ICS 25.040
N 10

中华人民共和国国家标准

GB/T 21109.3—2007/IEC 61511-3:2003

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

Functional safety—Safety instrumented systems for the process industry sector—Part 3:Guidance for the determination of the required safety integrity levels

(IEC 61511-3:2003,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3部分，等同采用IEC 61511-3:2003《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》(英文版)。为便于使用，对IEC 61511-3:2003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、附录F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)技术安全仪表系统。在逻辑解算器使用其他技术的情况下,宜使用 GB/T 21109 的基本原则。GB/T 21109 还论述了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工业(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案。为了使用一个合理和一致的技术策略,此方案已被采纳。

在大多数情况下,固有(inherently)安全过程设计就能很好地达到安全性。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)。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。为促成该方案,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。

本部分涉及到了危险和风险分析(H&RA)中确定要求的 SIL 范围的指南。这当中的信息用来提供一个用于实现 H&RA 的各种各样的全局方法的广泛概览。但提供的信息并未详细到足以实现这些方案中的任何一种。

在继续之前,应回顾一下 GB/T 21109.1 中提供的安全完整性等级(SIL)的概念和确定方法。本部分的附录描述了以下内容:

附录 A　提供允许风险和 ALARP 的概念的概述。

附录 B　提供一种用来确定要求的 SIL 的半定量方法的概述。

附录 C　提供一种用来确定要求的 SIL 的安全矩阵方法的概述。

附录 D　提供一种使用半定性风险图方法来确定要求的 SIL 的方法的概述。

附录 E　提供一种使用定性风险图方法来确定要求的 SIL 的方法的概述。

附录F　提供一种使用保护层分析(LOPA)方法来选择要求的SIL的方法的概述。

GB/T 21109的整体框架见图1。

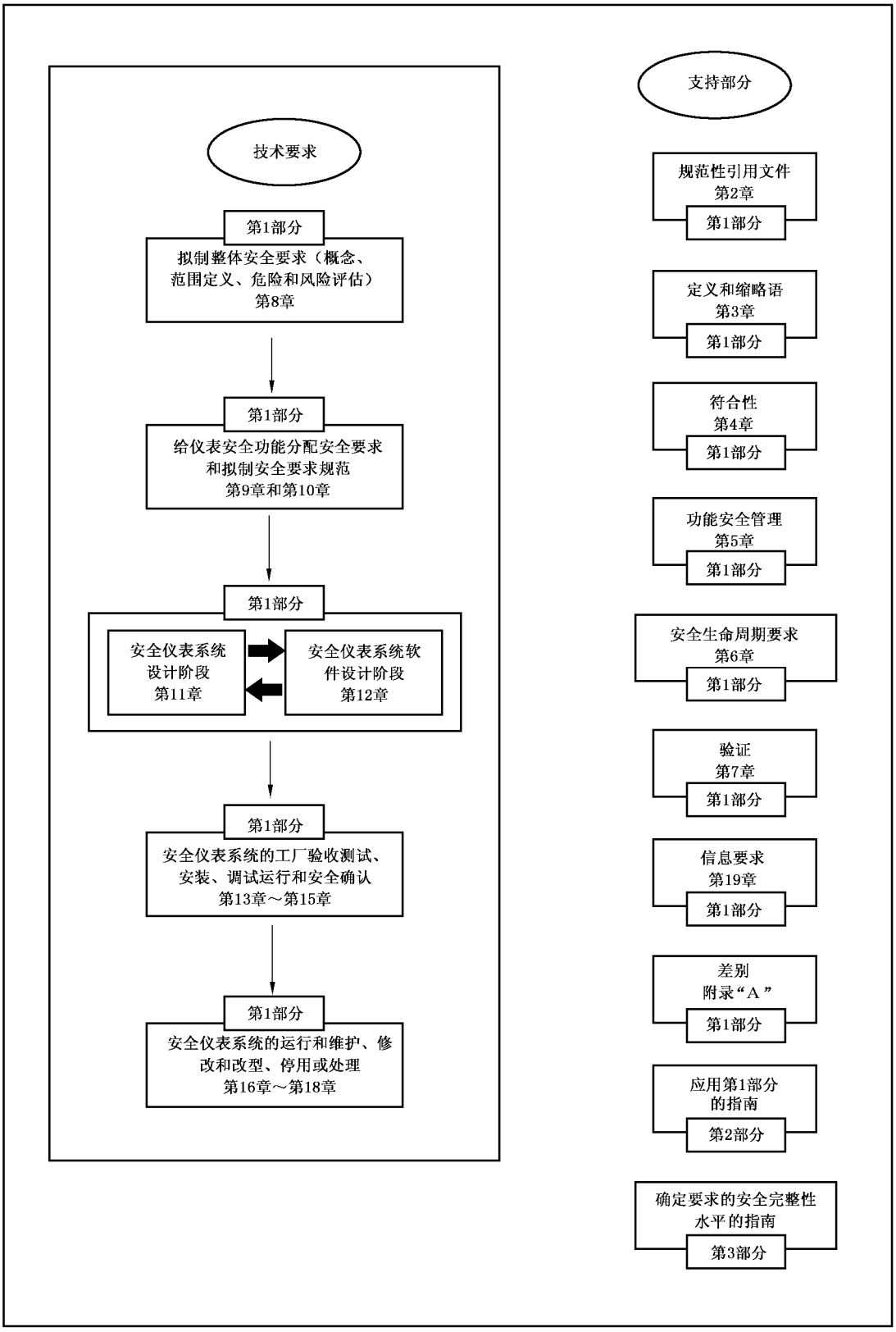

图1　GB/T 21109的整体框架

过程工业领域安全仪表系统的功能安全 第3部分:确定要求的安全完整性等级的指南

1 范围

本部分提供了与以下有关的信息:

——风险的基础概念、风险与安全完整性的关系,见第3章;

——允许风险的确定,见附录A;

——确定仪表安全功能的安全完整性等级的各种不同方法,见附录B、附录C、附录D、附录E和附录F。

特别是:

a) 为了保护人员、公共设施或环境,使用一个或多个仪表安全功能来达到功能安全时可使用本部分;

b) 在比如资产保护这类非安全应用中也可使用本部分;

c) 本部分说明了定义安全功能要求和每个仪表安全功能的安全完整性等级需要执行的典型危险和风险评估的方法;

d) 本部分说明了可用来确定要求的安全完整性等级的技术/措施;

e) 本部分为确立安全完整性等级提供了一个框架,但并不规定特殊应用要求的安全完整性等级;

f) 本部分不给出确定其他风险降低方法的要求的例子。

附录B、附录C、附录D、附录E和附录F说明了各种定量和定性方法,并且为了说明基础原理已对这些方法作了简化。本部分包含了这些附录以便说明这些方法的一般原理但并不提供一个权威的计算。

注:如打算使用这些附录中指出的那些方法,应查阅每个附录中引用的原始资料。

图1表示GB/T 21109的整体框架,并指出本部分在实现安全仪表系统的功能安全中所起的作用。

图2给出了风险降低方法的总览。