8章。

3.2.65

安全失效 safe failure

不会使安全仪表系统处于潜在的危险状态或功能故障状态的失效。

注1:潜在是否成为现实可能取决于系统通道结构。

注2:安全失效又称为扰乱性失效(nuisance failure)、假错误失效(spurious trip failure)、伪错误失效(false trip failure)或者故障安全失效(fail-to-safe failure)。

3.2.65.1

安全失效分数 safe failure fraction

导致安全失效或者可检测出的危险失效的装置总硬件随机失效率分数。

3.2.66

安全状态 safe state

达到安全时的过程状态。

注1:从某个潜在的危险工况达到最终的安全状态,过程可能不得不经过几个中间安全状态。在有些情况下,仅当过程处于连续控制时才存在安全状态。这样的连续控制可能是短时间的或是不确定的时段。

注2:本术语的定义同GB/T 20438.4—2006中的定义有差别,从而反映出过程领域术语中的差异。

3.2.67

安全 safety

不存在不可接受的风险。

注:本定义依据是ISO/IEC指南51。

3.2.68

安全功能 safety function

针对特定的危险事件,为达到或保持过程的安全状态,由SIS、其他技术安全相关系统或外部风险降低设施实现的功能。

注:本术语的定义同GB/T 20438.4—2006中的定义有差别,从而反映出过程领域术语中的差异。

3.2.69

仪表安全控制功能 safety instrumented control function

具有某个规定的SIL并运行在连续模式下,以防止发生危险工况和/或减轻其后果所必需的仪表安全功能。

3.2.70

仪表安全控制系统　safety instrumented control system

用来实现一个或几个仪表安全控制功能的仪表系统。

注：在过程工业中，仪表安全控制系统是少见的。在对待这种系统时，应把它们当成一种特殊情况处理，进行个案设计。应使用 GB/T 21109 中的要求，但需要更详细的分析以证明系统能够达到安全要求。

3.2.71

仪表安全功能　safety instrumented function;SIF

具有某个特定 SIL 的，用以达到功能安全的安全功能，它既可以是一个仪表安全保护功能，也可以是一个仪表安全控制功能。

3.2.72

安全仪表系统　safety instrumented system;SIS

用来实现一个或几个仪表安全功能的仪表系统。SIS 可以由传感器、逻辑解算器和最终元件的任何组合组成(示例见图 7)。

注 1：它可包含仪表安全控制功能，也可包含仪表安全保护功能，或包含这两者。

注 2：SIS 装置制造商和供应商应参见第 1 章 a)～d)。

注 3：SIS 可以包括或不包括软件。

注 4：见 A.2。

注 5：当人的动作是 SIS 的一部分时，操作员动作的可用性和可靠性在 SRS 中规定，并且包含在 SIS 性能计算中。在 SIL 计算中如何包含操作员动作的可用性和可靠性的指南见 GB/T 21109.2。

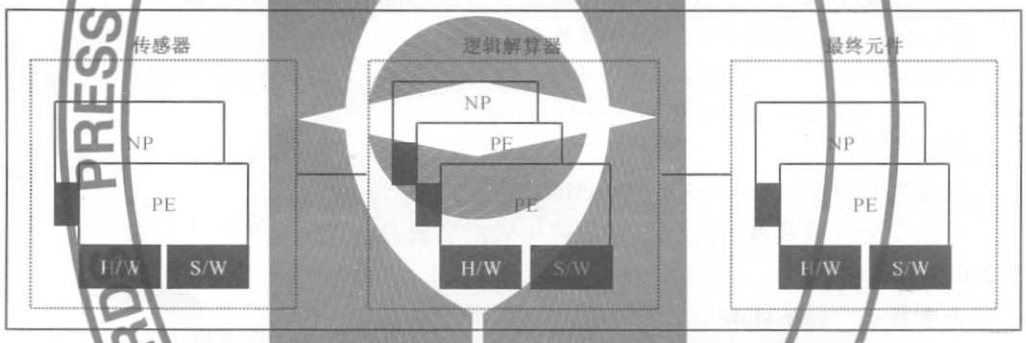


图 7　SIS 结构示例

3.2.73

安全完整性　safety integrity

安全仪表系统在规定时段内、在所有规定条件下满足执行要求的仪表安全功能的平均概率。

注 1：安全完整性等级越高，应执行所要求的仪表安全功能的概率也越高。

注 2：仪表安全功能的安全完整性等级分成 4 个等级。

注 3：在确定安全完整性时，应包括导致非安全状态的所有失效因素(硬件随机失效和系统失效)，如：硬件失效、软件导致的失效和电气干扰引起的失效。这些类型中的某些失效，特别是硬件随机失效，可以使用危险失效模式中的失效率或者要求时的仪表安全功能失效概率这样的量来量化。但 SIF 的安全完整性还取决于许多因素，它们不能精确量化，只能定性考虑。

注 4：安全完整性由硬件安全完整性和系统安全完整性组成。

3.2.74

安全完整性等级　safety integrity level;SIL

用来规定分配给安全仪表系统的仪表安全功能的安全完整性要求的离散等级(4 个等级中的一个)。SIL 4 是安全完整性的最高等级，SIL 1 为最低等级。

注 1：安全完整性等级的目标失效量见表 3 和表 4。

注 2：有可能使用几个安全完整性等级较低的系统来满足一个较高安全完整性等级功能的需要(例如：使用一个

SIL 2 和一个 SIL 1 的系统共同来满足一个 SIL 3 功能的需要)。

注 3：本术语的定义同 GB/T 20438.4—2006 中的定义有差别，从而反映出过程领域术语中的差异。

3.2.75

安全完整性要求规范　safety integrity requirements specification

包含了安全仪表系统应执行的仪表安全功能的安全完整性要求的规范。

注 1：本规范是安全要求规范的一部分(安全完整性部分)(见 3.2.78)。

注 2：本术语的定义同 GB/T 20438.4—2006 中的定义有差别，从而反映出过程领域术语的差异。

3.2.76

安全生命周期　safety life cycle

从项目概念阶段开始到所有的仪表安全功能不再适用时为止所发生的、包含在仪表安全功能实现中的必要活动。

注 1：严格地讲，术语“功能安全生命周期”更为准确，但从 GB/T 21109 上下文来看可不必考虑形容词“功能(的)”。

注 2：GB/T 21109 中使用的安全生命周期模型见图 8。

3.2.77

安全手册　safety manual

定义如何安全使用装置、子系统或系统的手册。

注：安全手册可以是一份独立文档、一份说明书、一份编程手册、一份标准文档，或包含在定义应用限制的用户文档中。

3.2.78

安全要求规范　safety requirements specification

包含安全仪表系统应执行的仪表安全功能的所有要求的规范。

3.2.79

安全软件　safety software

在安全仪表系统中具有应用软件功能性、嵌入式软件功能性或工具软件功能性的软件。

3.2.80

传感器　sensor

测量过程条件的装置或装置组合(如：变送器、传感器、过程开关和定位开关)。

3.2.81

软件　software

包括程序、进程、数据、规则和关于数据处理系统操作的相关文档的智能创作。

注 1：软件与记录它的媒体无关。

注 2：没有注 1 的本定义与 ISO 2382-1 不同，整个定义与 ISO 9000-3 的不同之处在于增加了词“数据”。

3.2.81.1　**SIS 子系统中的软件语言**

3.2.81.1.1

固定程序语言　fixed program language：FPL

限定用户只能调整几个参数(如压力变送器的量程、报警等级和网络地址)的语言类型。

注：使用 FPL 的装置的典型例子是：智能传感器(如压力变送器)、智能阀、事件时序控制器、专用智能报警盒和小型数据录入系统。

3.2.81.1.2

有限可变语言　limited variability language：LVL

被设计成过程领域用户容易理解并可为实现安全要求规范提供组合预定的、应用专用的库功能能力的一种语言类型。LVL 可提供一种与达到应用所要求的功能几乎一致的功能。

注 1：GB/T 15969.3 中给出了 LVL 的典型示例。它们包括梯形图、功能块图和顺序功能图。

注 2：使用 LVL 系统的典型示例：标准 PLC(如熔炉管理用的可编程逻辑控制器)。

3.2.81.1.3

全可变语言　full variability language;FVL

设计成计算机编程者易于理解，并可提供实现各种各样功能和应用的能力的一种语言。

注1：使用FVL的系统的典型例子是通用型计算机。

注2：在过程领域中，嵌入式软件常用FVL，而应用软件则很少使用FVL。

注3：FVL的例子包括：Ada、C、Pascal、指令表、汇编程序语言、C++、Java和SQL。

3.2.81.2　**软件程序类型**

3.2.81.2.1

应用软件　application software

用户应用专用软件。通常，它包含控制正确输入、输出、计算和决策的逻辑时序、允许值、极值和表达式，用以满足仪表安全功能所必须的要求。参见固定程序语言和有限可变语言。

3.2.81.2.2

嵌入式软件　embedded software

作为系统组成部分由制造商提供的软件，最终用户不能对其进行修改。嵌入式软件又叫固件或系统软件。见3.2.81.1.3。

3.2.81.2.3

工具软件　utility software

用来创建、修改和编写应用程序的软件工具。操作SIS并不需要这些软件工具。

3.2.82

软件生命周期　software life cycle

从开始构思软件到永久性停用软件期间发生的活动。

注1：一个典型的软件生命周期包括需求、开发、测试、集成、安装和修改等阶段。

注2：软件不能被维护，但可以被修改。

3.2.83

子系统　subsystem

见3.2.84。

3.2.84

系统　system

根据设计相互联系的一组元素；系统的一个元素可以是称为子系统的另一系统，该子系统可以是一个主控系统，也可以是一个受控系统，它可能包含硬件、软件和人的交互作用。

注1：人可以是系统的一部分。

注2：本定义不同于IEV 351-01-01。

注3：系统包括传感器、逻辑解算器、最终元件、通信和附属于SIS的辅助设备(如：电缆、管道系统和电源)。

3.2.85

系统失效　systematic failure

与某种起因以确定性方式有关的失效，只有对设计或制造过程、操作规程、文档或其他相关因素进行修改才能消除这种失效。

注1：仅凭借正确维护而不作修改通常不能消除失效起因。

注2：通过模拟失效起因能引发系统失效。

注3：本定义(注2以上)与IEV 191-04-19一致。

注4：系统失效起因的例子包括以下各项中的人为误差：

——安全要求规范；

——硬件的设计、制造、安装和操作；

——软件的设计和/或实现。

3.2.86

系统安全完整性　systematic safety integrity

在失效的危险模式中与系统失效(见 3.2.73 的注 3)有关的仪表安全功能的安全完整性部分。

注 1：系统安全完整性通常不能被量化(不同于硬件安全完整性)。

注 2：另见 3.2.29。

3.2.87

目标失效量　target failure measure

就安全完整性要求而言，应达到的预计危险模式失效概率，既可规定为要求时执行设计功能的平均失效概率(要求操作模式时)，也可规定为每小时执行 SIF 的危险失效频率(连续操作模式时)。

注：表 3 和表 4 给出了目标失效量的数值。

3.2.88

模板　template

软件模板　software template

保持原有结构的同时，易于改变以支持特定功能的结构化非专用应用软件段，例如：交互界面模板控制应用界面的过程流，但并非专用于正呈现的数据。程序员可以采用通用模板，并做特定功能修改，从而为用户生成一个新界面。

注：有时也使用相关术语“软件模板”。典型地，它指编程用于执行要求的一个或一组功能的一种算法或者算法集，并且它被构建成可在多个不同的事例中使用。在 GB/T 15969.3 中，它是可被选择用于多个应用的一个程序。

3.2.89

允许风险　tolerable risk

根据当今社会的水准，在给定范围内能够接受的风险。

注：见 GB/T 21109.3。

[ISO/IEC 指南 51]。

3.2.90

未检测到的　undetected

未揭露出的　unrevealed

不明显的　covert

与硬件和软件有关，未被诊断测试发现的或者在正常操作中未被发现的。

注：本术语的定义同 GB/T 20438.4—2006 中的定义有差别，从而反映出过程领域术语中的差异。

3.2.91

确认　validation

用以证明被考虑的仪表安全功能和安全仪表系统在安装之后，在各方面都能满足安全要求规范的活动。

3.2.92

验证　verification

在相关安全生命周期的每个阶段，通过分析和/或测试，证明对于特定的输入，输出应在各方面都能满足为该特定阶段所设置的目标和要求的活动。

注：验证活动的例子包括：

——为确保符合某阶段的目标和要求，考虑该阶段的特定输入，对其输出(来自安全生命周期所有阶段的文档)进行复审；

——设计复审；

——对设计的产品进行复审，以确保它们按规范工作；

——在系统各个部分分步组装到一起后进行集成测试，并进行环境性能试验以确保所有部分能按规定方式一起工作。

3.2.93

看门狗 watchdog

用来监视可编程电子(PE)装置正确运行,并能在检测到不正确运行时采取动作的诊断装置和输出装置(典型如开关)的组合。

注1:通过由软件控制的输出装置对外部装置(如硬件电子看门狗定时器)定期复位,看门狗可证实软件系统正确运行。

注2:当检测到危险失效时,为使过程进入某个安全状态,看门狗可用于断掉一组安全输出的电源。看门狗用于提高PE逻辑解算器的在线诊断覆盖率(见3.2.15和3.2.40)。

4 与GB/T 21109的符合性

为了符合GB/T 21109,应表明根据已规定的准则满足了第5章~第19章中列出的每项要求,因而也达到了各章的目的。

5 功能安全管理

5.1 目的

本章要求的目的是确定为确保满足功能安全目的所必需的管理活动。

注:本章的目的在于达到和保持安全仪表系统的功能安全,并且不同于为达到工作场所安全所需的通用健康和安全措施。

5.2 要求

5.2.1 概述

5.2.1.1 应确定实现安全的政策和策略连同评价达到它的方法,并在组织范围内进行交流。

5.2.1.2 安全管理系统应适当,以确保在使用安全仪表系统的场合下,它们能够把过程置于和/或保持在安全状态下。

5.2.2 组织和资源

5.2.2.1 应确定负责执行和复审每个安全生命周期阶段的人员、部门、组织或其他单位,并告知它们各自应负责的职责(包括相关的、发证的管理当局或安全法规团体)。

5.2.2.2 涉及安全生命周期活动的人员、部门或组织应能胜任执行它们所负责的活动。

注:当考虑安全生命周期活动中涉及的人员、部门、组织或其他单位的胜任能力时,至少应涉及以下各项:

a) 适合过程应用的工程知识、培训和经验;

b) 适合所使用应用技术的工程知识、培训和经验(如电气、电子或可编程电子);

c) 适合所使用传感器和最终元件的工程知识、培训和经验;

d) 安全工程知识(如过程安全分析);

e) 法律和安全法规要求的知识;

f) 适合其在安全生命周期中担当的角色的足够管理和领导技能;

g) 对事件潜在后果的理解;

h) 仪表安全功能的安全完整性等级;

i) 应用和技术的新颖性和复杂性。

5.2.3 风险评价和风险管理

应确定危险、评价风险和确定必要的风险降低,见第8章。

注:从经济角度来看,它可能也有助于考虑潜在的资金损失。

5.2.4 计划编制

应编制安全计划以确定要求执行的活动以及负责执行这些活动的人员、部门、组织或其他单位。在整个安全生命周期当中,必要时应重新编制安全计划(见第6章)。

注:安全计划编制可集成在:

——质量计划中名为"安全计划"的段;或

——名为"安全计划"的单独文档;或

——包含公司规程或作业指导书的几个文档。

5.2.5 执行和监视

5.2.5.1 应执行规程以确保即时跟踪和有关安全仪表系统的建议满意解决，这些建议来源于：

a) 危险分析和风险评估；

b) 评估和审核活动；

c) 验证活动；

d) 确认活动；

e) 事件后的和事故后的活动。

5.2.5.2 任何给全权负责安全生命周期一个或几个阶段的组织提供产品或服务的供应商，应按该组织的规定提供产品或服务，并应有质量管理系统。为了建立恰当的质量管理系统，这些规程应设置到位。

5.2.5.3 为了根据安全要求来评价安全仪表系统的性能，应执行下列方面的规程：

——确定和预防可能危及安全的系统失效；

——评估安全仪表系统的危险失效率是否符合设计中的假定值；

注1：通过检验测试、诊断或要求时操作失效可以揭示危险失效。

注2：应考虑规程来确定当失效率大于设计中的假定值时应采取的必要校正动作。

——在实际操作中，评估对仪表安全功能的要求率，以验证在确定完整性等级要求时进行风险评估所做的假设。

5.2.6 评估、审核和修改

5.2.6.1 功能安全评估

5.2.6.1.1 通过对安全仪表系统实现的功能安全和安全完整性做出判断，来定义和执行功能安全评估的规程。规程应要求指定包括特定安装所需的技术人员、应用和操作专家在内的评估小组。

5.2.6.1.2 评估组的成员至少应包括一位非工程项目设计组成员的高级资质人员。

注1：当评估组很大时，应考虑在组内包含多个与项目组无关的高级资质人员。

注2：在编制功能安全评估计划时，应考虑：

——功能安全评估的范围；

——参加功能安全评估的人员；

——功能安全评估组的技能、职责和权限；

——作为功能安全评估活动的结果所产生的信息；

——评估所涉及的任何其他安全团体的身份；

——为完成功能安全评估活动所要求的资源；

——评估组的独立水平；

——修改后重新确认功能安全评估的方法。

5.2.6.1.3 在安全计划编制过程中，应确定执行功能安全评估活动的安全生命周期阶段。

注1：当确定新的危险时，进行修改后和在操作间歇时，可能需要进行附加的功能安全评估活动。

注2：在以下阶段，应考虑执行功能安全评估活动(见图8)：

——阶段1：在已执行危险和风险评估、已确定要求的保护层和已制定安全要求规范之后；

——阶段2：在设计好安全仪表系统之后；

——阶段3：在完成安全仪表系统安装、预调试和最终确认，以及制定好操作和维护规程之后；

——阶段4：在取得操作和维护经验之后；

——阶段5：在对安全仪表系统进行修改之后和停用之前。

注3：功能安全评估活动的次数、规模和范围依赖于特定的情况。其决策因素大约包括：

——项目规模；

——复杂程度；

——安全完整性等级；

——项目持续时间；

——失效事件的后果；

——设计特征的标准化程度；

——安全规章制度的要求；

——相似设计的以往经验。

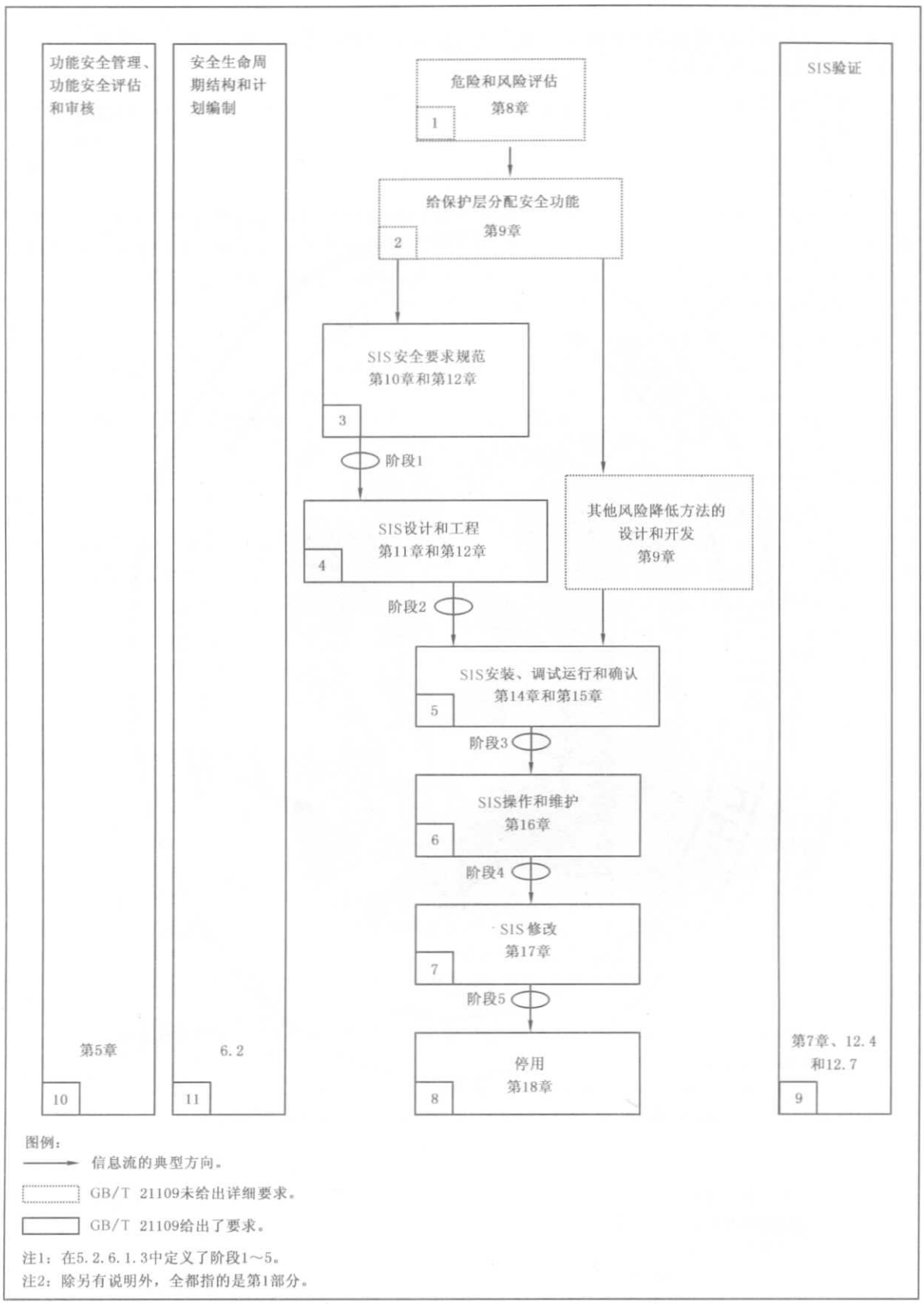


图 8 SIS 安全生命周期阶段和功能安全评估阶段

5.2.6.1.4 至少应执行一次功能安全评估。执行功能安全评估以确保能正确控制过程及其相关设备引起的危险。最低限度应在已被发现的危险成为现行之前(即阶段3)执行一次评估。在已被发现的危险成为现行之前,评估组应证实:

——已执行危险和风险评估(见8.1);

——已实现和解决由危险和风险评估提出的适用于安全仪表系统的建议;

——已到位并已正确执行项目设计更改规程;

——已解决由先前的功能安全评估提出的建议;

——根据安全要求规范设计、构造和安装安全仪表系统,已确认和解决任何差异;

——与安全仪表系统有关的安全、操作、维护和紧急规程都已到位;

——安全仪表系统确认计划编制是合适的并已完成确认活动;

——人员培训已完成,有关安全仪表系统的相应信息已提供给维护和操作人员;

——实现进一步功能安全评估的计划或策略已经就位。

5.2.6.1.5 当开发和生产工具被用于任何安全生命周期活动时,这些工具本身应进行功能安全评估。

注1:对这些工具的评估程度,取决于它们对所应达到的安全的影响。

注2:开发和生产工具包括例如:仿真和建模工具、测量设备、测试设备、维护活动中使用的设备和配置管理工具。

注3:工具的功能安全评估包括(但不限于):校准标准、操作历史和缺陷列表的可追溯性。

5.2.6.1.6 应提供功能安全评估的结果以及通过该评估提出的建议。

5.2.6.1.7 在必要时,所有相关信息都应能提供给功能安全评估组。

5.2.6.2 **审核和修订**

5.2.6.2.1 应按下列要求确定和执行审核规程:

——审核活动的频率;

——执行操作活动的人员、部门、组织或其他单位和执行审核活动的人员、部门、组织或其他单位之间的独立程度;

——记录和跟踪活动。

5.2.6.2.2 除非进行类型上的替换(即同类型替换),否则为启动、文档化、复审、实现和批准安全仪表系统的更改所需的修改规程的管理应到位。

5.2.7 **SIS配置管理**

5.2.7.1 **要求**

5.2.7.1.1 在SIS和软件安全生命周期阶段,应提供SIS配置管理规程;尤其是应规定:

——实现正式配置控制的阶段;

——用于惟一地标识一个项(硬件和软件)的所有组成部分的规程;

——防止未授权项进入服务的规程。

6 安全生命周期要求

6.1 目的

本章的目的是:

——定义和确定安全生命周期活动的各个阶段及要求;

——组织安全生命周期内的技术活动;

——确保有(或拟订有)适当的计划,以确保安全仪表系统能满足安全要求。

注:图8、图10和图11示出了GB/T 21109的整体方案。此方案只是用来说明并指出从初始构思一直到停用的典型安全生命周期活动。

6.2 要求

6.2.1 在编制安全计划过程中,应定义一个结合了GB/T 21109要求的安全生命周期。

6.2.2 应根据它的输入、输出和验证活动来定义安全生命周期的每个阶段(见表2)。

表2 SIS安全生命周期一览表

安全生命周期阶段或活动		目的	要求所在章或条	输入	输出
图8方框号	标题				
1	危险和风险评估	确定过程及相关设备的危险和危险事件、导致危险事件后果、与危险事件相关的过程风险、风险降低和要达到必要的风险降低所需要的安全功能要求	8	过程设计、布局、人员配备安排、安全目标	危险、要求的安全功能和相关风险降低的描述
2	给保护层分配安全功能	给保护层分配安全功能并为每个仪表安全功能分配相关的安全完整性等级	9	要求的仪表安全功能和相关安全完整性要求的描述	安全要求分配的描述(见第9章)
3	SIS安全要求规范	为了达到要求的安全功能,根据要求的仪表安全功能及其相关的安全完整性规定每个SIS的要求	10	安全要求分配的描述(见第9章)	SIS安全要求;软件安全要求
4	SIS设计和工程	设计SIS以满足仪表安全功能和安全完整性要求	11和12.4	SIS安全要求;软件安全要求	符合SIS安全要求的SIS设计;SIS集成测试的计划编制
5	SIS安装、调试运行和确认	集成和测试SIS;根据要求的仪表安全功能和要求的安全完整性,确认SIS在各方面都满足安全要求	12.3、14、15	SIS设计; SIS集成测试计划; SIS安全要求; SIS安全确认计划	完全能起作用并符合SIS设计的SIS;SIS集成测试的结果;安装、调试运行和确认活动的结果
6	SIS操作和维护	保证在操作和维护期间保持SIS的功能安全	16	SIS要求; SIS设计; SIS操作和维护计划	操作和维护活动的结果
7	SIS修改	对SIS进行校正、增强或自适应以保证达到和保持要求的安全完整性等级	17	修正过的SIS安全要求	SIS修改结果
8	停用	保证正确复审、部门组织确保SIF(继续恰当保留)	18	同建立的安全要求和过程信息一样	使SIF停止服务
9	SIS验证	测试和评估给定阶段的输出,确保其对于该阶段关于产品和标准输入的正确性和一致性	7、12.7	每个阶段SIS的验证计划	每个阶段SIS验证的结果
10	SIS功能安全评估	对SIS所达到的功能安全进行调查并作出判断	5	SIS功能安全评估计划编制、SIS安全要求	SIS功能安全评估结果

6.2.3 应编制安全生命周期所有阶段的安全计划，定义准则、技术、措施和程序，以：

——保证过程的所有相关模式都能达到 SIS 安全要求；这包括功能和安全完整性两个方面的要求；

——保证安全仪表系统正确安装和调试运行；

——保证安装后仪表安全功能的安全完整性；

——在操作(如检验测试、失效分析)过程中保持安全完整性；

——在安全仪表系统的维护活动期间管理过程危险。

7 验证

7.1 目的

本章的目的是通过复审、分析和/或测试，来证明要求的输出能满足在验证计划编制确定的安全生命周期的适当阶段(图 8)定义的要求。

7.1.1 要求

验证计划编制应定义安全生命周期的适当阶段(图 8)要求的所有活动。为了符合本部分，验证计划应提供以下各项：

——验证活动；

——验证所使用的程序、措施和技术，包括生成执行和解决方案建议；

——何时进行这些活动；

——负责这些活动的人员、部门和组织，包括它们的独立水平；

——确定要验证的项目；

——确定验证依据的信息；

——如何处理不一致性；

——工具和支持分析。

7.1.1.1 应根据验证计划进行验证。

7.1.1.2 验证过程的结果应可用。

注 1：验证过程中所使用的技术、措施及独立水平的选择依赖于一系列因素，包括复杂程度、设计的新颖性、技术的新颖性和要求的安全完整性等级等。

注 2：验证活动的例子包括设计复审、使用的工具和技术(包括软件验证工具和 CAD 工具)。

8 过程危险和风险评估

8.1 目的

本章的目的是：

——确定过程及其相关设备的危险和危险事件；

——确定导致危险事件的事件序列；

——确定与危险事件相关联的过程风险；

——确定风险降低的任何要求；

——确定达到必要的风险降低所要求的安全功能；

——确定每个安全功能是否是仪表安全功能(见第 9 章)。

注 1：本部分第 8 章的对象是过程工程师、危险和风险专家、安全管理人员及仪表工程师。该章的目的是认识多学科方法确定仪表安全功能的典型要求。

注 2：在合理可执行的情况下，应把过程设计成固有安全的。如果做不到，设计中就需要增加如机械保护系统和安全仪表系统这样的风险降低方法。这些系统可单独工作，也可相互组合。

注 3：图 9 示出了过程工厂中典型的风险降低方法(没有层次分别)。

8.2 要求

8.2.1 对过程及其相关设备(如 BPCS)应进行一次危险和风险评估。其结果应是:

——已识别的每个危险事件及其起因(包括人为误差)的描述;

——事件的后果和可能性描述;

——工况考虑,如正常运行、起动、停机、维护、过程扰乱(upset)、紧急停机;

——为达到要求的安全性需增加的风险降低要求的确定;

——关于为降低或消除危险和风险所采取的措施的信息的描述或者引用;

——在风险分析中对可能的要求率和设备失效率等所作的假设,以及对操作约束或人为干预的可信度的详细描述;

——在考虑到安全层之间、安全层和 BPCS 之间由共同原因失效引起有效保护潜在降低的情况下(见注 1),分配给各保护层的安全功能(见第 9 章);

——用作仪表安全功能的安全功能的确定(见第 9 章)。

注 1:在确定安全完整性要求时,需考虑产生要求的系统和被设计用来响应这些要求的保护系统之间共同原因的影响。例如,控制系统失效提出了(保护)要求,保护系统中使用的设备同控制系统中使用的设备类似或相同。在这种情况下,当一个共同原因使保护系统中的类似设备变得无效时,控制系统中设备的一次失效产生的(保护)要求可能就得不到有效地响应。因为在最初确定危险和分析风险的过程中,保护系统的设计未必就已完成,在这样早的一个阶段中还不可能辨别出共同原因问题。在这种情况下,只要完成了安全仪表系统和其他保护层的设计,就有必要重新考虑安全完整性要求和仪表安全功能要求。在确定过程和保护层整体设计是否满足要求时,需要考虑共同原因失效。

注 2:在 GB/T 21109.3 中示出了用于确立安全仪表系统所要求的 SIL 的例子。

8.2.2 对保护层提出要求的 BPCS 的危险失效率(不遵循 GB/T 21109)不应被假设小于 10^{-5}/h。

8.2.3 应记录危险和风险评估,使以上各项之间的关系清楚和可追溯。

注 1:上述要求并不强制风险和风险降低目标一定要赋数值。也可以使用绘图法(见 GB/T 21109.3)。

注 2:必要的风险降低的程度根据应用与国家法规要求的不同而有所不同。一个为多个国家所接受的原则是:采取额外的风险降低措施,直到花费的成本同取得的风险降低变得不成比例为止。

9 给保护层分配安全功能

9.1 目的

本章的目的是:

——给保护层分配安全功能;

——确定要求的仪表安全功能;

——确定每个仪表安全功能相关联的安全完整性等级。

注:在分配过程中应考虑其他工业标准或规程。

9.2 分配过程要求

9.2.1 分配过程应导出以下结果:

——给专用来预防、控制或减轻来自过程及其相关设备危险的保护层分配安全功能;

——给仪表安全功能分配风险降低目标。

注:法规要求或其他工业法规可确定分配过程中的优先权。

9.2.2 通过考虑仪表安全功能提供的风险降低要求,可推导出该功能要求的安全完整性等级。

注:相关指南见 GB/T 21109.3。

9.2.3 在要求模式下操作的每个仪表安全功能所需要的 SIL,应根据表 3 或表 4 来规定。当使用表 4 时,既不能用检验测试间隔也不能用要求率来确定安全完整性等级。

9.2.4 在连续操作模式下操作的每个仪表安全功能所需要的 SIL,应根据表 4 来规定。

表 3 安全完整性等级:要求时的失效概率

要求操作模式		
安全完整性等级(SIL)	要求时的目标平均失效概率	目标风险降低
4	$\geqslant 10^{-5} \sim < 10^{-4}$	$>10\ 000 \sim \leqslant 100\ 000$
3	$\geqslant 10^{-4} \sim < 10^{-3}$	$>1\ 000 \sim \leqslant 10\ 000$
2	$\geqslant 10^{-3} \sim < 10^{-2}$	$>100 \sim \leqslant 1\ 000$
1	$\geqslant 10^{-2} \sim < 10^{-1}$	$>10 \sim \leqslant 100$

表 4 安全完整性等级:SIF 的危险失效频率

连续操作模式	
安全完整性等级(SIL)	执行仪表安全功能的目标危险失效频率(每小时)
4	$\geqslant 10^{-9} \sim < 10^{-8}$
3	$\geqslant 10^{-8} \sim < 10^{-7}$
2	$\geqslant 10^{-7} < 10^{-6}$
1	$\geqslant 10^{-6} \sim < 10^{-5}$

注 1:另外的说明见 3.2.43。

注 2:安全完整性等级用数值定义以便为替代设计和解决方案的比较提供一个客观目标。然而应该认识到,在当前的知识状况条件下,许多失效的系统原因还只能进行定性评估。

注 3:对于连续模式下的一个仪表安全功能所要求的每小时的危险失效频率,是通过把在连续模式下操作的仪表安全功能失效所产生的风险(用危险失效率表示),连同在考虑到其他保护层的贡献时导致同一风险的其他设备的失效率一并考虑来确定的。

注 4:能用几个较低安全完整性等级的系统来满足一个较高等级功能的需要(如使用一个 SIL 2 和一个 SIL 1 的系统共同满足一个 SIL 3 功能的需要)。

9.3 安全完整性等级 4 的附加要求

9.3.1 分配给安全仪表系统仪表安全功能的安全完整性等级不能高于 4。在过程工业中要求某一个仪表安全功能的安全完整性等级为 4 的应用是罕见的。因为在合理的情况下,要在整个安全生命周期中达到和保持这样高的性能等级是困难的,所以应避免这种应用。在规定这种系统的情况下,要求在整个安全生命周期的所有方面都具备高等级的能力。

如果分析结果是指派给一个仪表安全功能的安全完整性等级为 4,则应考虑改变过程设计使过程变得更固有安全或者增加附加保护层。这些增强措施也许能降低仪表安全功能的安全完整性等级要求。

9.3.2 只有在满足下面的准则 a)或者 b)+c)时才允许仪表安全功能的安全完整性等级为 4:

a) 已由适当的分析方法和测试明显表明满足目标安全完整性失效量;

b) 已具有对被用作仪表安全功能组成部分的部件的广泛的操作经验;

注:这种经验应是在相似的环境中取得的,并且至少那些部件已用于相当复杂等级的系统中。

c) 安全仪表功能组成部分所包含部件的硬件失效数据已经足够多,从而可为要声明的硬件安全完整性目标失效量提供足够的置信度。

注:数据应是在相应的环境、应用和复杂程度下取得的。

9.4 对作为一个保护层的基本过程控制系统的要求

9.4.1 图 9 表示了作为一个保护层的基本过程控制系统。

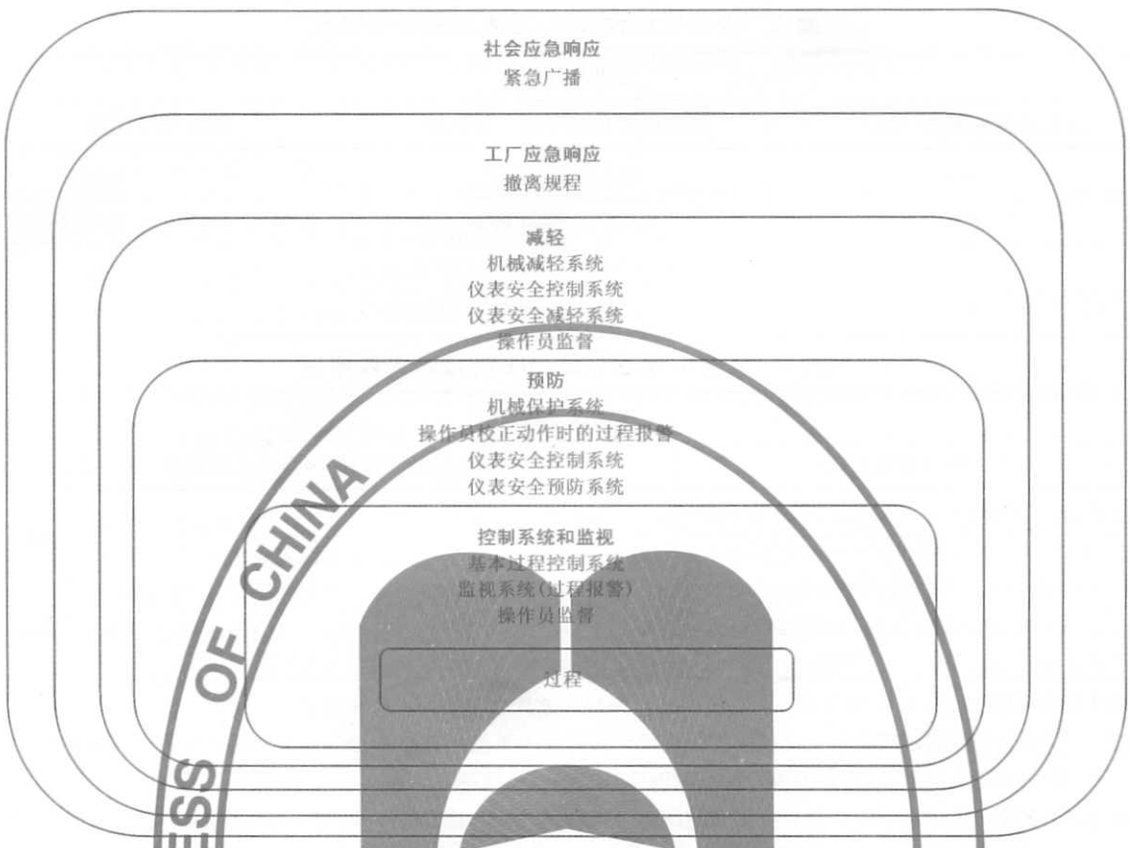


图 9 过程工厂中常见的典型风险降低方法

9.4.2 一个用作保护层的 BPCS 的风险降低因子(它并不符合 GB/T 21109 或者 GB/T 20438—2006)应小于 10。

注:当考虑一个 BPCS 降低风险的信任度有多大时,应考虑到这样一个事实,即 BPCS 的一部分也可以是一个事件的起源。

9.4.3 如果要求 BPCS 的风险降低因子大于 10,则应按 GB/T 21109 中的要求进行设计。

9.5 防止共同原因失效、共同模式失效和相关失效的要求

9.5.1 应对保护层的设计进行评估,以确保保护层之间、保护层同 BPCS 之间共同原因失效、共同模式失效和相关失效的可能性,同保护层的整体安全完整性要求相比足够低。这种评估可以是定性的也可以是定量的。

注:相关失效的定义见 3.2.12。

9.5.2 评估应考虑下列因素:

——保护层之间的独立性;

——保护层之间的多样性;

——不同保护层之间的物理分离;

——保护层之间、保护层同 BPCS 之间的共同原因失效(例如,在 SIS 中安全阀堵塞可能会产生与传感器堵塞相同的问题)。

10 SIS 安全要求规范

10.1 目的

本章的目的是规定仪表安全功能的要求。

10.2 一般要求

10.2.1 安全要求应从仪表安全功能分配和在安全计划编制过程中确定的那些要求中推导出来。

注：SIS要求应以下述方法表达和构建：

——清楚、精确、可验证、可维护和可行；

——易于被在生命周期任何阶段有可能使用这些信息的人理解。

10.3 SIS安全要求

10.3.1 这些要求对设计SIS而言应是足够的，它们应包括：

——达到要求的功能安全所必需的所有仪表安全功能的描述；

——识别和考虑共同原因失效的要求；

——对每个所确定的仪表安全功能的过程安全状态的定义；

——任何单个的过程安全状态的定义，当这些状态同时发生时就会产生一个单独的危险（如应急储存的过载、燃烧系统的多次泄压）；

——仪表安全功能要求和要求率的假定来源；

——检验测试间隔要求；

——SIS使过程进入其安全状态的响应时间要求；

——每个仪表安全功能的安全完整性等级和操作模式（要求/连续）；

——SIS过程测量和它们的脱扣点（trip point）的描述；

——SIS过程输出动作和成功操作准则的描述，例如密封截止阀的要求；

——过程输入和输出之间的功能关系，包括逻辑功能、数学功能和任何要求的许可；

——人工停机要求；

——与加电或断电脱扣（trip）有关的要求；

——在停机后复位SIS的要求；

——最大和可接受假脱扣率；

——失效模式和要求的SIS响应（如报警、自动停机）；

——与起动和重新起动SIS程序有关的任何特殊要求；

——SIS和任何其他系统（包括BPCS和操作员）之间的所有接口；

——工厂操作模式的描述，以及每种操作模式下仪表安全功能要求的识别；

——如12.2.2中列出的应用软件安全要求；

——超驰/禁止旁路要求，包括怎样清除它们；

——在检测到SIS中的故障事件时，达到和保持某个安全状态所必需的任何动作的规范，任何这样的动作都应考虑相关人员的因素；

——在考虑到运输时间、定位、备件安装、服务合同、环境约束时，SIS切实可行的平均修复时间；

——需要避免的SIS输出状态的危险组合的识别；

——应识别SIS可能遇到的所有极端环境条件，需考虑的有：温度、湿度、污染、接地、电磁干扰/射频干扰（EMI/RFI）、冲击/振动、静电放电、用电区等级、水淹、雷电和其他有关因素；

——不论装置作为一个整体（如装置起动）或单个装置操作规程（如设备维护、传感器校准和/或修理），确定其正常和异常模式，需要附加一些仪表安全功能以支持这些操作模式；

——任何能经受一次重大意外事故的仪表安全功能要求的定义，例如在一次火灾事故中阀门保持可操作性的时间要求。

注：SIS能执行非仪表安全功能以保证有序地停机或较快地起动。这些功能应同仪表安全功能分开。

10.3.2 软件安全要求规范应从安全要求规范和所选定的SIS结构推导出来。

11 SIS设计和工程

11.1 目的

本章的目的是设计一个或多个SIS，以提供仪表安全功能，并满足规定的安全完整性等级。

11.2 一般要求

11.2.1 应根据 SIS 安全要求规范，并考虑本章的所有要求来设计 SIS。

11.2.2 在要求 SIS 同时实现仪表安全功能和非安全功能时，在正常和故障状况下，对任何 SIF 有负面影响的所有硬件和软件应被当成 SIS 的组成部分，并符合对最高 SIL 的要求。

注 1：只要可行，就应把仪表安全功能同仪表非安全功能分开。

注 2：充分的独立性意味着任何非安全功能的失效或者利用仪表非安全软件功能编程都不能引起仪表安全功能失效。

11.2.3 在 SIS 实现不同安全完整性等级的仪表安全功能时，除非能表明较低安全完整性等级的仪表安全功能对较高安全完整性等级的仪表安全功能没有负面影响，否则共享或共用硬件和软件应符合最高安全完整性等级。

11.2.4 如果不打算让基本过程控制系统符合 GB/T 21109，基本过程控制系统应设计成单独的和独立的，从而不危及安全仪表系统的功能完整性。

注 1：可交换操作信息但不能危及 SIS 的功能安全。

注 2：当能表明基本过程控制系统的一次失效不会危害安全仪表系统的仪表安全功能时，SIS 的装置也可用于基本过程控制系统的功能。

11.2.5 为了有助于实现设计中的人为因素要求，在设计 SIS 的过程中，应涉及可操作性、可维修性和可测试性要求（如旁路设施使得在旁路时可进行在线测试和报警）。

注：应设计维护和测试设施，以便把因使用它们而引起的危险失效的可能性减少到切实可行的程度。

11.2.6 设计 SIS 应考虑人的能力和限制。并应适合于分派给操作员和维护人员的任务。所有的人—机接口设计应遵循良好的人员操作惯例，并应适合操作员可接受的培训或认知水平。

11.2.7 SIS 应设计成只要它把过程置于某个安全状态，它就会保持在安全状态直到启动一次复位为止，安全要求规范另有规定的情况除外。

11.2.8 与逻辑解算器无关的手动机制（如应急停机按钮）应用来启动 SIS 最终元件，安全要求规范另有规定的情况除外。

11.2.9 SIS 设计应全面考虑 SIS 和 BPCS 之间，以及 SIS 和其他保护层之间的独立性和相关性的所有方面。

11.2.10 一个装置作为执行仪表安全功能的一部分时，不应该（同时）用于基本过程控制目的，因为这个装置失效导致的基本过程控制功能失效，会引起对仪表安全功能的要求。除非分析后可以确认整体风险是可接受的。

注：当 SIS 的一部分用于控制并且公用设备的一次危险失效可能引起对 SIS 所执行的功能提出一次要求时，则会引入新的风险。附加的风险与共享部件的危险失效率有关，这是因为当共享部件发生故障时，立即就会产生一个要求，而 SIS 对此要求无力作出响应。因此在这些情况下需要进行额外的分析以保证共享部件的危险失效率足够低。以传感器和阀门为例，经常要考虑与 BPCS 共享设备的情况。

11.2.11 对掉电而并不丧失安全状态的子系统而言，应满足下列所有要求并按 11.3 采取动作：

——应检测电路完整性的丧失（如线路终端监视）；

——使用辅助电源（如备用电池，不间断电源）保证电源完整性；

——应检测子系统的掉电。

11.3 检测故障时的系统行为要求

11.3.1 在能允许单独一个硬件故障的任何子系统中，检测到危险故障时（利用诊断测试、检验测试或任何其他办法）应导致：

a) 用以达到或保持某种安全状态的一个规定动作（见注）；或者

b) 在修复故障部分的同时继续过程的安全运行。如果故障部分的修复不能在计算硬件随机失效概率中假定的平均恢复时间（MTTR）内完成，则会产生一个规定的动作以达到或保持某个安全状态（见注）。

注：在安全要求(见 10.3)中，应规定为达到或保持某个安全状态所需的规定动作(故障反应)。例如，它可以由过程或过程的某个部分的安全停机组成，该部分的风险降低依赖故障子系统或其他规定的减轻计划编制。

在上述动作有赖于操作员为响应一次报警而采取的特定动作(如打开或关闭一个阀门)的情况下，则应把报警当成安全仪表系统的一部分(即 BPCS 的独立性)。

在上述动作有赖于操作员为响应诊断报警而通知维护以便修复一个故障系统的情况下，该诊断报警可以是 BPCS 的一部分，但应经受适当的检验测试，并随 SIS 的其余部分一起进行变更管理。

11.3.2 当在子系统中检测到危险故障时(利用诊断测试、检验测试或任何其他办法)，如果该子系统是无冗余的、仪表安全功能完全依赖于该子系统(见注 1)，且子系统仅按要求模式实现仪表安全功能的情况下，则应导致：

a) 用以达到或保持某个安全状态的一个规定动作；或者

b) 在计算硬件随机失效概率中假定的平均恢复时间(MTTR)时段内修复故障子系统。在这段时期应由附加的措施和约束保证过程持续安全。这些措施和约束提供的风险降低，至少应等于无任何故障时的安全仪表系统所提供的风险降低。在 SIS 操作和维护程序中应规定这些附加措施和约束。如果不能保证在规定的平均恢复时间(MTTR)内完成修复，则应执行一个规定动作以达到或保持某个安全状态(见注 2)。

在上述动作有赖于操作员为响应一次报警而采取的特定动作(如打开或关闭一个阀门)的情况下，则应把报警当成安全仪表系统的一部分(即 BPCS 的独立性)。

在上述动作有赖于操作员为响应诊断报警而通知维护以便修复一个故障系统的情况下，该诊断报警可以是 BPCS 的一部分，但应经受适当的检验测试，并随 SIS 的其余部分一起进行变更管理。

注 1：如果该子系统的一次失效导致了所考虑的安全仪表系统中的仪表安全功能的一次失效，并且该安全功能还未被分配另一保护层，则可认为该仪表安全功能同该子系统完全相关(见第 9 章)。

注 2：在安全要求(见 10.3)中，应规定为达到或保持某个安全状态所需的规定动作(故障反应)。例如，它可以由过程或过程的某个部分的安全停机组成，该部分的风险降低依赖故障子系统或其他规定的减轻计划编制。

11.3.3 当在子系统中检测到危险故障时(利用诊断测试、检验测试或任何其他办法)，如果该子系统是无冗余的、仪表安全功能完全依赖于该子系统(见注 1)，且子系统仅按连续操作模式实现所有仪表安全功能的情况下(见注 2)，则应导致一个规定动作，以达到或保持某种安全状态。

在安全要求规范中应规定为达到或保持某种安全状态所需的规定动作(故障反应)。例如，它可以由过程或过程的某个部分的安全停机组成，该部分的风险降低依赖故障子系统或其他规定的减轻计划编制。检测故障及执行动作的总时间应少于发生危险事件的时间。

在上述动作有赖于操作员为响应一次报警而采取的特定动作(如打开或关闭一个阀门)的情况下，则应把报警当成安全仪表系统的一部分(即 BPCS 的独立性)。

在上述动作有赖于操作员为响应诊断报警而通知维护以便修复一个故障系统的情况下，该诊断报警可以是 BPCS 的一部分，但应经受适当的检验测试，并随 SIS 的其余部分一起进行变更管理。

注 1：如果该子系统的一次失效导致了所考虑的安全仪表系统中的仪表安全功能的一次失效，并且该安全功能还未被分配另一保护层，则可认为该仪表安全功能同该子系统完全相关。

注 2：当一个子系统的输出状态的一些组合有可能直接引起一个危险事件时，需要把子系统中的危险故障检测看作在连续模式下操作的一个仪表安全功能。

11.4 硬件故障裕度要求

11.4.1 对仪表安全功能而言，传感器、逻辑解算器和最终元件应具有最低的硬件故障裕度。

注 1：硬件故障裕度是一个部件或子系统在有一个或几个硬件危险故障的情况下，仍能继续承担所要求的仪表安全功能的能力。例如，硬件故障裕度为 1 意味着有两台装置，且其结构会使得两个部件或子系统的任何一个的危险失效都不能阻止安全动作发生。

注 2：为减轻 SIF 设计中的潜在缺陷，定义了最低的硬件故障裕度。这些潜在缺陷可能是由于 SIF 设计中所作假设的数目，以及在各种过程应用中使用的部件或子系统故障率的不确定性所导致的。

注3：值得注意的是，硬件故障裕度要求表示了最低的部件或子系统冗余。根据不同的应用，可能要求不同的部件失效率、检验测试间隔及附加冗余以满足11.9中对SIF的SIL的要求。

11.4.2 表5给出了对PE逻辑解算器的硬件故障裕度要求。

表5 PE逻辑解算器的最低硬件故障裕度

SIL	最低硬件故障裕度 SFF		
	<60%	60%～90%	>90%
1	1	0	0
2	2	1	0
3	3	2	1
4	应用特殊要求(见GB/T 20438—2006)		

11.4.3 假如主导(dominant)失效模式是达到安全状态，或者已检测出危险失效(见11.3)，那么除PE逻辑解算器外的所有子系统(如传感器、最终元件和非PE逻辑解算器)的最低硬件故障裕度见表6，否则故障裕度应增加1。

注：要确定优势失效模式是否是达到安全状态，需要考虑以下各项：

——装置的过程连接；

——用以确认过程信号的装置诊断信息的使用；

——装置固有的故障安全行为的使用(如非零最小输出(live zero)信号，断电导致安全状态)。

11.4.4 当使用的装置符合所有下列各项时，表6中规定的除PE逻辑解算器外所有子系统(如传感器、最终元件和非PE逻辑解算器)的最低硬件故障裕度可减少1：

——根据以往使用的情况选择装置硬件(见11.5.3)；

——装置只允许调整过程参数，如测量范围、上限或下限失效指示；

——装置过程参数的调整受保护，如跳线、密码；

——功能有小于4的SIL要求。

表6 传感器、最终元件和非PE逻辑解算器的最低硬件故障裕度

SIL	最低硬件故障裕度(见11.4.3和11.4.4)
1	0
2	1
3	2
4	应用特殊要求(见GB/T 20438—2006)

11.4.5 若根据GB/T 20438.2—2006的表2和表3进行了一次评估，则可使用替代的故障裕度要求。

11.5 选择部件和子系统的要求

11.5.1 目的

11.5.1.1 本条的首要目的是规定安全仪表系统的部件或子系统的选择要求。

11.5.1.2 本条的第二个目的是规定把部件或子系统集成到SIS结构中的要求。

11.5.1.3 本条的第三个目的是根据相关的仪表安全功能和安全完整性，规定部件和子系统的验收准则。

11.5.2 一般要求

11.5.2.1 对于SIL 1～SIL 3的应用而言，安全仪表系统部件和子系统适合的条件，应符合GB/T 20438.2—2006和GB/T 20438.3—2006的要求，或者符合本部分的11.4和11.5.3～11.5.6的要求。

11.5.2.2 对于SIL 4的应用而言，安全仪表系统部件和子系统适合的条件，应符合GB/T 20438.2—

2006 和 GB/T 20438.3—2006 的要求。

11.5.2.3 应通过以下考虑来证明所选部件和子系统的适合性：

——制造商硬件和嵌入式软件文档；

——如适用，合适的应用语言和工具选择(见 12.4.4)。

11.5.2.4 部件和子系统应符合 SIS 安全要求规范。

注：在选择部件和子系统时，本部分所有其他能适用的方面仍可使用，包括结构约束、硬件完整性、检测到故障时的行为和应用软件。

11.5.3 根据以往使用的情况选择部件和子系统的要求

11.5.3.1 应提供部件和子系统适用于该安全仪表系统的适当证据。

注 1：对于现场元件而言，在安全应用和非安全应用方面可能有广泛的操作经验。它们可作为基本证据。

注 2：证据的详细程度应依照所考虑的部件或子系统的复杂程度，和达到仪表安全功能的安全完整性等级所必需的失效概率。

11.5.3.2 适合性证据应包括：

——制造商的质量、管理和配置管理系统的考虑；

——部件或子系统满足要求的标识和规范；

——在类似操作行规和实际环境中部件或子系统性能的证明；

注：在现场装置(例如传感器和最终元件)满足某一给定功能的情况下，此功能在安全应用和非安全应用中通常是一样的，这意味着在两类应用中，装置将以同样的方式执行该功能。因此，考虑这种装置在非安全应用中的性能也可认为是满足此要求。

——大量的操作经验。

注：对于现场装置而言，与操作经验有关的信息主要记录在许可用于用户设施的用户设备清单中，该清单的形成是基于设备在安全和非安全应用中成功运行时的大量历史记录以及剔除不能成功执行功能的设备。倘若下列条件成立，现场装置清单则可用来支持操作经验的声明：

- 清单被定期更新和监视；
- 只有在获得足够的操作经验时，现场装置才可以加入该清单；
- 当现场装置的操作历史记录显示出它们不能完美地执行功能时，从该清单中删除它们；
- 清单中包含相关的过程应用。

11.5.4 根据以往使用的情况选择 FPL 可编程部件和子系统(如现场装置)的要求

11.5.4.1 使用 11.5.2 和 11.5.3 的要求。

11.5.4.2 在适合性证据中应标明部件和子系统未使用的特征，并且应确立它们不可能危害所要求的仪表安全功能。

11.5.4.3 针对硬件和软件的特定配置和操作行规的适合性证据应考虑：

——输入和输出信号的特点；

——使用的模式；

——使用的功能和配置；

——以前在类似应用和实际环境中使用的情况。

11.5.4.4 对于 SIL 3 应用，应对 FPL 装置进行一次正式评估(根据 5.2.6.1)以表明：

——FPL 装置能够执行要求的功能，并且以往使用表明当把该装置用作安全仪表系统的组成部分时，由于它的损坏(既可能是硬件随机失效，也可能是硬件或软件中的系统故障)可能导致一次危险事件的概率是足够低的；

——已经使用了针对硬件和软件的适当标准；

——在预定的操作行规的配置典型中已使用或者测试过 FPL 装置。

11.5.4.5 对于 SIL 3 应用，应提供一本可涵盖 FPL 装置的典型配置及预定的操作行规，并且包括操作、维护和故障检测约束的安全手册。

11.5.5 根据以往使用情况选择 LVL 可编程部件和子系统(如逻辑解算器)的要求

11.5.5.1 下面的要求仅适用于实现 SIL 1 或 SIL 2 仪表安全功能的安全仪表系统中使用的 PE 逻辑解算器。

11.5.5.2 应用 11.5.4 的要求。

11.5.5.3 在部件或子系统以往所经历过的操作行规和实际环境同它们在安全仪表系统中使用时的操作行规和实际环境存在任何差异时,应标明这些差异,并且如合适的话,应根据分析和测试作一次评估,以表明当用于安全仪表系统中时,系统故障的可能性是足够低的。

11.5.5.4 确定为证明适合性所需考虑的操作经验应包括:

——仪表安全功能的 SIL;

——部件或子系统功能的复杂程度。

注:另外的指南见 GB/T 21109.2。

11.5.5.5 倘若满足下列所有附加条款,则可在 SIL 1 或 SIL 2 应用中使用安全配置的一个 PE 逻辑解算器:

——理解非安全失效模式;

——使用用来论述所标明的失效模式的安全配置技术;

——嵌入式软件在安全应用中具有优良的使用历史;

——可保护未经授权的或非预定的修改。

注:安全配置的 PE 逻辑解算器是专门为安全应用而配置的一个通用工业级 PE 逻辑解算器。

11.5.5.6 应对在 SIL 2 应用中使用的任何 PE 逻辑解算器进行一次正式评估(根据 5.2.6.1)以表明:

——PE 逻辑解算器能执行要求的功能并且以往使用表明当把该装置用作安全仪表系统的组成部分时,由于它的损坏(既可能是硬件随机失效,也可能是硬件或软件中的系统故障)可能导致一次危险事件的概率是足够低的。

——在程序执行和启动相应的反应期间,已采取了检测故障的措施,这些措施应包括以下所有内容:

- 程序顺序监视;
- 防止修改或者通过在线监视检测失效的代码保护;
- 失效断言或多样化编程;
- 变量的范围检验,或者值的真实性检验;
- 模块化方法;
- 嵌入式软件和工具软件已使用合适的编码标准;
- 已在典型的配置中,通过预定操作行规的典型测试用例进行了测试;
- 使用值得信赖的,经验证过的软件模块和部件;
- 系统已经过动态分析和测试;
- 系统不使用人工智能,也不使用动态配置;
- 已执行文档化的故障插入测试。

11.5.5.7 对于 SIL 2 应用,应提供一本可涵盖 PE 逻辑解算器的典型配置及预定操作行规,并且包含操作、维护及故障检测约束的安全手册。

11.5.6 **选择 FVL 可编程部件和子系统(如逻辑解算器)的要求**

11.5.6.1 当使用一种 FVL 对应用程序进行编程时,PE 逻辑解算器应符合 GB/T 20438.2—2006 和 GB/T 20438.3—2006 的要求。

11.6 **现场装置**

11.6.1 选择和安装现场装置应最小化可能因过程条件和环境条件导致信息不准确的失效。应考虑的条件包括:腐蚀、管道中材料的冷却、悬浮固体、聚合、蒸煮、温度和压力极限,在干式冲击冷凝器气压管

中冷凝，在湿式冲击冷凝器气压管中不充分冷凝。

11.6.2 用于离散型脱扣输入/输出电路的加电，应采用一种方法以保证电路和电源的完整性。

注：此方法的例子是使用一个线路终端监视器，在这种情况上可连续监视一个辅助电流(pilot current)从而确保电路的连续性，而辅助电流的幅度不会影响 I/O 的正常工作。

11.6.3 除下列情况外，每个单独的现场装置都应具有连接到系统输入/输出的专线：

——多个离散的传感器串联到单独一个输入并且这些传感器全都监视同一过程条件(如电机过载)。

——多个最终元件连接到同一个输出。

注：当两个阀门连接到同一输出时，对使用两个阀门的所有仪表安全功能都要求这两个阀门同时改变状态。

——一条数字总线可同它所服务的，满足 SIF 完整性要求的整体安全性能通信。

11.6.4 除非适当的安全复审允许使用读/写，应对智能传感器进行写保护以防止来自远处的无意修改。复审应考虑例如不遵循规程这样的人为因素。

11.7 接口

与 SIS 的接口包括人机接口和通信接口，但不限于：

——操作员接口；

——维护/工程接口；

——通信接口。

11.7.1 操作员接口要求

11.7.1.1 在 SIS 操作员接口是借助于 BPCS 操作员接口的情况下，应考虑在 BPCS 操作员接口中可能发生的可信失效。

11.7.1.2 SIS 的设计应尽量减少需要操作员进行选择的选项，以及在单元(系统)运行时旁路系统的需要。如果设计不要求使用操作员动作，则设计应包含防止操作员错误的设施。

注：如果操作员不得不选择某个特殊选项，则应有一个重复的证实步骤。

11.7.1.3 为防止未经许可的使用，旁路开关应加键锁或口令保护。

11.7.1.4 应作为操作员接口的一部分提供 SIS 状况信息，这种信息对保持 SIL 是关键性的。此信息包括：

——过程按它的顺序进行的情况；

——已发生 SIS 保护动作的指示；

——旁路一个保护功能的指示；

——如已发生表决和/或故障处理退化时，自动动作的指示；

——传感器和最终元件的状况；

——影响安全的断电；

——诊断结果；

——支持 SIS 所需的环境改善设备的失效。

11.7.1.5 SIS 操作员接口的设计应能防止改变 SIS 应用软件。在需要把安全信息从 BPCS 传送给 SIS 的情况下，应使用能选择性地允许从 BPCS 写给 SIS 专用变量的系统。设备或程序应能用于证实 SIS 发送和接收到的正确选择，并且不会危害 SIS 的安全功能性。

注 1：如果在 BPCS 中选择选项或者旁路并下载给 SIS，则 BPCS 的失效可能会干扰在要求时 SIS 进行操作的能力。如果出现这种情况，则 BPCS 将变得与安全有关。

注 2：在批处理过程中，根据正在使用的处方(recipe)可使用一个 SIS 来选择不同的设定值或逻辑功能。在这些情况下，可使用操作员接口进行所要求的选择。

注 3：从 BPCS 到 SIS 的不正确信息预防措施不应危害安全性。

11.7.2 维护/工程接口要求

11.7.2.1 PE SIS 维护/工程接口的设计，应保证此接口的任何失效都不会对 SIS 使过程进入某个安

全状态的能力产生不利的影响。这也许要求在SIS正常运行过程中断开维护/工程接口，如编程面板。

11.7.2.2 维护/工程接口应为下列功能提供访问保密保护：

——SIS操作模式、程序、数据、停用报警通信的方法、测试、旁路和维护；

——SIS诊断、表决和故障处理服务；

——增加、删除或者修改应用软件；

——排除SIS故障所需的数据；

——在要求旁路的情况下，接口安装应使得报警和手动关机设施不会失效。

注：软件版本仅适用于使用PE技术的SIS。

11.7.2.3 维护/工程接口不应用作操作员接口。

11.7.2.4 只能由一个使用具有适当文档和保密措施的维护/工程接口的配置过程或编程过程来执行允许和禁止读-写访问。

11.7.3 通信接口要求

11.7.3.1 SIS通信接口的设计应保证通信接口的任何失效不会对SIS使过程进入某个安全状态的能力产生不利的影响。

11.7.3.2 SIS应能在不影响SIF的情况下与BPCS和外设进行通信。

11.7.3.3 通信接口应足够健壮以便能承受包括电源浪涌在内的电磁干扰而不会引起SIF的危险失效。

11.7.3.4 通信接口应适用不同参考地电位的装置间的通信。

注：也许需要一种替代媒体(如光纤)。

11.8 维护或测试设计要求

11.8.1 设计应允许对每一端或分几部分对SIS进行测试。在预定的过程停机时间之间的间隔大于检验测试间隔的情况下，需要在线测试设施。

注：术语端-端意味着从传感器端的过程流体到执行器端的过程流体。

11.8.2 当要求在线检验测试时，测试设施应是用来测试未检测到的失效的SIS设计的那一整个部分。

11.8.3 当SIS包括测试和/或旁路设施时，它们应符合：

——应按安全要求规范所定义的维护和测试要求设计SIS；

——应通过报警和/或操作规程警告操作员SIS任何部分的旁路。

11.8.4 应强制PE SIS的输入和输出不得用作以下各项的组成部分：

——应用软件；

——操作规程；

——维护，以下所说的除外。

SIS不停机就不允许强制输入和输出，除非增补规程和访问保密机制。如合适，任何这种强制都应通告或关断一个报警。

11.9 SIF的失效概率

11.9.1 每个仪表安全功能在要求时的失效概率应等于或小于安全要求规范中所规定的目标失效量。通过计算可对此进行验证。

注1：在要求操作模式下运行的仪表安全功能，应使用在要求时执行其设计功能的平均失效概率来表示目标失效量，如仪表安全功能的安全完整性等级所确定的那样(见表3)。

注2：在连续操作模式下运行的仪表安全功能，应使用每小时的危险失效频率来表示目标失效量，如仪表安全功能的安全完整性等级所确定的那样(见表4)。

注3：因为使用了不同的部件失效模式并且SIS的结构(用冗余表示)也可能有变化，所以对每个仪表安全功能的失效概率单独定量是必要的。

注4：目标失效量可以是要求时的平均失效概率的某个规定值，或者是根据定量分析得出的危险失效率的某个规定值，或者是由定性方法确定的与SIL相关的一个规定范围。

11.9.2 由硬件失效算出的每个仪表安全功能的失效概率应考虑：

a) SIS 的结构，这是由于它同所考虑的每个仪表安全功能有关；

b) 估计的每个子系统的失效率，它是由任何模式下的随机硬件故障产生的，这种故障可引起 SIS 的一次危险失效且已被诊断测试检测到；

c) 估计的每个子系统的失效率，它是由任何模式下的随机硬件故障产生的，这种故障可引起 SIS 的一次危险失效且未被诊断测试检测到；

注：使用来自一个已认知的工业源的数据或者为了以往应用预先在同样的环境下使用子系统的经验得到的部件或子系统失效数据，对设计进行一次定量失效模式分析，可确定一个子系统估计的失效率，并且这种使用经验足以证明所声明的平均失效时间的单边置信度下限按统计不低于 70%。

d) SIS 对共同原因失效的敏感度；

e) 任何定期的诊断测试的诊断覆盖率（按 GB/T 21109.2 确定的），相关的诊断测试间隔和诊断设施的可靠性；

f) 进行检验测试的时间间隔；

g) 已检测到的失效的修复时间；

h) 在任何模式下可能引起 SIS 一次危险失效的任何通信过程的估计危险失效率（包括诊断测试检测到的和未检测到的两种情况）；

i) 在任何模式下可能引起 SIS 一次危险失效的任何人为响应的估计危险失效率（包括诊断测试检测到的和未检测到的两种情况）；

j) 对电磁兼容性（EMC）干扰的敏感度（例如符合 GB/T 18268）；

k) 对气候和机械条件的敏感度（例如符合 GB/T 17214.1—1998 和 IEC 60654-3:1998）。

注 1：应提供建模方法，选择最合适的方法是分析人员的责任并同具体情况有关。适用的方法包括（见 GB/T 20438.6—2006附录 B）：

——仿真；

——因果分析；

——故障树分析；

——马尔可夫（Markov）模型；

——可靠性方框图。

注 2：诊断测试间隔时间加上修理持续时间构成了平均恢复时间（见 IEV 191-13-08），在可靠性模型中应考虑它。

12 应用软件要求，包括工具软件的选择准则

本章讨论：

——三类软件：

- 应用软件；
- 工具软件，即开发和验证应用软件所使用的软件工具；
- 嵌入式软件，即用作 PE 组成部分所提供的软件。

——三种软件的编写语言：

- 固定程序语言（FPL）；
- 有限可变语言（LVL）；
- 全可变语言（FVL）。

本部分仅限于使用 FPL 或者 LVL 编写的应用软件。下列要求适合于最高到 SIL 3 的应用软件的开发和修改。因此本部分对 SIL 1、SIL 2 和 SIL 3 不加以区别。

应按本部分使用 FPL 或 LVL 对最高到 SIL 3 的应用软件进行开发和修改。SIL 4 的应用软件的开发和修改则应遵循 GB/T 20438—2006。使用 FVL 编写和修改应用软件也应遵循 GB/T 20438—2006。

应按 12.4.4 的要求选择和使用工具软件(连同定义如何安全使用 PE 系统的制造商安全手册)。选择嵌入式软件应按 11.5 进行选择。

12.1 应用软件安全生命周期要求

12.1.1 目的

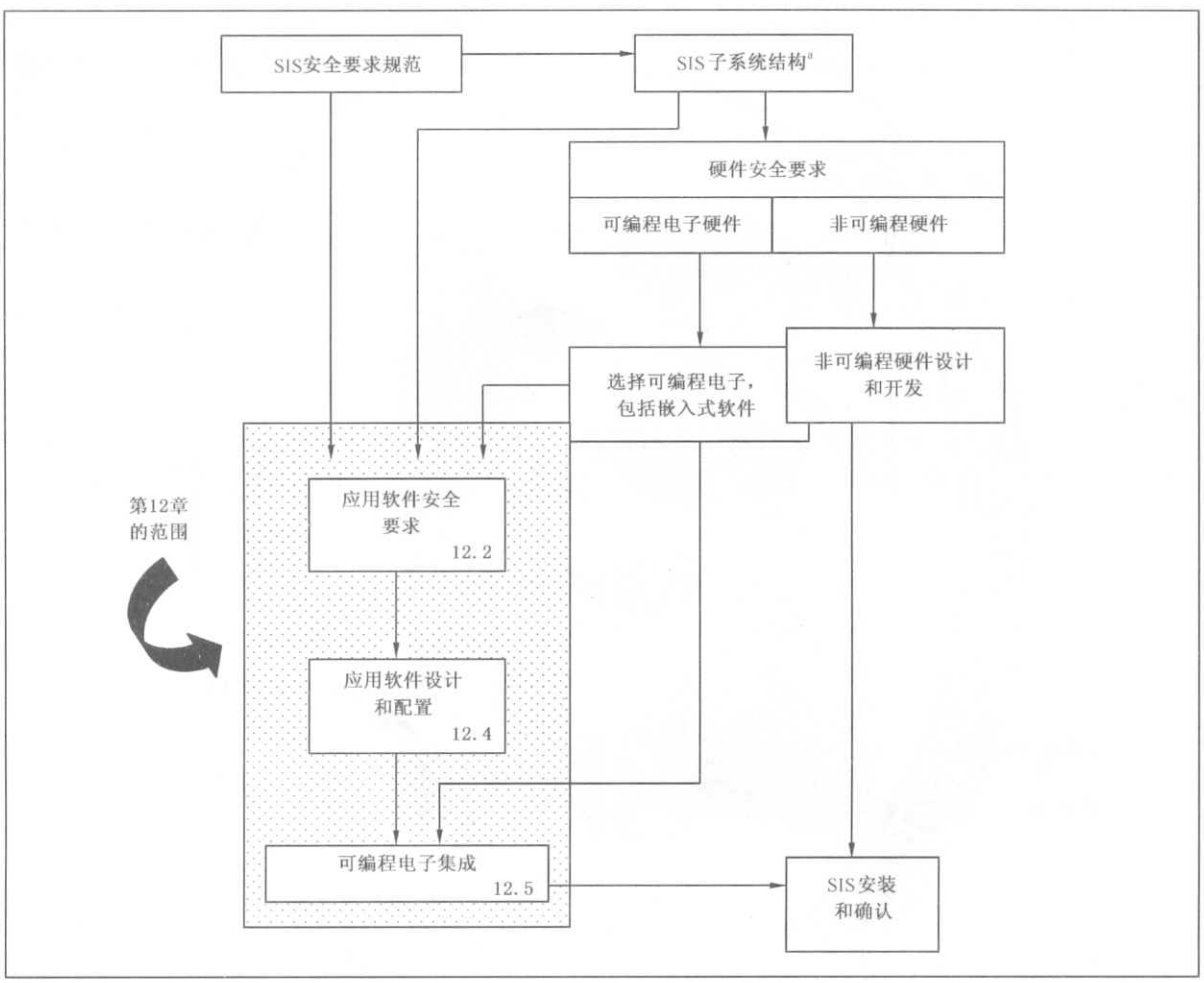
12.1.1.1 本章的目的是:

——定义每个 SIS 编程子系统应用软件开发中所要求的活动;

——定义怎样来选择、控制和使用用来开发应用软件的工具软件;

——保证有足够的计划使之能满足分配给应用软件的功能安全目的。

注:图 10 说明了在应用程序安全生命周期内第 12 章的范围。



[a] 例如传感器、逻辑解算器和最终元件。

图 10 应用软件安全生命周期及其与 SIS 安全生命周期的关系

12.1.2 要求

12.1.2.1 开发能满足本条要求的应用软件的安全生命周期应在编制安全计划期间确定,此周期应同 SIS 安全生命周期整合在一起。

12.1.2.2 应根据应用软件安全生命周期每个阶段的基本活动、目的、要求的输入信息和输出结果、验证要求(见 12.7)以及职责来定义这些阶段(见表 7 和图 11)。

注 1:如果应用软件安全生命周期满足表 7 的要求,裁减 V 模型(见图 12)阶段的深度、数量及规模以适合安全完整性和工程项目复杂程度考虑的要求是可以接受的。

注 2:用于应用程序功能的软件语言类型(FPL、LVL 或者 FVL)以及语言的严密性可能影响 V 模型阶段的范围。

注 3:应用软件安全要求规范可作为 SIS 安全要求规范的一部分。

注4：应用软件确认计划也可作为整个SIS或SIS子系统确认计划的一部分。

12.1.2.3 实现应用软件的PE装置应适合它为之服务的每个SIF所要求的安全完整性。

12.1.2.4 应针对每个生命周期阶段选择和使用各种方法、技术和工具，从而：

——尽量减少把故障引入应用软件中的风险；

——揭露并消除软件中已存在的故障；

——确保残留在软件中的故障不会导致不可接受的后果；

——确保该软件在整个SIS生存期内可维护；

——证明该软件的质量符合要求。

注：方法和技术的选择与特定的具体情况有关。其决策因素有：

——软件的总量；

——复杂程度；

——SIS的安全完整性等级；

——失效事件的后果；

——设计元素的标准化程度。

12.1.2.5 应对应用软件安全生命周期每个阶段进行验证(见12.7)并提供结果(见第19章)。

12.1.2.6 如果需要在与生命周期的某个前一阶段有关的任何时间段作某种更改，则应对安全生命周期的前一阶段及后面的所有阶段进行重新检查，在此过程中，如还有更改，则应重复以上过程并重新验证。

12.1.2.7 应用软件、SIS硬件、嵌入式软件和工具软件(工具)应服从配置管理(见5.2.7)。

12.1.2.8 应执行测试计划，并涉及下列问题：

——软件和硬件集成的策略；

——测试用例和测试数据；

——要执行的测试类型；

——测试环境(包括工具、支持软件和配置)描述；

——判断测试完成的测试准则；

——物理位置(例如工厂或现场)；

——与外部功能性的相关性；

——恰当的人员；

——不一致性。

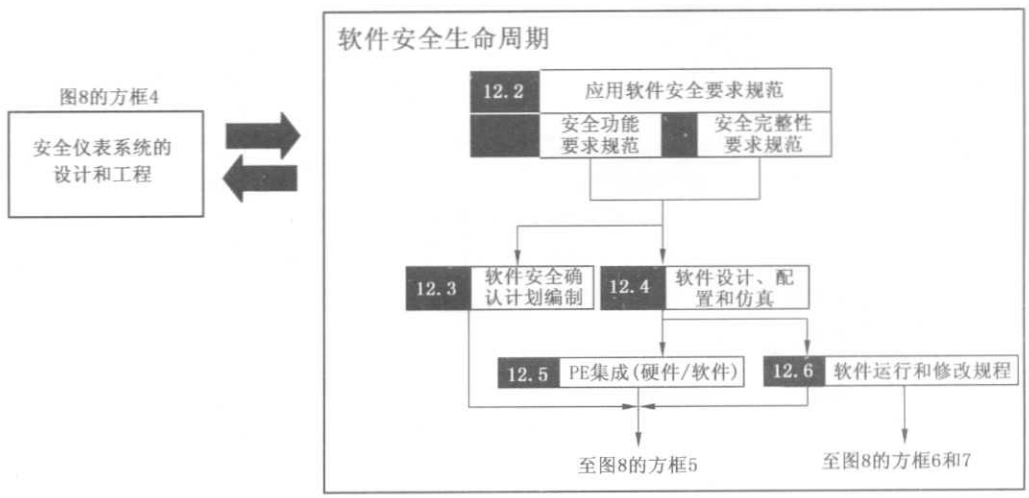


图11 应用软件安全生命周期(在实现阶段)

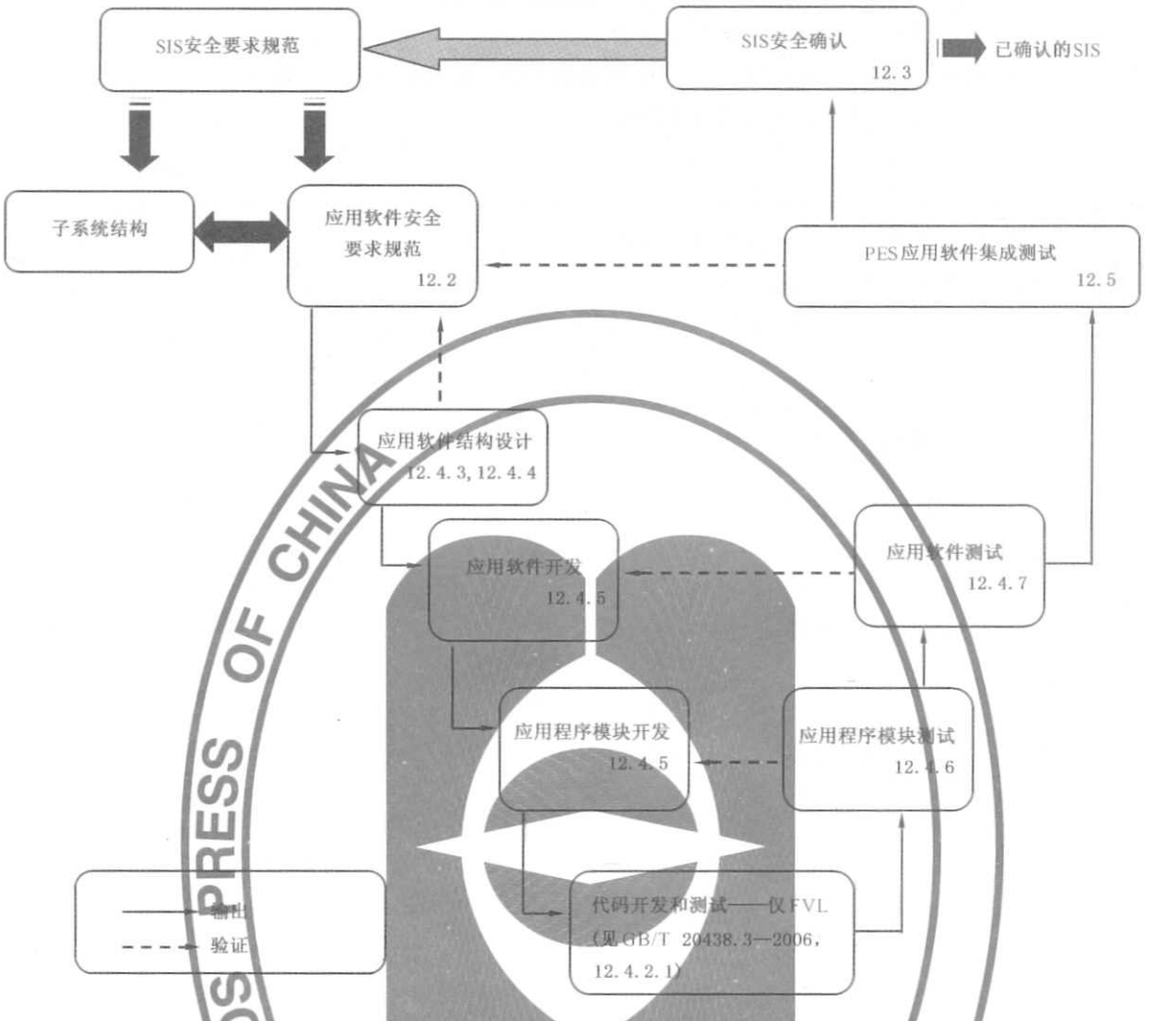


图 12 软件开发生命周期(V 模型)

表 7 应用软件安全生命周期一览表

安全生命周期阶段		目的	要求所在条	所需信息	要求的结果
图 11 方框号	标题				
12.2	应用软件安全要求规范	为实现要求的仪表安全功能所必需的每个 SIS 功能，规定软件仪表安全功能的要求 规定分配给该 SIS 的每个仪表安全功能的软件安全完整性要求	12.2.2	SIS 安全要求规范 所选 SIS 的安全手册 SIS 结构	SIS 应用软件安全要求规范 验证信息
12.3	应用软件安全确认计划编制	编制确认应用软件的计划	12.3.2	SIS 应用软件安全要求规范	SIS 应用软件安全确认计划 验证信息

表 7(续)

安全生命周期阶段		目的	要求所在条	所需信息	要求的结果
图 11 方框号	标题				
12.4	应用软件设计和开发	结构 创建能满足规定的软件安全要求的软件结构 复审和评价 SIS 硬件结构对软件的要求	12.4.3	SIS 应用软件安全要求规范； SIS 硬件结构设计手册	结构设计描述，例如将应用软件分离为相关的过程子系统和 SIL，例如辩别像泵或阀序列这类共用软件模块 应用软件结构和子系统集成测试规范 验证信息
	应用软件设计和开发	支持工具和编程语言 确定整个软件(工具软件)安全生命周期内适用的一组配置、库、管理以及仿真和测试工具 规定开发应用软件的规程	12.4.4	SIS 应用软件安全要求规范 结构设计描述 SIS 手册 所选的 SIS 逻辑解算器安全手册	使用工具软件的规程列表 验证信息
	应用软件设计和开发	应用软件开发和应用程序模块开发 实现能满足规定的应用软件安全要求的应用软件	12.4.5	结构设计描述 为使用工具软件所选 PES 的手册和规程列表	1)应用软件程序(例如功能块图、梯形逻辑) 2)应用程序仿真和集成测试 3)专用应用软件安全要求规范 4)验证信息
12.4	使用全可变语言编写应用程序	程序编写和测试——仅对 FVL 实现能满足规定的软件安全要求的全可变语言	12.4.6 和 12.4.7	专用应用软件安全要求规范	见 GB/T 20438.3—2006

表 7(续)

安全生命周期阶段		目的	要求所在条	所需信息	要求的结果
图 11 方框号	标题				
12.4	应用软件设计和开发	应用软件测试： 1) 验证已达到软件安全要求 2) 显示所有的应用程序子系统和系统可正确地相互作用，从而执行它们的预定功能而不执行非预定的功能 如有满意的测试覆盖率，则可同下一阶段合并(12.5)	12.4.6， 12.4.7， 12.7	应用程序仿真和集成测试规范(基于结构的测试) 软件结构集成测试规范	1)软件测试结果 2)经验证和测试过的软件系统 3)验证信息
12.5	可编程电子集成(硬件和软件)	把软件集成到目标可编程电子硬件上	12.5.2	软件和硬件集成测试规范	软件和硬件集成测试结果 经验证过的软件和硬件
12.3	SIS 安全确认	确认包括安全应用软件的 SIS 能满足安全要求	12.3	软件和 SIS 安全确认计划	软件和 SIS 确认结果

12.2 应用软件安全要求规范

注：本阶段是图 11 的方框 12.2。

12.2.1 目的

12.2.1.1 本条的目的是给符合 SIS 结构的，用来实现要求的仪表安全功能所必需的每个可编程 SIS 子系统的应用软件安全要求规范提供要求。

注：硬件和软件结构关系见图 13。

可编程 SIS 子系统结构		
硬件结构	软件结构(软件结构由嵌入式软件和应用软件组成)	
在硬件中的通用和应用专用特征。 示例包括： ——诊断测试； ——冗余处理器； ——双 I/O 卡。	嵌入式软件 示例包括： ——通信驱动程序； ——故障处理； ——可执行软件。	应用软件 示例包括： ——输入/输出功能； ——派生功能(例如当不提供与嵌入式软件相同服务时的传感器检验)。

图 13 SIS 硬件和软件结构之间的关系

12.2.2 要求

12.2.2.1 应编制一份应用软件安全要求规范。

注 1：一个 SIS 通常由 3 个结构化子系统组成：传感器、逻辑解算器和最终元件。此外，子系统可能具有冗余装置以便达到要求的安全完整性等级。

注 2：一种具有冗余传感器的 SIS 硬件结构，也许会对 SIS 逻辑解算器提出额外的要求(例如实现 1oo2 逻辑)。

注 3：在 SIS 的要求中已经规定有 SIS 子系统软件安全要求(见第 10 章)，此处不需重复。

注4：需要一个软件安全要求规范以便确定PE软件功能性的最低能力，同时也是为了约束选择可能导致不安全状况的任何功能性。

12.2.2.2 给每个SIS子系统的软件安全要求规范的输入应包括：

a) 规定的SIF的安全要求；

b) 由SIS结构得出的要求；以及

c) 安全计划编制的任何要求(见第5章)。

注1：应向应用软件开发者提供此信息。

注2：此要求并不意味着SIS结构开发者、负责装置配置的组织以及应用软件开发者之间不存在重迭。当应用软件安全要求和可能的应用软件结构(见12.4.3)变得更精确时，也许会对SIS硬件结构有影响，为此，SIS结构开发者、SIS子系统供货商和应用软件开发者之间的紧密合作就显得非常重要(见图5)。

12.2.2.3 应用软件安全要求规范应足够详细，以使设计和实现能达到要求的安全完整性，并且使之能执行功能安全评估。应考虑：

——应用软件所支持的功能；

——能力和响应时间性能；

——设备和操作员接口及其可操作性；

——在SIS安全要求规范中所规定的所有有关的过程操作模式；

——对如超出范围的传感器值，检测到的开路和短路这种不良过程变量采取的动作；

——外部装置(如传感器和最终元件)的检验测试和诊断测试；

——软件自监视(例如包括应用程序驱动的看门狗和数据范围确认)；

——SIS中的其他装置(如传感器和最终元件)的监视；

——在过程运转时启动仪表安全功能的定期测试；

——引用一些输入文档(如SIF规范、SIS配置和结构、SIS硬件安全完整性要求)。

12.2.2.4 应用软件开发者应复审规范中的信息以保证要求无歧义、一致和可理解。应为SIS子系统开发者标明规定的安全要求中的任何不足之处。

12.2.2.5 表达和构建规定的软件安全要求的形式，应使：

——那些在SIS安全生命周期任何阶段使用文档的人员便于理解；这包括工厂操作人员和维护人员，以及应用程序编程人员在使用术语和描述时不会有歧义和能理解；

——它们应可验证、可测试和可修改；

——它们可以追溯到SIS安全要求规范。

12.2.2.6 应用软件安全要求规范提供的信息应使之能选择正确的设备。应考虑：

——使过程能达到或保持某个安全状态的功能；

——与检测、通报和管理SIS所有子系统故障有关的功能；

——与仪表安全功能进行定期在线测试有关的功能；

——与仪表安全功能进行定期离线测试有关的功能；

——允许SIS能被安全地修改的功能；

——与非安全相关功能的接口；

——能力和响应时间性能；

——上述每个功能的安全完整性等级。

注1：这些功能中的一些功能可能是系统软件的一部分，这取决于所选SIS子系统的属性。

注2：接口包括离线和在线修改设施。

12.3 应用软件安全确认计划编制

注：此阶段是图11的方框12.3。

12.3.1 目的

12.3.1.1 本条的目的是保证能编制出合适的应用软件确认计划。

12.3.2 要求

12.3.2.1 应根据第15章编制应用软件确认计划。

12.4 应用软件设计和开发

注：此阶段是图11的方框图12.4。

12.4.1 目的

12.4.1.1 本条的首要目的是创建一个与硬件结构一致，并且满足规定的软件安全要求(见12.2)的应用软件结构。

12.4.1.2 本条的第二个目的是复审和评价SIS的硬件和嵌入式软件结构对软件的要求。这些要求包括SIS硬件/软件行为的副作用、SIS硬件应用的专门配置、SIS的固有故障裕度以及SIS硬件和嵌入式软件结构与安全应用软件的相互作用。

12.4.1.3 本条的第三个目的是选择一套合适的工具(包括工具软件)以便开发应用软件。

12.4.1.4 本条的第四个目的是设计和实现或选择能满足规定的软件安全要求(见12.2)的应用软件，这些要求是可分析、可验证和可被安全修改的。

12.4.1.5 本条的第五个目的是验证是否已经达到软件安全要求(指要求的软件仪表安全功能)。

12.4.2 一般要求

12.4.2.1 全可变语言应用程序的编写、测试、验证和确认应符合GB/T 20438.3—2006。

12.4.2.2 设计方法应同所使用的SIS子系统已知的开发工具和约束条件一致。

注：应在设备安全手册中定义对保证符合GB/T 21109所需的SIS子系统应用程序的约束条件。

12.4.2.3 所选设计方法和应用程序语言(LVL或FPL)的特征应具有：

a) 抽象、模块化和控制复杂性的其他特征：只要有可能，软件应使用具有良好检验性的软件模块为基础，这些模块可以包括用户库功能和良好的链接软件模块的规则。

b) 表达：

——功能性，最理想的是表示成一个逻辑描述或一些算法功能；

——应用功能的模块元素之间的信息流；

——顺序要求；

——保证仪表安全功能总是在规定的时间约束内运转；

——避免不确定的行为；

——保证不会错误地复制内部数据项，定义所使用的所有数据类型以及当数据超过范围或者不恰当时则发生适当的动作；

——设计假设及其相关性。

c) 理解，需要理解设计的开发人员和其他人员应了解应用功能和认识技术约束条件。

d) 验证和确认，包括应用软件代码的覆盖率，集成应用程序的功能覆盖率，与SIS的接口及其应用的专用硬件配置。

e) 应用软件的修改，包括模块化、可追溯性和文档化。

12.4.2.4 完成的设计应：

a) 包括数据集成检验和合理性检验；

注：例如通信链路中的端到端检验，传感器输入的边界检验，数据参数的边界检验及应用功能的多样化执行。

b) 可追溯到要求；

c) 可测试；

d) 具有安全修改的能力；

e) 能使SIF应用软件的复杂性的规模最小。

12.4.2.5 在应用软件需实现不同安全完整性等级的仪表安全功能或者非安全功能的情况下，除非设计能显示出不同安全完整性等级的仪表安全功能之间是独立的，否则应把所有软件当成属于最高安全

完整性等级对待。独立性的合理性证明应被文档化，不论声明或者不声明独立性都应标明每个 SIF 预定的 SIL。

注 1：GB/T 21109.2 提供了要在 SIS 中实现仪表安全功能和非安全功能时，怎样设计和开发应用软件的指南。

注 2：GB/T 21109.2 提供了要在 SIS 中实现不同 SIL 的 SIF 时，怎样设计和开发应用软件的指南。

12.4.2.6 如果要把以往开发的应用软件库用作设计的一部分，则应证明它们适合应用软件安全要求规范(见 12.2)的正确性。适合性的根据是：

——当使用 FVL 时，应符合 GB/T 20438.3—2006；或者

——当使用 FPL 或 LVL 时，应符合 GB/T 21109；或者

——在类似应用中能满意运行的证据，已证明这些应用具有同样的功能性或者服从对任何新开发软件所期望的相同验证和确认规程(见 11.5.4 和 11.5.5)。

注：在编写安全计划过程中，就可制定合理性证明(见第 8 章)。

12.4.2.7 在应用程序文档集或相关文档集中至少应包含如下信息：

a) 法人实体(如公司、作者)；

b) 描述；

c) 对应用功能要求的可追溯性；

d) 使用的逻辑协定；

e) 使用的标准库功能；

f) 输入和输出；

g) 包含修改更历史的配置管理。

12.4.3 应用软件结构要求

12.4.3.1 应用软件结构的设计应在 SIS 系统结构的约束范围内、根据要求的 SIS 安全规范进行。该设计的要求应与所选用的子系统、设计它的成套工具和安全手册相一致。

注 1：软件结构定义了系统和应用软件的主要部件和子系统以及怎样把它们互连起来、怎样达到所要求的属性和尤其是安全完整性。系统软件模块的例子包括操作系统、数据库和通信子系统。应用软件模块的例子包括整个工厂都要复制的应用功能。

注 2：应用软件结构还应由供货商提供的 SIS 子系统的基础结构确定。

12.4.3.2 应用软件结构设计的描述应：

a) 提供内部构造和 SIS 子系统及其部件的全面描述；

b) 包括所有被确定的部件的规范以及那些部件(硬件和软件)之间的连接和相互作用的描述；

c) 标出在 SIS 子系统中包含的但并不用于 SIF 中的那些软件模块；

d) 描述对于输入/输出子系统的数据逻辑处理的次序以及逻辑解算器的功能性，包括由扫描时间强加的任何限制；

e) 标明所有的非 SIF，并保证它们不会影响任何 SIF 的正常运行。

注：特别重要的是，对 SIS 子系统而言，结构文档集应是最新的和完整的。

12.4.3.3 应标明开发应用软件所使用的一套方法和技术，并证明选择它们的基本理由是正确的。

注：选择这些方法和技术的目的是保证：

——SIS 子系统行为的可预见性；

——故障裕度(与硬件相符)和故障避免，包括冗余和多样化。

12.4.3.4 在设计应用软件中使用的方法和技术，应同 SIS 子系统安全手册中规定的任何约束相符。

12.4.3.5 应描述用于保持所有数据安全完整性的特征并证明其合理性。这些数据可包括工厂输入/输出数据、通信数据、操作数据、维护数据和内部数据库数据。

注：硬件结构和软件结构之间存在相互影响(见图 11)，因此需同硬件开发者讨论诸如可编程电子硬件和软件集成测试规范(见 12.5)这种问题。

12.4.4 支持工具、用户手册和应用程序语言的要求

12.4.4.1 应选择一组合适的工具，包括：应用程序编程语言子集、配置管理、仿真、测试全套(harness)工具和当适用时使用的自动测试覆盖率的测量工具。

12.4.4.2 应考虑提供合适的工具(指在开发系统初期不一定使用的那些工具)以便在SIS的整个生存期内支持有关的服务。

注：应根据应用软件开发活动、嵌入式软件和软件结构来选择开发工具(见12.4.3)。

12.4.4.3 应考虑安全手册约束、可能把故障引入应用软件的已知缺点以及对前一次验证和确认的覆盖率的限制，确定一套合适的使用工具的规程。

12.4.4.4 选择的应用程序语言应：

——使用经评估过的一个翻译器/编译器来实现；

——被完整地和无歧义地定义或者被限定为所定义的特征是无歧义的；

——同应用的特点相匹配；

——包含有助于检测编程失误的特征；

——支持同设计方法相匹配的特征。

12.4.4.5 在应用软件结构设计描述(见12.4.3)过程中，当不能满足12.4.4.4时，应对所使用的语言的合理性证明文档化。合理性证明应详述对语言目的的适合性，和涉及已识别的任何语言缺陷的任何附加措施。

12.4.4.6 使用应用程序语言的规程应规定良好的编程习惯，禁止不安全的一般软件特征(如未定义的语言特征、非结构化设计)，确定检测配置中故障的检验以及规定应用程序文档的规程。

12.4.4.7 适当的话，安全手册应涉及下列各项：

a) 为执行安全功能使用的诊断；

b) 认证/验证安全库的清单；

c) 强制测试和系统停机逻辑；

d) 看门狗的使用；

e) 对工具和编程语言的要求和限制；

f) 装置或系统适合的安全完整性等级。

12.4.4.8 应验证工具的适合性。

12.4.5 应用软件的开发要求

12.4.5.1 在开始详细设计应用软件之前应提供以下信息：

a) 软件安全要求规范(见12.2)；

b) 应用软件结构设计描述(见12.4.3)，包括应用程序逻辑和故障裕度功能性的识别、输入和输出数据表、所使用的一般软件模块和支持工具以及应用软件编程规程。

12.4.5.2 应按某种结构化方式生产应用软件以便达到：

——功能性的模块化；

——功能性(包括故障裕度特征)和内部结构的可测试性；

——安全修改能力；

——应用功能和相关约束的可追溯性和说明。

注：尽可能地使用经验证的软件模块。

12.4.5.3 每个应用程序模块的设计应涉及其健壮性，包括：

——每个输入变量(包括用来提供输入数据的任何全局变量)的真实性检验；

——所有输入和输出接口的定义；

——系统配置检验，包括期望的硬件和软件模块的存在及可访问。

12.4.5.4 应规定每个应用软件模块的设计和适用于每个应用软件模块的结构化测试。

12.4.5.5 应用软件应：

——可读、可理解和可测试；

——满足相关设计原则；

——满足在安全计划编制过程中规定的相关要求(见 5.2.4)。

12.4.5.6 应对应用软件进行复审以保证符合规定的设计、设计原理和安全确认计划编制要求。

注：应用软件复审技术包括软件检查、走查和正式分析。复审应结合仿真和测试以保证应用软件满足与它相关的规范。

12.4.6 应用软件模块测试要求

注：测试应用软件模块是否能正确满足其规范的活动是一个验证活动(另见 12.7)。它是复审和结构化测试的组合，从而为应用软件模块满足其相关规范即验证提供了保证。

12.4.6.1 应通过复审、仿真和测试技术，来检验每个输入点经过处理逻辑到输出点的配置，从而证实 I/O 数据能够映射到正确的应用逻辑上。

12.4.6.2 应通过复审、仿真和测试技术，来检验每个应用软件模块，以确定预定的功能可被正确执行以及不执行非预定的功能。

测试应适用于被测试的专用模块并应考虑：

——考验应用程序模型的所有部分；

——考验数据边界；

——执行顺序产生的时间(timing)影响；

——正确时序的实现。

12.4.6.3 应提供应用软件模块测试的结果。

12.4.7 应用软件集成测试要求

注：软件被正确集成的测试活动是一个验证活动(另见 12.7)。

12.4.7.1 应用软件测试应显示所有的应用软件模块、部件/子系统相互之间以及它们同基础的嵌入式软件之间能正确地相互作用，从而执行它们的预定功能。

注：还应执行另外的一些测试，以证实软件不执行可能危及其安全要求的非预定功能。

12.4.7.2 应提供应用软件集成测试的结果并应说明：

a) 测试结果；

b) 是否满足测试规范的目的和准则。

如失败，则应报告失败的原因。

12.4.7.3 在集成应用软件的过程中，对软件的任何修改需经安全影响分析以确定：

a) 受影响的所有软件模块；

b) 必要的重新设计和重新验证活动(见 12.6)。

12.5 应用软件与 SIS 子系统的集成

注：此阶段是图 11 的方框 12.5。

12.5.1 目的

12.5.1.1 本条的目的是要证明 SIS 子系统中使用的硬件和嵌入式软件运转时，应用软件能满足软件安全要求规范。

注：根据应用的特性，这些活动可和 12.4.7 相结合。

12.5.2 要求

12.5.2.1 为了保证应用软件同硬件和嵌入式软件平台兼容，从而满足功能和性能安全要求，应在软件安全生命周期内尽早规定集成测试。

注 1：根据以往经验可减小测试的范围。

注 2：应涉及：

——应用软件划分成可管理的集成集；

——测试用例和测试数据；

——被执行的测试类型；

——测试环境、工具、配置和程序；

——测试准则，依据这些准则可判断测试完成；

——测试过程中出现失败时，改正动作的规程。

12.5.2.2 在测试过程中，任何修改或更改都应经过安全影响分析以确定：

a) 所有受影响的软件模块；

b) 必要的重新验证活动(见12.7)。

12.5.2.3 应提供如下测试信息：

a) 被测试的配置项；

b) 支持测试的配置项(工具和外部功能性)；

c) 涉及的人员；

d) 测试用例和测试脚本；

e) 测试结果；

f) 是否满足测试目的和准则；

g) 如果不成功，失败的原因、失败和改正记录(包括重新测试和重新验证)的分析(见12.5.2.2)。

12.6 FPL和LVL软件修改规程

注：修改主要适用于软件运行阶段中发生的更改。

12.6.1 目的

12.6.1.1 本条的目的是保证在修改之后软件能继续满足软件安全要求规范。

12.6.2 修改要求

12.6.2.1 应根据5.2.6.2.2、5.2.7和第17章以及下列附加要求执行修改：

a) 修改前应分析修改的修改对过程安全和软件设计状态的影响并用以指导修改；

b) 应提供修改和重新验证的安全计划编制；

c) 应按计划编制执行修改和重新验证；

d) 应考虑编制修改和测试过程中要求的条件的计划；

e) 应更新受修改影响的所有文档；

f) 应提供所有SIS修改活动的细节(如日志)。

12.7 应用软件验证

12.7.1 目的

12.7.1.1 本条的首要目的是要证明信息是令人满意的。

12.7.1.2 本条的第二个目的是证明输出结果满足应用软件安全生命周期每一阶段所定义的要求。

12.7.2 要求

12.7.2.1 应按第7章执行应用软件安全生命周期每个阶段的验证计划编制。

12.7.2.2 应在以下方面验证每阶段的结果：

a) 对照某个特定的生命周期阶段的要求，验证该阶段输出的符合性；

b) 复审、检查和/或测试的输出覆盖面的符合性；

c) 不同生命周期阶段产生的输出之间的兼容性；

d) 数据的正确性。

12.7.2.3 验证还应涉及：

a) 可测试性；

b) 可读性；

c) 可追溯性。

注1：应在下列方面对应用程序数据格式进行验证：

——完整性；

——自相一致性；

——对未经授权的替换的保护；

——与功能要求的一致性。

注2：应在以下方面对应用程序数据进行验证：

——与数据结构的一致性；

——完整性；

——与基础系统软件的兼容性(如执行顺序、运行时间)；

——数据值的正确性；

——在已知的安全边界内运行。

注3：应对可修改的参数进行验证，以防止下列方面：

——无效的未定义的初始值；

——误差值；

——未经授权的更改；

——数据讹误。

注4：应在以下方面对通信接口、过程接口和相关软件进行验证：

——失效检测；

——防止报文讹误；

——数据确认。

12.7.2.4 应在下列方面对和安全信号和安全功能集成在一起的非安全功能和过程接口进行验证：

——不干扰安全功能；

——在非安全功能出现故障的情况下可防止干扰安全功能。

13 工厂验收测试(FAT)

注：本章为资料性部分。

13.1 目的

13.1.1 工厂验收测试(FAT)的目的是一起测试逻辑解算器及其相关的软件，以保证它能满足安全要求规范中所定义的要求。通过安装在工厂之前测试逻辑解算器及其相关软件，能够较容易地识别和纠正误差。

注：工厂验收测试有时又称为集成测试，并且可以是确认的一部分。

13.2 建议

13.2.1 在工程项目设计阶段就应规定需要进行一次工厂验收测试(FAT)。

注1：为了编写集成测试，可能需要逻辑解算器供货商和设计承包商之间紧密协作。

注2：这些活动应紧随设计和开发阶段之后并在安装和调试运行之前进行。

注3：这些活动适用于装有或未装可编程电子的SIS子系统。

注4：FAT通常是在安装在车间和调试之前在工厂环境下进行。

13.2.2 编制FAT计划应规定：

——要执行的测试类型，包括黑盒系统功能性测试(即把系统视为一个“黑盒”的测试设计方法，从而无需使用系统内部结构知识，通常黑盒测试设计主要测试功能要求，黑盒测试的同义词包括：行为测试、功能性测试、不透明盒测试，以及密封盒测试)、性能测试(定时、可靠性和可用性、完整性、安全目标和约束)、环境测试(包括EMC、寿命和应力测试)、接口测试、在各种降级和/或故障模式下进行的测试、异常状态下的测试、SIS维护和操作手册的应用。

——测试用例、测试描述和测试数据。

注：落实谁负责制定测试用例、谁负责执行测试和见证测试是非常重要的。

——与其他系统接口的依赖性。

——测试环境和工具。

——逻辑解算器配置。

——判断测试完成的测试准则。

——测试失败时采取的改正动作的规程。

——测试人员的胜任资格。

——实际的场地。

注：对于实际上不能演示的测试，通常应提供一个正式的论据，来说明为什么SIS达到了要求、目标或约束。

13.2.3 应在逻辑解算器的一个已定义版本上进行FAT。

13.2.4 应按照FAT计划编制进行FAT。这些测试应显示能正确执行所有的逻辑。

13.2.5 为了执行每项测试应涉及：

——所使用的测试计划编制的版本；

——所测试的仪表安全功能和性能的特性；

——详细的测试规程和测试描述；

——按日期编排的测试活动的记录；

——使用的工具、设备和接口。

13.2.6 FAT的结果应被文档化，文档中应说明：

a) 测试用例；

b) 测试结果；

c) 是否满足测试准则的目的和准则。

如果测试过程中出现失败，则应把失败原因编入文档，并应进行分析，采取相应的改正动作。

13.2.7 在FAT过程中，任何修改或变更都应经过安全分析以确定：

a) 对每个仪表安全功能的影响程度；

b) 应被定义和实现的重新测试的范围。

注：根据FAT的结果，在采取改正动作的同时可进行调试运行。

14 SIS安装和调试运行

14.1 目的

14.1.1 本章的目的是：

——根据规范和图纸安装安全仪表系统；

——调试安全仪表系统以便为最终的系统确认做好准备。

14.2 要求

14.2.1 安装和调试运行计划编制应定义安装和调试运行所需的所有活动。计划编制应提供：

——安装和调试运行活动；

——安装和调试运行所使用的规程、措施和技术；

——何时进行这些活动；

——负责这些活动的人员、部门和组织。

在合适的情况下，可把安装和调试运行计划编制整合到整个工程项目计划编制中。

14.2.2 应按设计和安装计划正确安装安全仪表系统的所有部件(见14.2.1)。

14.2.3 应根据计划编制调试运行安全仪表系统，以用于最终的系统确认。调试运行活动应包括(但不限于)证实：

——已正确接地；

——已正确接通电源并可供电；

——已停止搬运并已拆除包装材料；

——无物理损伤；

——已正确校准好所有的仪表；

——所有现场装置都可供使用；

——逻辑解算器和输入/输出可供使用；

——到其他系统和外设的接口可供使用。

14.2.4 应产生SIS调试运行的相应记录，说明测试结果以及在设计阶段所确定的目的和准则是否得以满足，如果调试运行中出现失败，则应记录失败的原因。

14.2.5 对实际上并不依据设计信息进行安装的情况，应由有资格的人员对其差异进行评价，并确定可能对安全产生的影响。如已确定这种差异对安全没有影响，则应把设计信息更新为“竣工(as-built)”状况，如果这种差异对安全有负面影响，则应修改安装来满足设计要求。

15 SIS安全确认

15.1 目的

15.1.1 本章的目的是通过审查和测试来确认安装和调试好的安全仪表系统及相关的仪表安全功能达到了安全要求规范中所声明的那些要求。

注：有时也把这称为一种现场验收测试(SAT)。

15.2 要求

15.2.1 编制SIS确认计划应定义确认所需的所有活动。活动项目应包括：

——在安全要求规范方面对安全仪表系统进行确认在内的确认活动，这包括由此产生的建议的实现和决定。

——过程及其相关设备的所有有关的操作模式的确认，包括：

- 为使用所作的准备工作，包括设置和调整；
- 启动、自动、手动、半自动、稳定运行状态；
- 重置、停机、维护；
- 合理可预见的异常工况，例如通过风险分析阶段识别出的那些异常工况。

——确认所使用的规程、措施和技术。

——何时进行这些活动。

——负责这些活动的人员、部门和组织，以及确认活动的独立性水平。

——执行确认活动所依据的引用信息(如因果图)。

注：确认活动的例子包括回路测试、校准规程和应用软件仿真。

15.2.2 编制安全应用软件附加确认计划应包括：

a) 在开始调试运行之前需在每种过程操作模式下进行确认的安全软件的标识。

b) 有关确认的技术策略的信息，包括：

——手动和自动技术；

——静态和动态技术；

——分析和统计技术。

c) 根据b)，为证实每个仪表安全功能符合规定的软件仪表安全功能(见12.2)要求和规定的软件安全完整性要求(见12.2)，应使用的措施(技术)和规程。

d) 进行确认活动所要求的环境(例如，为了测试，要求包括校正工具和设备)。

e) 为完成软件确认所需的通过/失败准则，包括：

——要求的过程和操作员输入信号以及它们的顺序和值；

——预期的输出信号以及它们的顺序和值；

——其他验收准则，如存储器用法、定时和值的容差。

f) 评价确认结果(特别是失败)的策略和规程。

注：这些要求基于12.2的一般要求。

15.2.3 在要求把测量精度作为确认的一部分时，应对照一个可追溯到某个标准的规范，把用于此功能的仪表校准到适合该应用的某个不确定度范围内。如果这种校准不可行，则应使用一种替代方法并文档化。

15.2.4 应根据安全仪表系统确认计划编制对安全仪表系统及其相关的仪表安全功能进行确认。确认活动应包括(但不限于)：

——如安全要求规范中标明的那样，在正常和异常操作模式(如启动和停机)下安全仪表系统都能履行其职能；

——证实基本过程控制系统和连接的其他系统的相互作用，不会对安全仪表系统的正确运行产生不利的影响；

——安全仪表系统能同基本过程控制系统或任何其他系统或网络正确地通信；

——传感器、逻辑解算器和最终元件，包括所有冗余通道，按安全要求规范运行；

注：如果已按第13章对逻辑解算器进行过工厂验收测试(FAT)，也可以把FAT认作是对逻辑解算器的确认。

——安全仪表系统文档应与被安装的系统相符；

——证实能按照规定对无效过程变量值(如超出范围)执行仪表安全功能；

——建立正确的停机顺序；

——安全仪表系统提供正确的通告和运行显示；

——安全仪表系统中包含的计算是准确的；

——按安全要求规范中定义的那样执行安全仪表系统的复位功能；

——旁路功能正确运转；

——启动超驰正确操作；

——手动停机系统正确运转；

——在维护规程中已编入检验测试间隔；

——按要求的那样执行诊断报警功能；

——证实在中断共用设施供应(如电、空气和液压)时，能按要求的那样运转安全仪表系统，并证实当恢复供应时，安全仪表系统可返回到所期望的状态；

——证实已达到安全要求规范中所规定的EMC抗扰性。

15.2.5 软件确认应显示出所有规定的软件安全要求(见12.2)都能被正确执行，并且在SIS的故障工况下及降级操作模式下，或者在执行规范中未定义的软件功能性期间，软件都不会危害安全要求。应提供确认活动的信息。

15.2.6 应产生SIS确认结果的相应信息，它们包括：

——所使用的SIS确认计划编制的版本；

——被测试(或分析)的仪表安全功能，及其在SIS确认计划编制过程中被标识要求的特定引用；

——使用的工具和设备，及其校准数据；

——每次测试的结果；

——使用的测试规范的版本；

——集成测试的验收准则；

——被测试SIS硬件和软件的版本；

——预期的和实际的结果之间的任何差异；

——在出现差异的情况下，对差异所作的分析，以及对是否继续进行测试或是发布一个变更请求而作出的决定。

15.2.7 当预期的和实际的结果之间出现差异时，应把所作的分析和对是否继续进行测试或是发布一个变更请求并返回到开发生命周期的较早部分所作的决定当作安全确认的部分结果提供出来。

15.2.8 在安全仪表系统确认之后以及所存在的风险被识别出来之前，应进行下列活动：

——应返回所有旁路功能(如：对 PE 逻辑解算器和 PE 传感器的强制、禁止报警)的正常位置；

——应按过程起动要求和规程设置所有的过程隔离阀；

——应移除所有的测试材料(如流体)；

——应移除所有的强制，如适用还应消除所有强制使能。

16 SIS 操作和维护

16.1 目的

16.1.1 本章的目的是：

——保证在操作和维护过程中能保持所要求的每个仪表安全功能的 SIL；

——操作和维护 SIS 使之能保持设计的功能安全。

16.2 要求

16.2.1 应编制安全仪表系统的操作和维护计划。此计划应提供：

——例行的和异常的操作活动；

——检验测试活动、预防性维护和故障维修活动；

——操作和维护使用的规程、措施和技术；

——遵从操作和维护规程的验证；

——何时进行这些活动；

——负责这些活动的人员、部门和组织。

16.2.2 应根据相关的安全计划编制制定操作和维护规程，此规程应提供：

——为保持"同设计一样的"SIS 的功能安全所需执行的例行动作，例如遵从由 SIL 确定所定义的检验测试间隔；

——在维护或操作期间，为防止一个危险事件的不安全状态和/或减小事件后果需要采取的动作和约束(例如，为了测试或维护一个系统，何时需对它进行旁路，以及需实现何种附加缓解步骤)；

——需保留的系统失效以及对 SIS 的要求率的信息；

——显示对 SIS 进行审核和测试的结果需保持的信息；

——当 SIS 发生故障或失效时应遵从的维护规程，它包括：

- 故障诊断和修理规程；
- 重新确认规程；
- 维护报告要求；
- 跟踪维护性能的规程。

注：应考虑：

- 报告失效的规程；
- 分析系统失效的规程。

——保证在正常维护活动期间使用的测试设备已被正确校准和维护。

16.2.3 应根据相关规程进行操作和维护。

16.2.4 应就操作员所在领域内的 SIS 功能和操作对它们进行培训。这样的培训应保证它们能了解：

——SIS 怎样工作(脱扣点及 SIS 因此所采取的动作)；

——SIS 能预防的危险；

——所有旁路开关的操作以及在什么样的情况下才应使用这些旁路；

——任何手动停机开关的操作和手动起动活动以及何时才应启动这些手动开关；

注：也许还应包括"系统复位"和"系统重新起动"。

——对任何诊断报警的启动的预期行为(例如当启动任何 SIS 报警,从而指示 SIS 存在某种问题时,应采取什么样的动作)。

16.2.5 应按要求培训维护人员,使得 SIS(硬件和软件)的功能特性能维持它的目标完整性。

16.2.6 应分析预计的和实际的 SIS 行为之间的差异,必要时应作修改以保持要求的安全,这包括监视:

——紧随对系统提出要求后所采取的动作;

——在例行测试或者实际要求过程中作为 SIS 组成部分的设备所产生的失效;

——提出要求的原因;

——伪脱扣的原因。

注:分析预期行为和实际行为之间的所有差异是十分重要的。它不应同在正常运行中所遇到的监视要求相混淆。

16.2.7 操作和维护规程可能需要修订,有必要时应在修订后进行:

——功能安全审核;

——SIS 测试。

16.2.8 应编写每个 SIF 的书面检验测试规程,以便揭露诊断未检测到的危险失效。这些书面的测试规程应描述需要执行的每个步骤并应包括:

——每个传感器和最终元件的正确操作;

——正确的逻辑动作;

——正确的报警和指示。

注:下面的方法可用来确定需被测试的未检测到的失效:

- 故障树检查;
- 失效模式和影响分析;
- 以可靠性为核心的维护。

16.3 检验测试和检查

16.3.1 检验测试

16.3.1.1 应使用一个书面的规程(见 16.2.8)进行定期的检验测试以便揭露未检测到的故障,这种故障会阻碍 SIS 按安全要求规范操作。

16.3.1.2 应测试包括传感器、逻辑解算器和最终元件(如停机阀和电机)在内的整个 SIS。

16.3.1.3 检验测试频率应同使用 PFD_{avg} 计算所决定的一样。

注:SIS 的不同部分可能要求不同的测试间隔,例如,逻辑解算器的测试间隔可能与传感器或最终元件的不同。

16.3.1.4 应以一种安全和及时的方式修复检验测试过程中发现的任何缺陷。

16.3.1.5 应以某些定期的间隔(由用户确定),根据各种因素,包括:历史测试数据、工厂经验、硬件降级和软件可靠性等,重新评价测试频率。

16.3.1.6 应用逻辑的任何改变都需要进行全面检验测试。只有在进行过适当的复审,以及对改变的部分进行测试以保证能正确地实现改变时才允许有例外。

16.3.2 检查

应对每个 SIS 进行定期目视检查,以保证不存在未经授权的修改和可观察到的缺损(如缺螺栓或仪表罩、固定架生锈、线断开、管道破裂、加热保温层破损、绝缘缺失)。

16.3.3 检验测试和检查的文档

用户应保存可证实检验测试和检查已按要求完成的记录,这些记录至少应包括以下信息:

a) 执行的测试和检查的说明;

b) 测试和检查的日期;

c) 执行测试和检查的人员姓名;

d) 被测系统的序列号或者别的惟一标识符(如回路号、工位号、设备号和 SIF 号);

e) 测试和检查的结果(如"发现 as-found"和"听任 as-left"状况)。

17 SIS 修改

17.1 目的

17.1.1 本章的目的是:

——在对任何安全仪表系统进行修改之前应正确编制修改计划并对修改进行复审和批准;

——保证不管 SIS 作何改变都能保持所要求的 SIS 安全完整性。

注:应对 BPCS、其他设备、过程和操作条件的修改进行复审,以确定它们的这种修改是否会对 SIS 的要求特性和频率造成影响。应进一步考虑有不利影响的那些修改,以确定风险降低水平是否依然足够。

17.2 要求

17.2.1 在对安全仪表系统进行修改之前,授权和控制更改的规程应到位。

17.2.2 规程应包括确定和请求要作的工作的简明方法,以及可能会受到影响的危险。

17.2.3 应进行一次分析,以确定所建议的修改结果对功能安全的影响。当分析显示所建议的修改将影响安全时,则应返回安全生命周期的第一个受修改影响的阶段。

17.2.4 未经正式授权不得开始修改活动。

17.2.5 对 SIS 的所有更改都应保留相应的信息。这些信息包括:

——修改或更改的描述;

——更改的理由;

——可能会受影响的已确定的危险;

——修改活动对 SIS 的影响的分析;

——更改要求的所有批准;

——验证所有更改已正确实现,以及 SIS 按要求执行所使用的测试;

——相应的配置历史;

——验证所有更改不会对未修改的 SIS 组成部分产生不利影响所使用的测试。

17.2.6 应由经过适当培训的合格人员来执行修改。包括所有受影响的和适当的人员被通知变更,并应就更改对它们进行培训。

18 SIS 停用

18.1 目的

18.1.1 本章的目的是:

——保证任何安全仪表系统在停用之前要对它进行一次正确的复审,并应得到必要的授权;

——保证在停用活动过程中保持要求的仪表安全功能继续运行。

18.2 要求

18.2.1 在执行一个安全仪表系统的任何停用之前,授权和控制更改的规程应到位。

18.2.2 规程应包括确定和请求要作的工作的简明方法,以及可能会受到影响的危险。

18.2.3 应分析由于所建议的停用活动结果对功能安全的影响。评估应包括危险和风险评估的更新,该更新应足以确定其后应重新执行的安全生命周期各阶段的深度和广度。评估还应考虑:

——在执行停用活动过程中的功能安全;

——停用某个安全仪表系统对相邻的操作单元和设施服务的影响。

18.2.4 在编制安全计划来重新启用 GB/T 21109.1 的相关要求(包括重新验证和重新确认)的过程中,应使用影响分析的结果。

18.2.5 未经正式授权不得开始停用活动。

19 信息和文档要求

19.1 目的

19.1.1 本章的目的是：

——保证能提供必要的信息并把这些信息文档化，以便能有效地执行安全生命周期的所有阶段；

——保证能提供必要的信息并把这些信息文档化，以便能有效地执行验证、确认和功能安全评估活动。

注1：文档结构的例子参见GB/T 20438.1—2006附录A，更详细的信息参见IEC 61506。

注2：文档可采用不同的形式(如书面、胶片或者显现在屏幕或显示器上的任何数据媒体)。

19.2 要求

19.2.1 应提供本部分要求的文档。

19.2.2 文档应：

——描述安装、系统或设备及其使用；

——准确；

——容易理解；

——适合它所预定的目的；

——以一种可访问和可维护的形式提供。

19.2.3 文档应有惟一的标记从而有可能引用不同的部分。

19.2.4 文档应有名称以表示信息类型。

19.2.5 文档应可追溯到本部分的要求。

19.2.6 文档应有一个版本索引(版本号)使之能够辨认不同的版本信息。

19.2.7 文档结构应使之能搜索有关信息。应能标识一个文档的最新修订(版本)。

注：文档实际结构随一系列因素(如系统大小、复杂程度和组织要求)而变。

19.2.8 所有相关文档都应被修订、补充、复审和批准，并处于一个合适的信息控制模式的控制之下。

19.2.9 应维护与以下有关的当前文档：

a) 危险和风险评估的结果及相关假设；

b) 用于仪表安全功能的设备连同对它的安全要求；

c) 负责保持功能安全的组织；

d) 为达到和保持SIS功能安全所必需的规程；

e) 17.2.5中定义的修改信息；

f) 设计、实现、测试和确认。

注：在第14章和第15章中包含有对信息的更详细的要求。

附 录 A
（资料性附录）
差 异

本附录说明了 GB/T 21109 和 GB/T 20438—2006 之间的关键差异。

GB/T 21109 同 GB/T 20438—2006 有一些不同。在 A.1 和 A.2 中讨论了这些差异，这些差异是根据对比这两个标准的当前版本得出的，见表 A.1 和表 A.2。

A.1 组织上的差异

表 A.1 组织上的差异

GB/T 20438—2006	GB/T 21109	注释
第 1 部分	第 1 部分	GB/T 20438—2006 第 1～4 部分已结合进本部分
第 2 部分	第 1 部分	包含在本部分中
第 3 部分	第 1 部分	包含在本部分中
第 4 部分	第 1 部分	包含在本部分中
第 5 部分	第 3 部分	包含在 GB/T 21109.3 中
第 6 部分	第 2 部分	本部分的指南
第 7 部分	所有部分	每个部分作为附录被包含在资料性引用文件中(需要时)

A.2 术语

表 A.2 术语上的差异

GB/T 20438—2006	GB/T 21109 的本部分	注释
E/E/PE 安全相关系统	SIS	GB/T 20438—2006 称为 E/E/PE 安全相关系统，而 GB/T 21109则称为安全仪表系统
PES	SIS	GB/T 20438—2006 中"PES"包含传感器和最终控制元件，而 GB/T 21109 则使用术语 SIS
过程控制系统	基本过程控制系统	对于过程领域而言，基本过程控制系统是一个全局性的术语
EUC	过程	GB/T 20438—2006 称为 EUC(受控设备)，而 GB/T 21109 则称为过程
安全功能	仪表安全功能(SIF)	GB/T 20438—2006 中由 E/E/PES、其他技术的安全相关系统、或者外部风险降低设施实现安全功能。GB/T 21109 中，单独由 SIS 实现 SIF

参 考 文 献

[1] IEC 60050-191:1990 国际电工词汇 第191章:可靠性和服务质量
[2] IEC 60050-351:1998 国际电工词汇 第351部分:自动控制
[3] IEC 60617-12:1997 简图用图形符号 第12部分:二进制逻辑元件
[4] IEC 61131-3:1993 可编程控制器 第3部分:编程语言
[5] IEC 61506:1997 工业过程测量和控制 应用软件的文件编制
[6] 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
[7] IEC 61508-4:1998 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
[8] IEC 61508-6:2000 电气/电子/可编程电子安全相关系统的功能安全 第6部分:IEC 61508-2和IEC 61508-3的应用指南
[9] GB/T 21109.3—2007 过程工业领域安全仪表系统的功能安全 第3部分:确定要求的安全完整性等级的指南
[10] ISO/IEC 2382(所有部分) 信息技术 词汇
[11] ISO/IEC 2382-1:1993 信息技术 词汇 第1部分:基本术语
[12] ISO/IEC 指南51:1999 安全方面 在标准中引入安全条款的指南
[13] ISO 9000:2000 质量管理系统 基础和词汇
[14] ISO 9000-3:1997 质量管理和质量保证标准 第3部分:ISO 9001:1994应用于计算机软件开发、供应、安装和维护的指南