ICS 25.040
N 10

中华人民共和国国家标准

GB/T 18272.7—2006/IEC 61069-7:1999

工业过程测量和控制 系统评估中系统特性的评定 第7部分:系统安全性评估

Industrial-process measurement and control—Evaluation of system properties for the purpose of system assessment—Part 7:Assessment of system safety

(IEC 61069-7:1999,IDT)

2006-05-08 发布　　2006-11-01 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 18272《工业过程测量和控制　系统评估中系统特性的评定》由以下部分组成：

——第1部分：总则和方法学；

——第2部分：评估方法学；

——第3部分：系统功能性评估；

——第4部分：系统性能评估；

——第5部分：系统可信性评估；

——第6部分：系统可操作性评估；

——第7部分：系统安全性评估；

——第8部分：与任务无关的系统特性评估。

本部分是其中的第7部分。

本部分与GB/T 18272其余各部分的关系以及本部分在各部分中的相对位置见图1。

本部分等同采用IEC 61069-7:1999《工业过程测量和控制　系统评估中系统特性的评定　第7部分：系统安全性评估》(英文版)。

本部分等同翻译IEC 61069-7:1999。

本部分在制定时按GB/T 1.1—2000《标准化工作导则　第1部分：标准的结构和编写规则》和GB/T 20000.2—2001《标准化工作指南　第2部分：采用国际标准的规则》的有关规定做了如下编辑性修改：

——删除IEC国际标准前言；

——原引用标准的引导语按GB/T 1.1—2000的规定改成规范性引用文件的引导语；

——“本标准”一词改为“GB/T 18272的本部分”。

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第一分技术委员会归口。

本部分由上海工业自动化仪表研究所、浙江中控技术股份有限公司负责起草。

本部分参加起草单位：上海自动化仪表股份有限公司、清华大学自动化系、兵器工业系统总体部。

本部分主要起草人：徐晓燕、李明华。

本部分参加起草人：徐义亨、刘铁椎、杨佃福、李光沐、张庆军、刘华美。

引　言

GB/T 18272 的本部分论述了评估工业过程测量和控制系统的安全性特性所采用的方法。本部分所涉及的安全仅限于工业过程测量和控制系统本身出现的危险源。如果系统的使命包含有可能影响被控过程或装置安全性的活动，则有关这些活动的要求应符合 IEC 61508 的规定。

所谓系统评估，就是根据各种迹象判断该系统是否适用于某一特定使命或者某一类使命。

要想获取所有迹象，就需要全面地(即在各种影响条件下)评定与系统的特定使命或一类使命相关的所有各种系统特性。

但是这种做法不切实际，因此系统评估所依据的基本原理是：

——确定每一种相关系统特性的临界状态；

——通过对评定各种特性的成本效益的研究，制定出评定系统相关特性的计划。

在实施系统评估时，关键是要考虑必需以有限的经费和时间最大限度地提高系统适用性的置信度。

只有在明确(或规定)了系统的使命或者能够假设系统使命的情况下，评估才能得以进行。没有使命就无法进行评估。但仍可以为其他部门开展的评估工作确定并实施各种评定(如 GB/T 18272.1 所规定的评估活动)。

在这种情况下，由于评定是评估的组成部分，因此可以把本部分作为制定评定计划的指南，提供评定的实施程序。

GB/T 18272 的基本框架如图 1 所示。

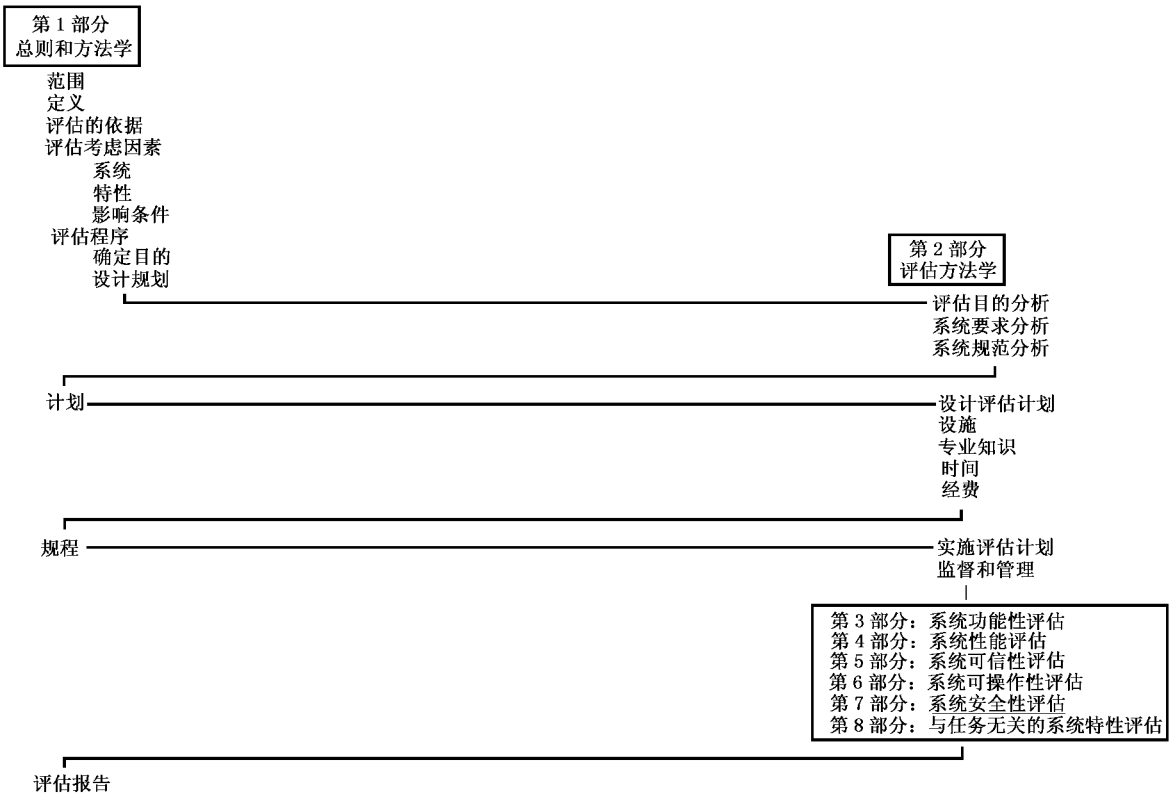

图 1　GB/T 18272 的基本框架

工业过程测量和控制
系统评估中系统特性的评定
第7部分:系统安全性评估

1 范围

GB/T 18272的本部分详细阐述了系统地评估工业过程测量和控制系统的安全性特性的方法。

本部分所涉及的安全仅限于工业过程测量和控制系统本身出现的危险源。本部分不考虑由被评估的工业过程测量和控制系统所控制的过程或装置可能引入的危险源。如果系统的使命包含有可能影响被控过程或装置安全性的活动,则有关这些活动的要求应符合IEC 61508的规定。

2 规范性引用文件

下列文件中的条款通过GB/T 18272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 4793.1—1995 测量、控制和试验室用电气设备的安全要求 第1部分:通用要求(idt IEC 61010-1:1990)

GB/T 16935.1—1997 低压系统内设备的绝缘配合 第一部分:原理、要求和试验(idt IEC 60664-1:1992)

GB/T 18272.1—2000 工业过程测量和控制 系统评估中系统特性的评定 第1部分:总则和方法学(idt IEC 61069-1:1991)

GB/T 18272.2—2000 工业过程测量和控制 系统评估中系统特性的评定 第2部分:评估方法学(idt IEC 61069-2:1993)

GB/T 18272.5—2000 工业过程测量和控制 系统评估中系统特性的评定 第5部分:系统可信性评估(idt IEC 61069-5:1994)

GB/T 20000.4—2003 标准化工作指南 第4部分:标准中涉及安全的内容(ISO/IEC 51:1999,MOD)

IEC 61508-1:1998 电气/电子可编程序电子安全相关系统的功能安全 第1部分:一般要求

3 术语和定义

下列术语和定义适用于GB/T 18272的本部分。

3.1

系统安全性 system safety

系统作为一个物理实体,其本身不会造成危险源的程度。

注:系统的安全性不包括被控过程或装置的安全性。如果系统用于执行安全功能(见IEC 61508-1:1998),则被控过程或装置的安全性依赖于系统的可信性。

3.2

危险源 hazard

潜在的伤害源。