ICS 25.040
N 10

中华人民共和国国家标准

GB/T 21109.2—2007/IEC 61511-2:2003

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

Functional safety—Safety instrumented systems for the process industry sector—Part 2:Guidelines for the application of GB/T 21109.1

(IEC 61511-2:2003,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2部分:GB/T 21109.1的应用指南
GB/T 21109.2—2007/IEC 61511-2:2003
*
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 3.75 字数 101千字
2008年1月第一版 2008年1月第一次印刷
*
书号:155066·1-30412 定价 38.00 元

GB/T 21109.2—2007/IEC 61511-2:2003

GB/T 21109.2-2007

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2部分，等同采用IEC 61511-2:2003《过程工业领域安全仪表系统的功能安全　第2部分：IEC 61511-1的应用指南》(英文版)。为便于使用，对IEC 61511-2:2003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、附录B、附录C、附录D、附录E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,来处理安全仪表系统和其他安全系统间的接口。安全仪表系统包括传感器、逻辑解算器和最终元件。

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。安全生命周期形成了核心框架,从而将本部分的大多数概念连接在一起。

安全仪表系统逻辑解算器包括电气(E)/电子(E)/可编程电子(PE)技术。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 GB/T 21109.1—2007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。本部分的目的是提供如何符合本部分的指南。

为了方便 GB/T 21109 的使用,提供的章、条号与GB/T 21109.1(附录除外)中对应的规范性内容相一致。

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、热力学的(如灭火器)、可编程电子的)。任何安全策略都需要将每个单独的安全仪表系统放在其他保护系统环境下进行考虑。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;

——给安全功能和相关安全系统(如安全仪表系统)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。

GB/T 21109 的整体框架见图 1。

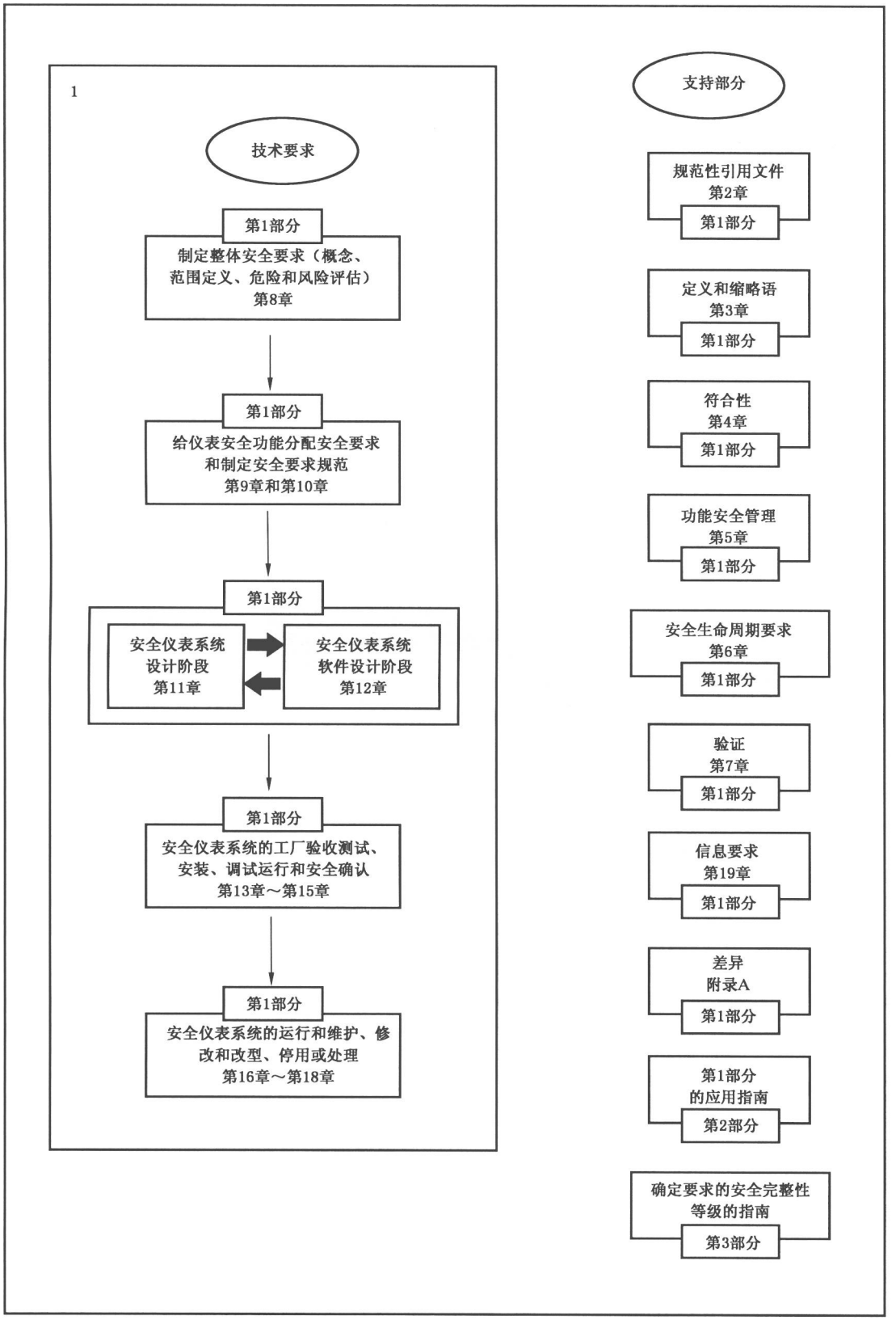

图 1　GB/T 21109 的整体框架

目　次

过程工业领域安全仪表系统的功能安全 第2部分:GB/T 21109.1的应用指南

1 范围

本部分提供了按GB/T 21109.1中定义的仪表安全功能及其相关的安全仪表系统的规范、设计、安装、操作和维护的应用指南。为了方便GB/T 21109的使用,提供的章、条号与GB/T 21109.1(附录除外)中对应的规范性内容相一致。

2 规范性引用文件

见GB/T 21109.1。

3 术语、定义和缩略语

术语、定义和缩略语见GB/T 21109.1。GB/T 21109.1—2007中以下两条术语在本部分中做了补充说明。

3.2.68

安全功能 safety function

一个安全功能应能防止一个特定的危险事件。例如"防止压力容器#ABC456中压力超过100 bar"。可以通过下列办法达到这个安全功能:

a) 单独一个安全仪表系统(SIS);或者

b) 一个或几个安全仪表系统和/或其他的保护层。

在情况b)中,每个安全仪表系统或其他的保护层应有达到安全功能的能力并且组合整体一定要达到要求的风险降低(过程安全目标)。

3.2.71

仪表安全功能 safety instrumented function

仪表安全功能源于安全功能,仪表安全功能具有一个相关联的安全完整性等级(SIL)并由一个特定的安全仪表系统来执行它。例如"当压力容器#ABC456中的压力达到100 bar时,在5 s内关闭阀门#XY123"。多个仪表安全功能有可能使用同一个安全仪表系统的部件。

4 与GB/T 21109的符合性

见GB/T 21109.1。

5 功能安全管理

5.1 目的

GB/T 21109.1—2007第5章的目的是为保证满足功能安全目标必需实现的管理活动提供要求。

5.2 要求

5.2.1 概述

5.2.1.1 见GB/T 21109.1。

5.2.1.2 当一个组织负责执行功能安全所必需的一项或几项活动,并且该组织按照质量保证规程进行工作时,则出于质量的目的,本章中描述的许多活动将要被执行。在这种情况下,对功能安全来说,没有

必要重复这些活动。但应对质量保证规程进行复审，以确定它们对达到功能安全目标是合适的。

5.2.2 组织和资源

5.2.2.1 应定义一个公司/现场/工厂/工程项目范围内与安全仪表系统有关联的组织结构，并应清楚地了解和互通每个组成部分的作用和职责。应确定结构内的各个角色，包括它们的描述和目的。应清楚地标明每个角色的责任；并判明各自的特殊职责。此外，还应标明各个报告提交给谁和委派谁来写报告。目的是保证组织中的每一个人都要了解它们对安全仪表系统而言所扮演的角色以及它们的职责。

5.2.2.2 应确定为实现与安全仪表系统有关的安全生命周期的任何活动所需的技能和知识；并应确定每种技能所要求的能力水平。应根据可胜任的每种技能以及每种技能所需的人数对资源进行评估。当查明有差异时，应制定一个开发计划使之能及时地达到要求的胜任能力水平。当出现技术力量短缺时，可招收或签约合格的有经验人员。

5.2.3 风险评价和风险管理

GB/T 21109.1—2007的5.2.3中规定的要求是确定危险、评价风险并确定必要的风险降低。公认的进行这些评价的适用方法有很多种。GB/T 21109.1并未认同任何一种特殊的方法。换句话说，在GB/T 21109.3中鼓励读者就这一问题对这些方法进行复审。

5.2.4 计划编制

本条的目的是要保证在整个项目范围内，实施适当的安全计划编制以便论述生命周期每个阶段所要求的活动(例如工程设计、工厂运行)。本部分未要求任何特殊结构用于这些计划编制活动，但它强调要求定期更新或复审这些活动。

5.2.5 实现和监视

5.2.5.1 本条的目的是要确保有效的管理规程能到位从而：

——保证危险分析、风险评估、其他评估和审核活动、验证和确认活动产生的建议得以圆满解决。

——确定SIS在它的整个工作寿命期内都能按安全要求规范运行。

5.2.5.2 在本部分中，供货商可能还包括设计承包商和维护承包商以及部件供货商。

5.2.5.3 应定期对SIS的性能进行复审，以保证在开发安全要求规范(SRS)过程中仍然遵守原来的设想。例如，应对SIS中的各个部件假设的失效率进行定期的复审，以保证它保持同初始定义相同。如果失效率比初始预计的更差，则有必要修改设计。同样还应对SIS的要求率进行复审。如果对SIS的要求率大于最初假定值，则可能需要对SIL进行调整。

5.2.6 评估、审核和修订

评估和审核是以误差检测和消除为目标的手段。后续段落阐明了这些活动之间的差别。

功能安全评估的目的是评价在所评估的各生命周期阶段中为实现安全所做的准备是否充分。评估者应对负责实现功能安全人员所作的决定作出判断。例如：在调试运行之前应对维护规程是否充分作一次评估。

功能安全审核人员应通过工程项目记录或者工厂记录来确定是否是具有必要资格的人员以规定的频率使用必要的规程。不要求审核者对它们考虑的工作的充分性作出判断。然而，如果它们发觉更改有益，则应在报告中包括对此的一个说明。

在许多情况下，评估者和审核者的工作之间有可能重迭。例如，一个审核者可能不仅需要确定一个操作员是否已得到必要的培训，而且还要对培训是否使操作员达到了要求的胜任能力作出判断。

5.2.6.1 功能安全评估

5.2.6.1.1 功能安全评估(FSA)的使用是证明一个安全仪表系统(SIS)满足仪表安全功能和安全完整性等级(SIL)要求的基础。这种评估的基本目的是通过系统开发过程的独立评估来证明符合一致同意的标准和惯例。在各个生命周期阶段，可能都需要对SIS进行一次评估。为了进行一次有效的评估，应拟定一个定义该评估范围的规程以及评估组组成的指南。

良好的功能安全评估(FSA)惯例应考虑以下属性：

——对每个功能安全评估(FSA)都应拟制一个计划,这个计划应根据评估范围、评估人员、评估人员的能力以及评估将产生的信息来编排。

——FSA 应考虑到公司外部或者内部的标准、指南、规程或编程习惯(codes of practice)范围内所包含的标准和作法。FSA 计划应定义对于特定的评估/系统/应用领域应评估些什么。

——在不同的系统开发过程,功能安全评估的频次可能改变,但至少在系统面临潜在危险之前应进行一次 FSA。有些公司也可能在构建/安装阶段之前进行一次评估,以防止在生命周期的较后阶段出现高成本的返工。

——在定义 FSA 频次和严密性时应考虑以下系统属性:

- 复杂程度;
- 安全重要性;
- 类似系统以往的经验;
- 设计特征的标准化。

——在评估之前应提供足够的设计、安装、验证和确认活动的证据。足够证据的可用性本身可能是一个评估准则。证据应代表系统设计或安装的当前/认可状态。

——评估者的独立性一定要合适。

——评估者应具有适合于所评估系统的技术和应用领域的经验和知识。

——在整个生命周期和对所有系统而言,实现 FSA 的方案都应保持系统性和一致性。FSA 是一种主观的活动,为了尽可能多地消除主观性,可以使用检查列表来定义一个组织可接受活动的详细指南。

FSA 产生的记录应是完整的,并且在生命周期下一阶段开始之前,评估结论应同负责 SIS 功能安全管理人员的意见一致。

5.2.6.1.2 为了增强评估的客观性,需要独立于项目组的评估人员。需要高级(例如经验、等级、职位)评估人员,以保证它们所关心的问题能被适时的关注和涉及。进一步建议,对于某些大型项目组或评估组,可能有必要拥有多个独立于初始项目组的高级人员。

根据公司组织结构和公司内部的专家意见,也许不得不通过外部组织来满足对独立评估人员的要求。相反地,对于熟练进行风险评估及安全仪表系统应用的内部组织的公司可使用它们本身的资源来满足独立组织的要求,当然这样的内部组织应独立于负责项目的那些组织并在管理和其他资源方面是同负责项目的那些组织分开的。

5.2.6.1.3 评估量与工程项目的规模和复杂程度有关。在同一时间可以对不同阶段的结果进行评估。在正在运行的工厂中改变不大的情况下尤其可能。

5.2.6.1.4 在某些地区,在阶段 3 进行的功能安全评估常被称为起动前的安全复审(Pre-Startup-Safety-Review(PSSR))。

5.2.6.1.5 见GB/T 21109.1。

5.2.6.1.6 见GB/T 21109.1。

5.2.6.1.7 评估组应能得到它们执行评估所需要的任何信息。这包括从设计阶段一直到安装、调试运行和确认阶段所作的危险和风险评估得到的信息。

5.2.6.2 审核和修订

5.2.6.2.1 本条给出有关审核的指南,并通过一个例子来说明相关活动。

a) 审核类别

安全仪表系统的审核可给工厂管理、仪表维修工程师和仪表设计工程师提供有用的信息。这使管理具有前瞻性,以及使之能了解它们的安全仪表系统的实现程度和有效性。存在有许多种能执行的审核类型。任何特殊活动审核的实际类型、范围和频率应反映该活动对安全完整性的潜在影响。

审核类型包括：

1) 审核，包括独立审核和自审核；

2) 检查；

3) 安全巡视(例如工厂走查和事故(incident)复审)；

4) 安全仪表系统调查(通过调查表)。

需要在“监督和检查”以及审核活动之间进行区别。监督和检查的重点在于评价特定生命周期活动的性能(例如在部件恢复工作之前，监督员检查维修活动的完成)。相反，审核活动更广泛，并且主要集中在与安全生命周期有关的整个安全仪表系统的实现上。一次审核包括确定是否执行了监督和检查程序。

审核和检查可由公司/现场/工厂/项目的人员来执行(如自审核)，或由独立人员来执行(如公司的审核员、质量保证部门、调节员(regulator)、客户或者第三方)。

各级管理应使用相关类型的审核，以获取它们的安全仪表系统的实现有效性信息。来自审核的信息可用来确定可指导改进实现，但还未真正使用过的规程。

b) 审核策略

现场/工厂/项目实现审核的程序可以考虑滚动程序、独立程序或者自审核和检查程序。

应定期更新滚动程序，以便反映以往安全仪表系统的性能和审核结果，以及当前关心的问题和重点。这些包含了在一个适当的时段内和适当深度上，现场/工厂/项目有关的所有活动和安全仪表系统的所有方面。

进行审核的主要原因以及它所产生的附加价值在于对它们提供的信息及时采取动作。这些动作的目的是增强安全仪表系统的有效性。例如，有助于降低雇员或成员公众受伤害或致命的风险、有助于提高安全文明、有助于防止任何应避免释放的物质进入环境。

总之，审核策略可以拥有各种审核类型的组合，它是由管理(客户)产生的、并为了把相关的信息反馈给管理链以便及时动作。

c) 审核过程和协议

总的目的是使审核的效能达到最大。仅当各方(包括审核者、联络员、工厂经理和部门负责人等)了解每个审核的需要并能影响每个审核时，才能达到最大效能。以下审核过程和协议也许有助于确保达到这些目的的方案的某种一致性。它们涉及审核过程的下列5个关键阶段：

1) 审核策略和程序

应清楚地定义每个审核的目的以及确定审核组以及每个组的任务和职责。

应有一个审核策略。

应有一个审核程序。

应对审核过程、程序和策略的实现进行复审。

2) 审核准备和预编制

开始进行某个审核之前，应为现场/工厂/项目的高级经理和/或适当的审核协调员确定一位联络员。

在早期阶段审核人员和联络员应对以下问题进行讨论、理解并达成一致：

——审核的范围；

——审核的时间安排；

——需要参加的人员；

——审核的依据或者审核标准；

——为了增加审核的成功机率在准备阶段要作的额外工作和涉及到的工厂人员。

以下各项可用作每个阶段所需时间的指南：

——审核准备：30%；

——进行审核：40%；

——审核结果报告：20%；

——审核跟踪：10%。

审核员应为审核收集信息、规程/指令等，以及在适当的时候准备数据和编制检查列表。

如果发现严重的观察结果/缺陷，审核员应强调和解释在审核过程中审核范围发生改变的可能性。

3) 实施审核

审核员应在对现场/工厂/项目人员可能造成的干扰具有足够的认识后，在设定的审核时段内的几组连续工作日中实施审核。

对在审核过程中已确定的审查结果，应定期向联络员通报，以免在审核结束时感到意外。

在审核过程中，审核员应设法接近工厂人员，以便将知识和理解（过程和审查结果的）通告给物主（achieve ownership）。

审核员的风格对审核的成功是决定性的——他应努力作到有耐心、态度积极、有礼貌、精力集中和客观。

至少审核员应力图作到在改变商定好的范围和时间表时需经协商。

4) 审查结果报告

在审核结束时或稍后，但应在发布最终报告之前，审核员应举行一个结束会议。

应给相关的管理部门提供对草案报告和审查结果提意见的机会，如有要求可在正式的结束会议上进行讨论。

通常的作法是请求现场/工厂/项目的一份行动计划，以便提交报告的审查结果。

5) 审核跟踪

通常审核报告要求用一份行动计划的形式作出回应。只要合适，审核员可在预定日期或者下次审核时，验证行动完成的满意程度。

现场/工厂/项目跟踪系统可用来检验行动计划的实现。

应考虑每个审核组的审核结果的定期复审/总结，并就其结果进行广泛沟通。

审核结果/输出可用于复审审核的频次，并可用于安全仪表系统的管理复审的输入。

5.2.6.2.2 本条增强了变更管理在审核过程中所起的作用。

5.2.7 SIS 配置管理

5.2.7.1 要求

5.2.7.1.1 为了在整个生命周期内管理和保持装置的可追溯性，可以建立一种用于标记、控制和追踪每个装置的型号/版本的机制。

在安全生命周期最早可能的阶段，应给每台装置标上一个独特的工厂标识。在某些情况下，也可保留和控制仍在使用中的较早型号版本。这只是配置管理程序中的第一步，配置管理程序还应包括以下考虑。

配置管理系统可以包括：

a) 在生命周期的所有阶段，准备所有装置的标识规程。

b) 每台装置包括软件的型号/版本以及建造状况的独特标识，包括供货商、日期和应用地方、最初规定的型号/版本的变更情况。

c) 故障观察和审核产生的所有动作和改变的标识和跟踪。

d) 发布一个交付使用的版本的控制措施、标记相关装置的状况及型号/版本。

e) 已建立的安全防护措施,以确保在运行中的SIS不会遭受未经授权的变更/修改。

f) 每个软件项的版本标识,这些版本一起构成了一台完整装置的一个特定版本。

g) 提供在一个或多个工厂中多套SIS更新的协调。

h) 交付使用的书面授权。

i) 批准装置交付使用的一份签字批准的列表。

j) 阶段(stage/phase)装置被纳入配置控制之下。

k) 可交付使用的相关文档的控制。

l) 一台装置的每个型号/版本的标识:

——功能规范;

——技术规范。

m) SIS的管理和维护涉及的所有部门/组织的确定、职责分配及其理解。

6 安全生命周期要求

6.1 目的

任何过程设施中所达到的功能安全,都有赖于一系列活动的圆满执行。针对一个安全仪表系统采用一种系统的安全生命周期方法的目的,是确保能执行达到功能安全所必要的全部活动,以及保证能向其他人证明已按适当次序执行了这些活动。在GB/T 21109.1—2007的图8和表2中提出了一个典型的生命周期。在GB/T 21109.1—2007的第8章～第16章中给出了每个生命周期阶段的要求。

GB/T 21109考虑了如果遵守所有的要求,那么可以用不同的方法构建规定的活动。如果允许把安全活动较好地集成到常规的项目规程中,这种重新构建可能是有益的。GB/T 21109.1—2007的第6章的目的是当使用不同的安全生命周期时,确保已定义了生命周期每个阶段的输入和输出,及所有最基本的要求。

6.2 要求

6.2.1 考虑的关键是在事先定义将被使用的SIS安全生命周期。经验表明,除非事前对这个活动作了很好的计划并且所有人员、部门和组织对承担的职责达成了一致意见,否则有可能发生问题。出现问题时,最好的情况是某些工作被延误或不得不重做;最糟糕的情况是可能损害了安全。

6.2.2 虽然并没要求把建议的SIS安全生命周期(包括适用于项目的GB/T 21109.1—2007图8中的那些方框)映射到过程的项目生命周期上,但在某个早期阶段,这样做是有好处的。当作这件事时,应考虑开始某个安全生命周期活动所需的信息以及谁能提供这些信息。在某些情况下,直到设计阶段的后期,都不可能精确确定某个特殊问题的相关信息。在这种情况下,有必要根据以往经验进行估计,然后在稍后的某个时候再证实这些数据。如果存在这种情况,那么在安全生命周期中注意这点是很重要的。

6.2.3 安全生命周期计划编制的另一重要部分是确定在每个阶段将使用的技术。确定这些技术是重要的,因为通常需要使用某个专门的技术,这种技术要求人员或部门要具有独特的技能和经验。例如,在某个特定应用中的后果可能与失效事件后形成的最大压力有关;能够确定这种关系的惟一方法就是建立过程的动态模型。因此,动态建模的信息要求对设计过程将有重大影响。

7 验证

7.1 目的

验证的目的是要保证验证计划编制所确定的每个安全生命周期阶段的活动实际上已得到执行,并保证阶段的输出(无论是文档形式,还是硬件和软件形式)已被产生且适合它们的用途。

7.1.1 要求

7.1.1.1 GB/T 21109.1已考虑各个组织将有它们自己的验证规程，并且并不总是要求以同样的方式执行这些规程。换句话说，本条的目的是在事先就计划好所有的验证活动，连同任何会被使用的规程、措施和技术。

7.1.1.2 见GB/T 21109.1。

7.1.1.3 提供验证结果是重要的，这样可以证明在安全生命周期的各个阶段都已进行了有效的验证。

8 过程危险和风险评估

8.1 目的

本章的总体目标是确定用以保证过程安全所需的安全功能(如保护层)，及其相关性能水平(风险降低)。在过程领域中，使用多个安全层是常见的，这样在某一层失效时才不会导致或者允许产生有害的后果。在GB/T 21109.1—2007的图9中表示了典型的安全层。

8.2 要求

8.2.1 只能根据任务的结果来规定危险和风险评估的要求。这意味着组织可以使用它认为有效的任何技术，只要该项技术能得到安全功能及其相关性能水平的清楚描述。

危险和风险评估应确定和涉及在所有合理的可预见的情况下(包括故障工况和合理的可预见的误用)发生的危险和危险事件。

就过程领域的一个典型工程项目而言，需要在基本过程设计的初期就执行预先的危险和风险评估。在此阶段假设通过固有安全原理以及好的工程实践的应用，已把危险消除掉了或者已把危险降低到了合理可行的程度(在GB/T 21109的范围内不包含这种降低危险的活动)。对SIS而言，这种预先的危险和风险评估是很重要的，因为确立、设计和实现一个SIS是复杂的任务，需要占用相当长的时间。及早了解这个工作的另一理由是在完成过程和仪表图之前需要系统结构方面的信息。

一般只要完成了过程流程图和提供了所有的原始过程数据，启动预先危险和风险评估的信息就足够了。应该认识到当进行详细设计时，可能引入附加危险。因此，一旦完成了过程和仪表图，还有必要进行一次最终的危险和风险评估。一般这个最终的分析使用一个正式的和全文档化的规程，如危险和可操作性研究(HAZOP)。应证实所设计的安全层足以保证工厂的安全。在该最终分析期间，需考虑安全系统的失效是否会导致任何新的危险或者请求。如果在此阶段确定有任何新的危险，则有必要定义新的安全功能。另一较可能产生的结果是查明了可导致在初始阶段已识别危险的附加事件。于是需考虑是否需要对初始分析所确定的安全功能及其性能要求进行修订。

用来确定危险的方法取决于正在考虑的应用，对有些简单的过程来说，在对一种标准设计(如海上钻井平台)具有广泛操作经验的情况下，使用工业上编制的检查列表(例如ISO 10418和API RP 14C中的安全分析检查表)可能是足够的。在考虑更复杂的设计或是新的过程设计的情况下，有必要采用一种更结构化的方法(例如IEC 60300-3-9:1995)。

注：ISO 17776中给出了有关选择合适技术的其他信息。

当考虑特定失效事件的后果时，应分析所有可能的结果，及对结果产生影响的失效事件的频率。在风险分析中应忽略或去除不可靠的结果。使管道或压力容器承受超过设计的压力不一定会产生灾难性的污染损失。在许多情况下，设备都经过超过设计的压力试验，惟一可能导致火灾的后果是可燃物质的泄漏。在评价后果时，需咨询负责工厂机械完整性的人员。它们不但需要考虑原始试验压力还要考虑包括腐蚀允许量在内的原始设计以及腐蚀管理程序是否到位。在后果是基于这些假设的情况下，清楚地讲明这个问题是很重要的，这样就能把相关的规程结合到安全管理系统中。当考虑后果时，另外一个问题是许多人可能会受到某种特殊危险的影响。许多情况下，操作和维护人员只是偶尔在危险区域出现，在预测后果时应考虑到这一点。在使用这种统计方法时应注意并非对所有的情况它都有效，比如只是在起动期间才发生危险以及人员经常出现在危险区的情况。还应考虑到由于在事件的发生过程中要

对征兆进行调查，所以在危险事件附近出现的人数还可能增加。

当对 SIS 的潜在要求源进行评估时，评估应包括以下情况：起动、连续操作、停机、维修错误、手动干预（如手动控制器）、供应的中断（如空气、冷却水、氮、动力、蒸汽、加热保温层等）。

当考虑要求频率时，在某些复杂情况下，可能有必要进行一次故障树分析。仅在因多个事件的同时失效而产生严重后果的情况下（例如，未为所有泄压的最坏情况设计减压收集器），这经常是必要的。应对什么时候应把操作员错误包含在可能引起的危险事件，以及这种事件发生的频率的事件清单中做出判断。如果操作员动作需经允许规程或者开锁设施（为防止偶然动作而配备的）才能执行，那么通常就可排除操作员错误。还需注意的情况是在什么场合，由于操作员动作降低要求频率是可信任的。这种信任会受到人为因素（比如需要多快地采取动作）和涉及任务的复杂程度的限制。在操作员对报警采取动作以及所声明的风险降低因子大于 10 的情况下，则需要根据GB/T 21109.1设计整个系统。承担安全功能的系统包括检测危险工况的传感器、报警显示、人工响应以及操作员用来消除任何危险的设备。声明的风险降低因子不大于 10 的情况无需遵从 GB/T 21109，这时应仔细考虑人为因素问题。由于报警而降低风险的任何声明必须得到三个方面的支持：对该报警必要响应的文档化描述，足以供操作员采取正确动作的时间，保证操作员采取预防动作的培训。

倘若下列条件成立，降低对 SIS 的要求率就能把一个报警系统用作一种风险降低的方法：

——当失控将导致对 SIF 的一次要求时，用于报警系统的传感器不用作控制目的；

——用于报警系统的传感器不用作 SIS 的组成部分；

——已经考虑到关于风险降低的限制，这种风险降低可被声明用于 BPCS 和共同原因问题。

GB/T 21109.3给出了可用来确定安全仪表系统的 SIL 的技术示例，还包含在选择用于某个特定应用的方法时需考虑哪些问题的指南。

当确定是否需要风险降低时，需要具有一些过程安全和环境目标。它们专用于特定的现场或操作公司，并且可同未使用附加安全功能的风险水平进行比较。在确定需要风险降低之后，有必要考虑需要执行什么样的功能以使过程返回到某个安全状态。理论上，可以用通用术语描述这些功能而无需涉及某个特殊技术。例如在过压保护的情况中，可把功能描述成防止压力上升超过某个规定值。无论是一个安全阀或是一个安全仪表系统都能执行此功能。当如上描述功能时，则可在生命周期的下一阶段（给保护层分配仪表安全功能）来决定所使用的技术类型的选择。实际上，根据所选的系统类型，功能要求是不相同的；在某些情况下，此阶段和下一阶段可结合起来。

总之，危险和风险分析应考虑：

——每个已确定的危险事件和导致该危险事件的事件序列；

——与每个危险事件相关联的事件序列的后果和可能性，可定量或定性表示它们；

——每个危险事件的必要的风险降低；

——为降低或消除危险和风险而采取的措施；

——在分析风险过程中所作的假定，包括估计的要求率和设备的失效率，应详细说明操作约束或人为干预取得的任何信任；

——在每个 SIS 生命周期阶段（如验证和确认活动）对与安全相关系统有关的关键信息的引用。

构成危险和风险分析组成成分的信息和结果都应文档化。

当已经做出了决定并且可用的信息变得更精确时，可能有必要在整个 SIS 安全生命周期的各个阶段反复进行危险和风险评估。

8.2.2 在过程工业中，在许多应用中需考虑要求的一个重要理由是 BPCS 失效。传感器、阀或控制系统都可能引起 BPCS 失效。

在过程工业中使用的控制系统有时具有冗余处理器，传感器和阀一般没有冗余。当给 BPCS 分配一个失效率时，需要知道失效率有一个重要限制。GB/T 21109.1对与某个特殊危险有关的危险失效率作了限制，即除非系统的实现符合该标准的要求，能声明的危险失效率只能到每小时 10^{-5}。这种限制

的理由是如果声明的危险失效率较低，它应是在GB/T 21109.1—2007表4的失效率范围之内。此限制保证了不满足GB/T 21109.1要求的系统不会有高的置信度水平。

8.2.3 见GB/T 21109.1。

9 给保护层分配安全功能

9.1 目的

为了确定所需的SIS和相关的SIL，考虑现有一些(或需要有些)什么样的其他保护层以及它们所提供的保护功能有多大是很重要的。在考虑了其他保护层之后，应对SIS保护层的需要作出判定。如果需要一个SIS保护层，则应确定该SIS的仪表安全功能的SIL。

9.2 分配过程的要求

9.2.1 本条的要求是商定将使用的安全层和分配仪表安全功能的性能目标。实际上，在许多情况下，只有在使用固有的安全设计或其他技术系统存在问题的场合，才将安全功能分配给安全仪表系统。

这类问题的例子包括对燃烧容量的限制或者针对放热反应的保护。使用基于仪表的系统而不是像安全阀这类更传统方案的任何决定，都需要有坚实的理由来支持，而这种理由要经受得住制定规章制度的权威机构的质询。

如上所述，危险和风险评估与分配可能同时进行；在某些情况下，分配可以在危险和风险评估前进行。决定给安全层分配安全功能通常应根据用户组织发现是切实可行的依据做出。还应考虑已确定的良好的行业惯例。然后在假定其他安全层是可信任的情况下，对安全仪表系统做出判定。例如，在已安装安全阀，并且它们是根据工业法规设计和安装的情况下，判定它们本身是否达到足够的风险降低。在安全阀的大小和性能还不完全满足应用，或者禁止将气体释放到大气中的情况下，安全仪表系统仅用于限制压力。

9.2.2 见GB/T 21109.1。

9.2.3 在把一个安全功能分配给一个仪表安全功能时，需考虑应用是以要求模式还是以连续模式操作。过程领域中的大多数应用在要求不是很频繁的情况下都使用要求操作模式。在这类情况中，GB/T 21109.1—2007的表3是常用的合适量值。有些应用要求很频繁(例如要求率每年大于1)，这类应用更适合当作连续模式，因为危险失效概率主要是由SIS的失效率决定的。在这些情况下，宜使用GB/T 21109.1—2007表4中的适当量值。失效导致即时危险，在连续模式中是很少见的。如果对于控制系统的所有失效模式而言，保护系统不能满足要求，燃烧器或汽轮机速度控制就可采用连续模式应用。

GB/T 21109.1—2007的表3中SIL是通过PFD_{avg}来定义的。而目标PFD_{avg}是通过要求的风险降低来确定的。要求的风险降低能通过对没有SIS时的过程风险同允许风险进行比较来确定的。它能够通过GB/T 21109.3中的技术按照定量或定性的原则来确定。

GB/T 21109.1—2007的表4用执行SIF的危险失效目标频率来定义SIL。可通过SIS的允许失效率并考虑特定应用中失效的后果来确定SIL。当使用GB/T 21109.1—2007的表4来确定要求的SIL时，目标会基于安全仪表系统的危险失效频率。在使用GB/T 21109.1—2007的表4时，使用检验测试间隔或要求率把危险失效频率转换成要求时的危险失效概率是不正确的。尽管单位看起来是一样的，但这会导致GB/T 21109.1—2007的表4的不恰当转换，并可能导致安全功能的SIL要求的不规范。

要求时的平均失效概率目标或者每小时的危险失效频率目标适用于仪表安全功能，并不适用于单个部件或子系统。一个部件或子系统(如传感器、逻辑解算器和最终元件)除了它被用于某个特定SIF之外，不能给它指派一个SIL。但它具有独立的最大SIL能力的申明。

危险和风险评估和分配过程的输出，应该是安全系统所执行功能的一个清晰的描述，包括潜在的安全仪表系统及其所有仪表安全功能的安全完整性等级要求(连同操作模式——连续或要求)。它构成了SIS安全要求规范的基础。应清楚地描述确保能维持安全所需要执行的功能。

在此实现阶段，不必规定传感器和阀门的架构的细节。决定采用什么样的架构比较复杂，特定系统是否要求 2oo3 传感器和 1oo2 阀取决于许多因素。

9.2.4 需要完全了解GB/T 21109.1—2007中表 3 和表 4 的含意。特别是，单个仪表安全功能可以声明的 PFD_{avg} 限制到 10^{-5}，这相当于 10^5 的风险降低(SIL 4)。可靠性分析指出由于硬件随机失效的 PFD_{avg} 小于 10^{-5} 是可以达到的，但GB/T 21109.1认为系统失效和共同模式失效会限制实际可能达到的性能。强烈推荐在风险分析显示出需要高的风险降低的情况下，应注意到过程领域中要达到 SIL 4 的仪表安全功能是困难的。解决办法是使用几个较低完整性的独立 SIS。

根据GB/T 21109.1—2007的 9.2.4 的注 4：

为了达到较高的风险降低水平(如大于 10^3)，可以使用多个 SIS。当使用多个 SIS 来达到较高的风险降低时，重要的是每个 SIS 应能独立地执行安全功能，并且各 SIS 之间应有足够的独立性。例如，把一个 SIL 2 的压力检测回路同一个 SIL 1 的液位检测回路组合起来，以达到具有 10^3 风险降低要求的过压安全功能也许并不可取；因为液位传感器检测到一个高液位之前，压力容器就可能已经超过了它的压力限值。

另外，在使用多个 SIS 时，还应考虑共同原因失效。此外，还要满足GB/T 21109.1中定义的所有其他要求，包括表 5 中定义的最低故障裕度要求。

为了说明怎样组合所使用的多个 SIS 来达到较高的风险降低水平，考虑下例：

一个由 2oo3 变送器组、一个 2oo3 逻辑解算器和一个 1oo2 最终元件组构成的一个具有 PFD_{avg} 为 3.05×10^{-4} 的 SIS。该 SIS 达到的风险降低大约为 3.3×10^3。

假定使用两个这样的系统来产生一个 10×10^6($3.3\times10^3\times3.3\times10^3$)的风险降低是不正确的。共同原因因素(如使用相同的技术、根据同样的功能规范设计两个系统)、人为因素(如编程、安装、维护)和外部因素(如腐蚀、堵塞、空气管道的冻结、闪电)都将限制系统提高。还有必要考虑两个系统间任何共享的部件。

一种较可行的解决办法是使用尽可能多样性的部件(为了最小化潜在的共同原因问题)的一个非冗余第二系统。

例如，考虑包含仅一个开关、继电器逻辑和仅一个最终元件的系统，该系统具有一个 7.7×10^{-3} 的 PFD_{avg}。此系统达到的风险降低大约为 1.3×10^2。

把基于软件的 SIS 和单纯继电器型 SIS 组合起来，可得到的总体理论风险降低为 4.3×10^5($3.3\times10^3\times1.3\times10^2$)。如上所述，尽管在理论上性能的组合似乎是可能的(因为无论哪个 SIS 都能使过程单元停机)，但同样不得不考虑共同原因因素，并且由于这些因素使之可达到的风险降低要稍微低一点。

9.3 安全完整性等级 4 的附加要求

9.3.1 见GB/T 21109.1。

9.3.2 见GB/T 21109.1。

9.4 作为一个保护层的基本过程控制系统的要求

9.4.1 基本过程控制系统也可视为是一个遵从某些条件的保护层。如果在 BPCS 中，以降低过程风险为目的的功能得到实现，针对预定要降低的确定的风险，也可给 BPCS 分配一个风险降低。

9.4.2 不需遵从GB/T 21109.1，仪表型系统就可声明低于 10 的风险降低。这使得 BPCS 可用于某些风险降低，而无需按GB/T 21109.1的要求实现该系统。应通过考虑 BPCS 的完整性(由可靠性分析或者性能数据确定)和用于配置、修改、操作和维护的规程表证明所作的任何声明都是合理的。当在 BPCS 中给功能分配风险降低时，保证提供访问保密和更改管理是重要的。能声明的一个 BPCS 功能的风险降低也可由 BPCS 功能和诱发原因之间的独立程度来确定。图 2 说明了 BPCS 功能和诱发原因之间的独立性。