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

中华人民共和国
国家标准
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
GB/T 21109.1—2007/IEC 61511-1:2003
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 4.25 字数 119千字
2008年1月第一版 2008年1月第一次印刷
*
书号:155066·1-30411 定价 42.00元

GB/T 21109.1-2007

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。

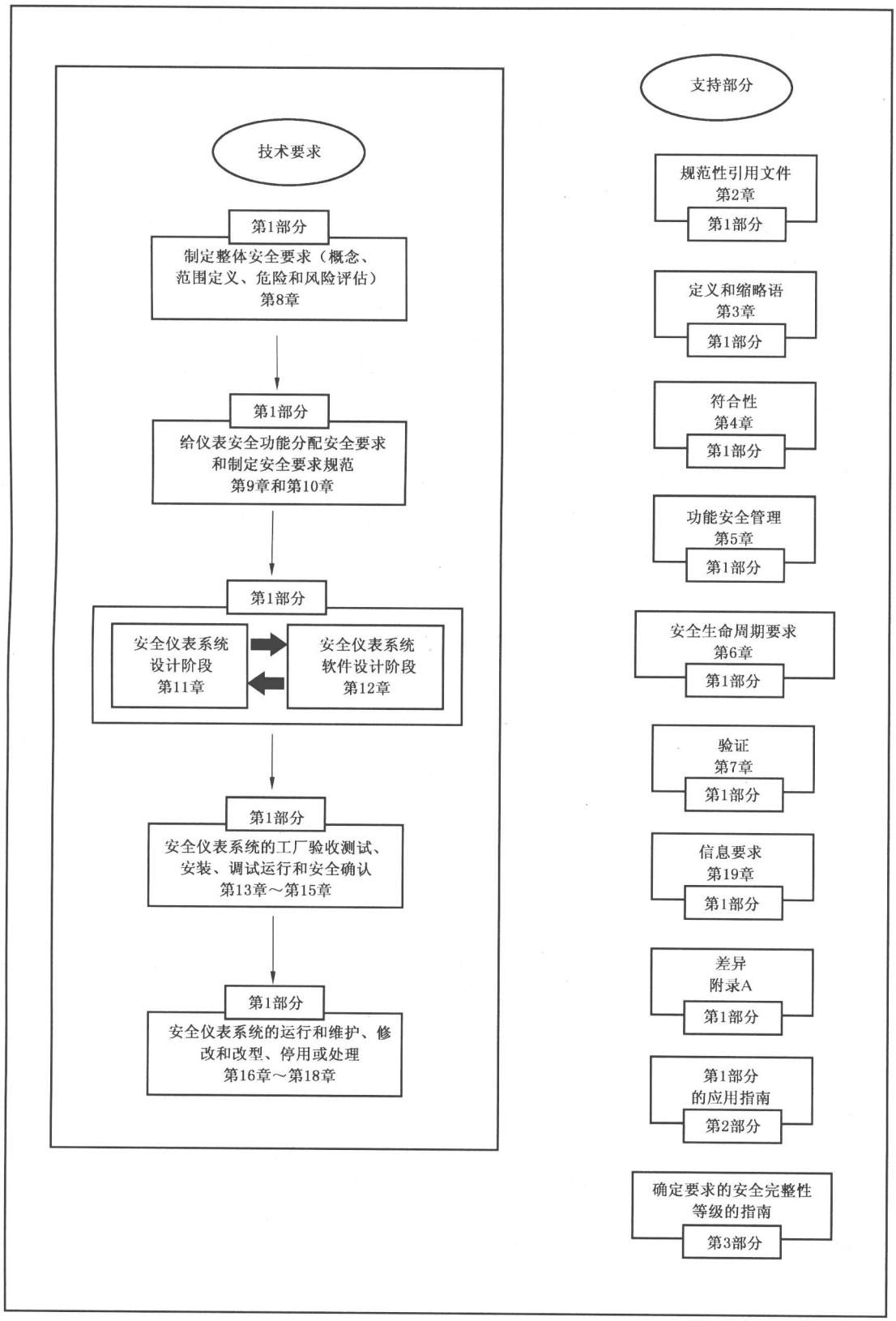

图 1　GB/T 21109 的整体框架

目　次

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。

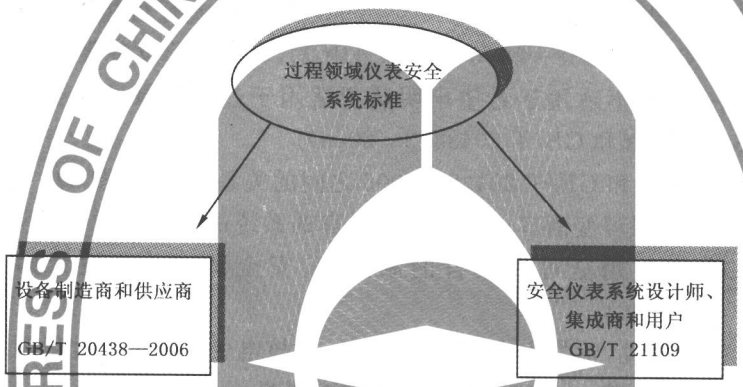

图 2 GB/T 21109 与 GB/T 20438—2006 的关系

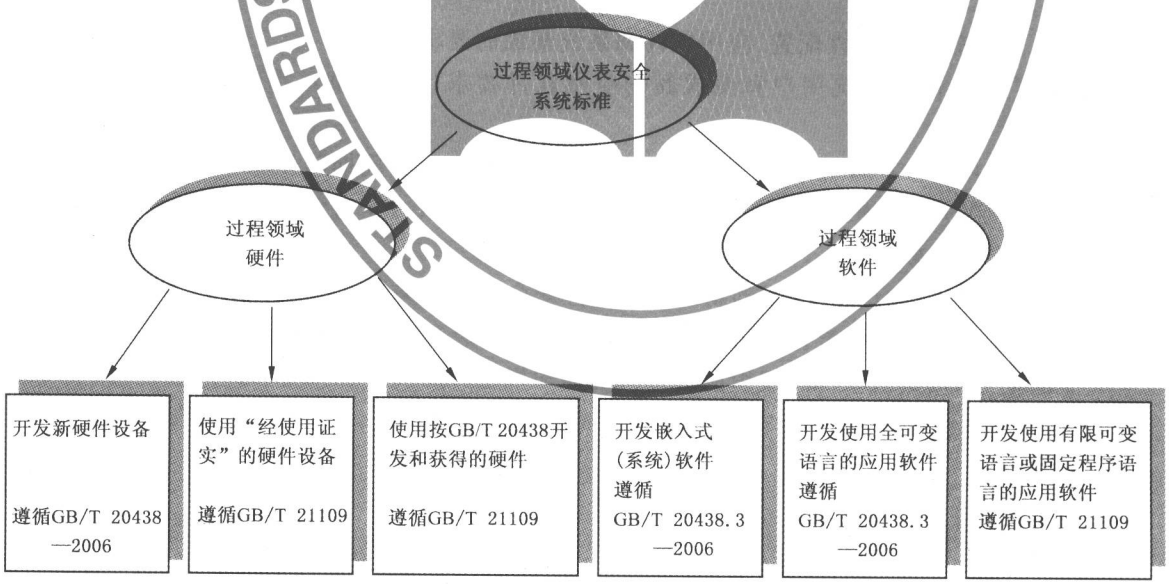

图 3 GB/T 21109 与 GB/T 20438—2006 的关系(见第 1 章)

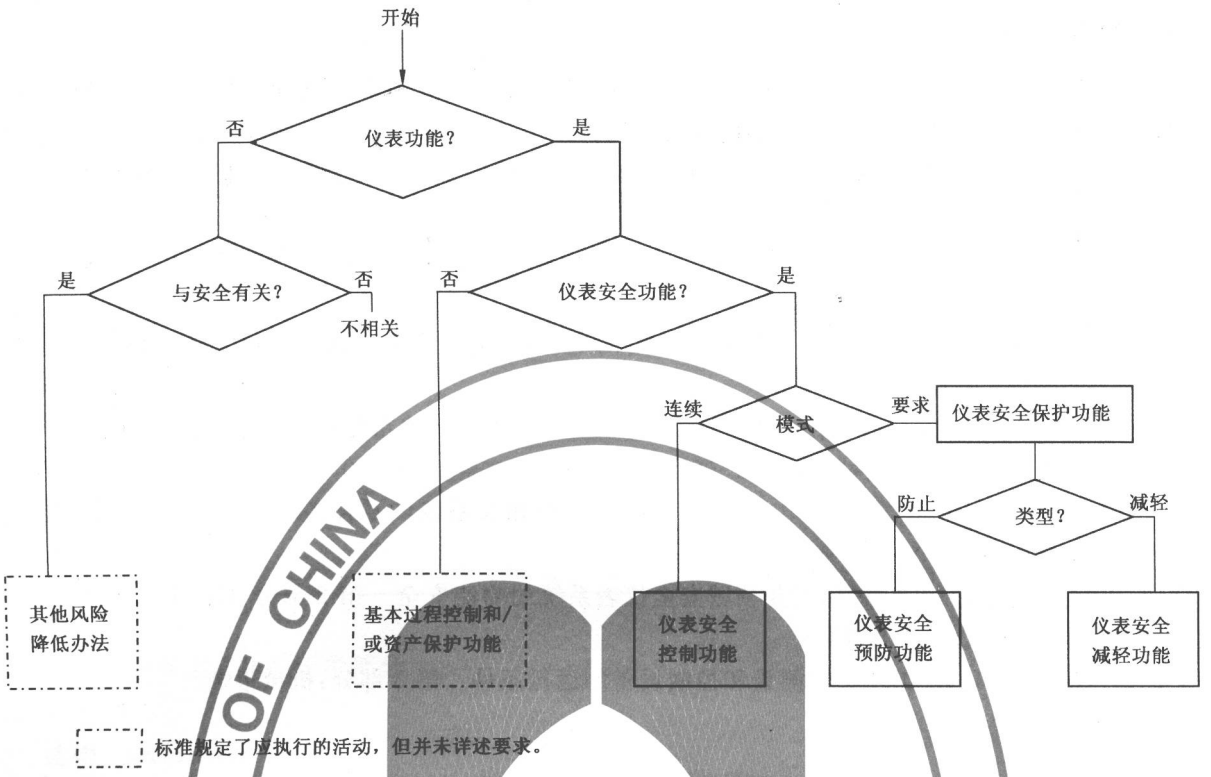

图 4 仪表安全功能和其他功能的关系

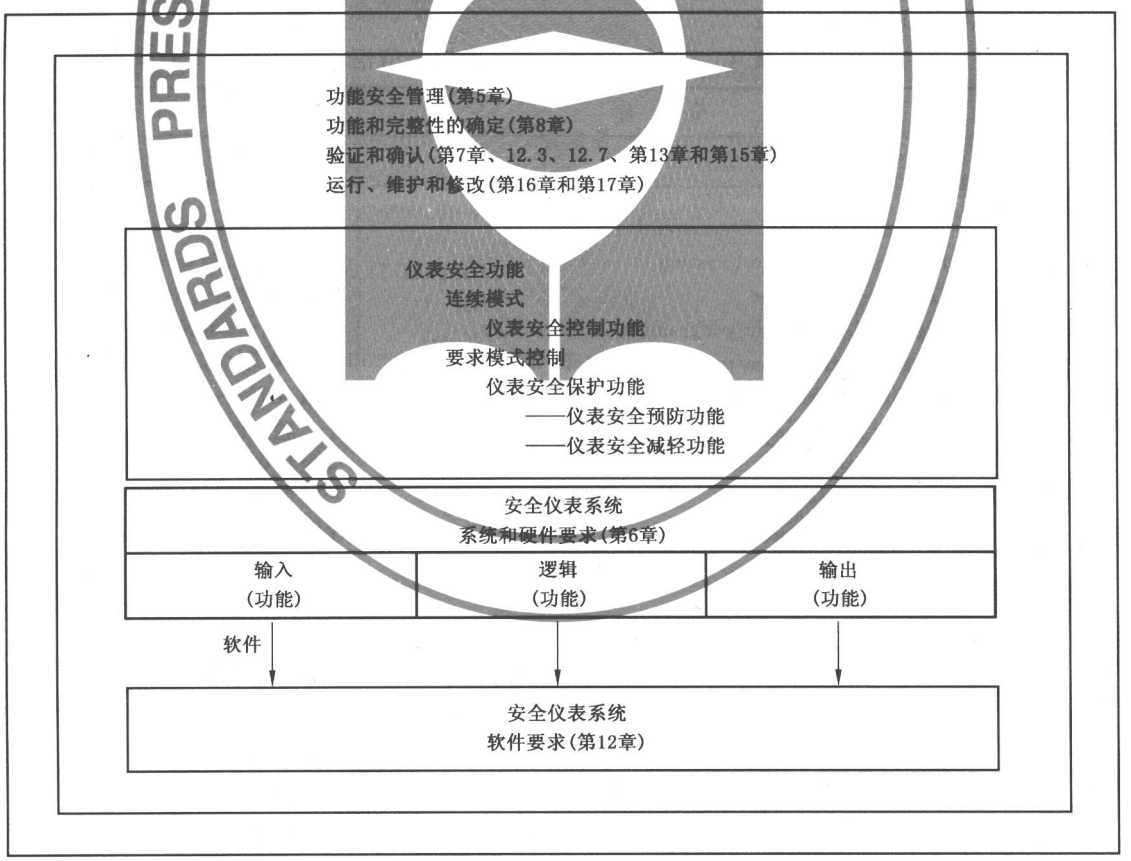

图 5 本部分的系统、硬件和软件的关系

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)；

——固态非可编程电子装置(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。