ICS 25.040
N 10

中华人民共和国国家标准

GB/T 18272.5—2000
idt IEC 61069-5:1994

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

Industrial-process measurement and control—Evaluation of system properties for the purpose of system assessment—Part 5:Assessment of system dependability

2000-12-11 发布　　2001-08-01 实施

国家质量技术监督局 发布

目　　次

前　言

本标准是根据国际电工委员会标准 IEC 61069-5:1994《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》制定的,在技术内容和编写规则上与之等同。

GB/T 18272 在《工业过程测量和控制　系统评估中系统特性的评定》的总标题下,包括以下 8 个部分:

第 1 部分:总则和方法学　(GB/T 18272.1　idt IEC 61069-1:1991)

第 2 部分:评估方法学　(GB/T 18272.2　idt IEC 61069-2:1993)

第 3 部分:系统功能性评估　(GB/T 18272.3　idt IEC 61069-3:1996)

第 4 部分:系统性能评估　(待制定)

第 5 部分:系统可信性评估　(GB/T 18272.5　idt IEC 61069-5:1994)

第 6 部分:系统可操作性评估　(待制定)

第 7 部分:系统安全性评估　(待制定)

第 8 部分:与任务无关的系统特性评估　(待制定)

本标准是其中的第 5 部分。

本标准的附录 A、附录 B、附录 C 和附录 D 是提示的附录。

本标准由国家机械工业局提出。

本标准由全国工业过程测量和控制标准化技术委员会归口。

本标准负责起草单位:上海工业自动化仪表研究所。

本标准参加起草单位:重庆工业自动化仪表研究所、上海自动化仪表股份有限公司、重庆川仪股份有限公司、西仪集团有限责任公司、中国航空工业总公司第 634 研究所、北京和利时系统工程股份有限公司、国家工业控制机及系统工程技术研究中心。

本标准主要起草人:吴庆祈、徐晓燕、李明华。

本标准参加起草人:张春明、刘铁椎、刘慕尹、于美梅、李光沐、苏伟辉、刘鑫。

本标准委托上海工业自动化仪表研究所负责解释。

IEC 前言

1) IEC(国际电工委员会)是一个由各个国家电工委员会(IEC 国家委员会)组成的世界性标准化组织。IEC 的目标是促进电工电子领域标准化问题的国际合作。IEC 为此目的而出版国际标准,并举办其他各种活动。国际标准的制定工作是委托技术委员会进行的,对所制定标准感兴趣的任何一个 IEC 国家委员会都可以参与国际标准的制定工作。与 IEC 有联系的国际组织、政府机构和非官方组织也可以参与标准制定工作。IEC 与国际标准化组织(ISO)按照双方达成的协议紧密合作。

2) IEC 有关技术问题的正式决议或协议,是由各技术委员会代表了对这些问题特别关切的所有国家委员会提出的。这些决议和协议尽可能地表达了对所涉及的问题在国际上的一致意见。

3) 这些决议或协议以标准、技术报告或导则的形式出版,并以推荐标准的形式供国际上使用,并在此意义上为各国家委员会所承认。

4) 为了促进国际上的统一,IEC 各国家委员会承诺在其国家标准或地区标准中最大限度地采用 IEC 国际标准。IEC 标准与相应的国家或地区标准之间,如有不一致之处,应在国家标准或地区标准中明确指出。

国际标准 IEC 61069-5 由 IEC 第 65 技术委员会:"工业过程测量和控制"的 65A 分委员会:"系统方面"制定。

IEC 61069-5 的文本以下列文件为依据:

国际标准草案	表决报告
65A(CO)37	65A/166/RVD

有关表决批准本标准的详细情况可参见上表指明的表决报告。

整个标准由一系列出版物组成,这是其中的第 5 部分。

第 1 部分为总的导则,因而作为一个"独立"的出版物。

第 2 部分详细论述了评估方法学。

第 3 部分至第 8 部分为各类特性的评估指南。

第 3 部分至第 8 部分对特性作了划分,将各种相关特性归入同一类别。

整个标准由以下各部分组成:

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

附录 A、附录 B、附录 C 和附录 D 仅供参考。

IEC 引言

IEC 61069 的这一部分论述了在评估工业过程测量和控制系统的可信性时所采用的评估方法。

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 IEC 61069-1 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，因此可以把本标准作为制定评定计划的指南，提供评定的实施程序。

IEC 61069 的基本轮廓如图 1 所示。

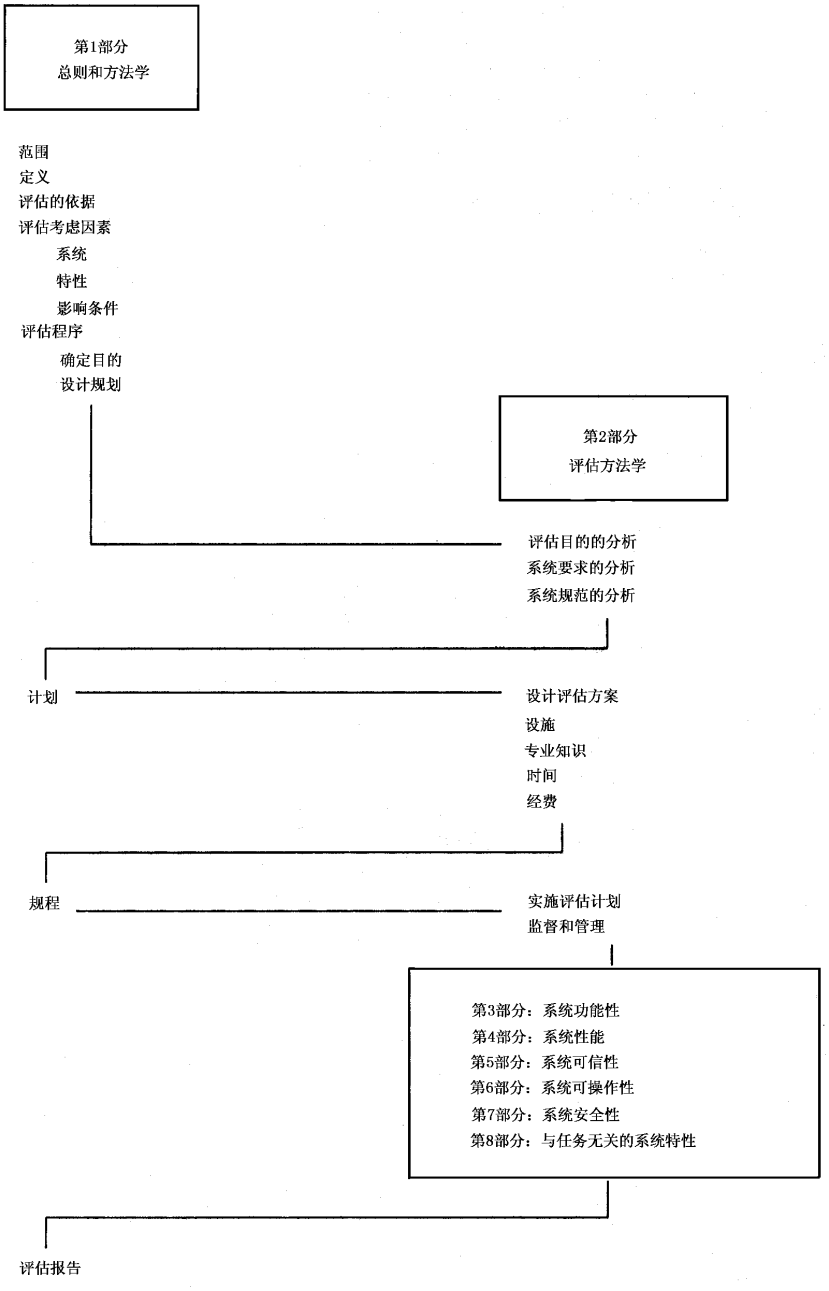


图 1　IEC 61069 的基本轮廓

中华人民共和国国家标准

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

GB/T 18272.5—2000
idt IEC 61069-5:1994

Industrial-process measurement and control—Evaluation of system properties for the purpose of system assessment—Part 5: Assessment of system dependability

1 范围

本标准详细论述了系统地评估工业过程测量和控制系统的可信性所采用的方法。

GB/T 18272.2 所述的评估方法学适用于制定可信性评估大纲。

本标准分析了可信性的子特性，同时对评估可信性时需要考虑的评判依据做了说明。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 2423(所有部分) 电工电子产品基本环境试验(IEC 60068：环境试验)

GB/T 2424(所有部分) 电工电子产品基本环境试验规程(IEC 60068：环境试验)

GB/T 7289—1987 可靠性、维修性与有效性预计报告编写指南(eqv IEC 60863：1986)

GB/T 7826—1987 系统可靠性分析技术 失效模式和效应分析(FMEA)程序 (idt IEC 60812：1985)

GB/T 14733.3—1993 电信术语 可靠性、可维修性和业务质量 (eqv IEC 60050，IEV 191：1990)

GB/T 15647—1995 稳态可用性验证试验方法(idt IEC 61070：1991)

GB/T 17626(所有部分) 电磁兼容试验和测量技术(idt IEC 61000)

GB/T 18272.1—2000 工业过程测量和控制 系统评估用系统特性的评定 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 系统评估用系统特性的评定 第2部分：评估方法学(idt IEC 61069-2：1993)

3 定义

下列定义适用于本标准。

标有“*”的定义与 GB/T 14733.3 的相同。为使各定义在 GB/T 18272 各部分中的理解完全一致，本章末的注对这些定义做了说明。

3.1 **可信性** dependability

假定具备必要的外部资源，系统能在规定的条件下，在规定的一瞬间或一段时间内正确地专门完成

国家质量技术监督局 2000-12-11 批准 2001-08-01 实施

一项任务的可信赖程度。

3.2 **可靠性*** reliability

在给定条件下和规定的时间间隔内，产品(装备)执行所需功能的能力。

3.3 **维修性** maintainability

一个实体在规定的条件下采用规定的程序和资源进行维修以后，可在规定的使用条件下保持或恢复到能完成规定功能的状态的能力。

3.4 **可用性*** availability

在要求的外部资源得到保证的前提下，产品(装备)在规定的条件下，在给定的瞬时或在给定的时间间隔内，处于执行所需功能状态的能力。

3.5 **忠实性** integrity

系统对于将正确完成任务，否则将对任务可能导致不能正确完成任务的系统状态做出提示的保证。

3.6 **防护性** security

系统对于拒绝接受任何错误的输入或者未经许可的存取的保证。

3.7 **信任性** credibility

系统能够识别系统状态并发出相应信号，抵制错误的输入或者未经许可的存取的程度。

注：本标准所说的“实体”指的是工业过程测量和控制系统；“要求的功能”指的是任务。在评定时，“任务”应理解为“系统任务”。GB/T 18272.1—2000 的 2.2.4 和 2.2.5 分别对任务和功能做了定义。

4 可信性特性

4.1 概述

作为一个可信赖的系统，它必须随时可以执行其功能。这属于可用性方面的问题，它取决于系统的故障发生频率(可靠性)和系统恢复正常所需的时间(维修性)。

但事实上，当系统准备执行其功能时，并不表示系统功能一定会被正确执行。

这就涉及到信任性方面的问题，它取决于：

——在系统处于不能正确执行某些或全部功能的状态时，系统发出警告的能力(忠实性)；

——系统拒绝任何不正确输入或未经许可进入系统的能力(防护性)。

要评估一个系统的可信性，就必须确定和评估对系统的可信性起决定作用的一些子特性。

可信性及子特性的关系如图 2 所示。

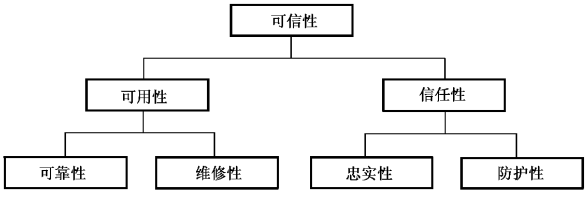


图 2 可信性的层次

4.2 可信性

可信性无法直接评估，必须分别对其每一种子特性进行评估。

每一种子特性都取决于系统模块的结构配置以及这些模块的可信性特性。

这些模块的子可信性特性与系统的可信性特性之间的关系可能是相当复杂的。

系统级的每一种子特性可能取决于模块级的若干种子特性。

例如：

——如果系统结构包括冗余，则系统的可用性取决于冗余模块的忠实性特性；

——如果系统结构包括系统防护性机理，则系统的防护性取决于履行防护性机理的模块的可用性

特性；

——如果结构中包含了用于核对由系统内部其他部件传送来的数据的模块，则系统的忠实性取决于这些模块的防护性特性。

可信性不可能简单地用数字加以描述，其某些特性可以用概率表示，其余特性是确定的，有些方面可以量化，而另一些方面只能以定性的方式加以描述。

当一个系统执行若干个系统任务时，其可信性可能会因系统任务的不同而发生变化。这就需要分别对每一项任务进行分析。

4.3 可用性

系统的可用性取决于系统各个部件的可用性以及这些部件在执行系统任务时的协作方式。部件的协作方式可包括功能冗余(同类或不同类)、功能退化和功能下降。事实上，可用性取决于所采用的程序和可用于维持系统工作的资源。系统的可用性对于系统的每一项任务来说可能是各不相同的。各项任务的系统可用性可以按两种方式加以量化：

4.3.1 预计系统的可用性时，可按下式计算：

$$\text{可用性}=\frac{\text{平均失效前时间}}{(\text{平均失效前时间}+\text{平均恢复时间})}$$

式中：

——“可用性”是规定任务的系统可用性；

——“平均失效前时间”是从系统恢复到执行规定任务的状态起，至因故障而中止执行任务止的平均时间；

——“平均恢复时间”是从系统因故障而中止执行任务起，至恢复执行规定任务止所需总时间的平均值。

4.3.2 对于正在工作中的系统，可以用下列公式计算可用性：

$$\text{可用性}=\frac{\text{系统已经能执行任务的总时间}}{\text{预计系统执行任务的总时间}}$$

4.4 可靠性

系统的可靠性取决于系统各个部件的可靠性以及这些部件在执行系统任务时的协作方式。部件的协作方式可包括功能冗余(同类或不同类)、功能退化和功能下降。

系统的可靠性相对于每一项任务来说可能是各不相同的。各项任务的可靠性均可量化，但其预计置信度水平则各不相同。

系统各个硬件的可靠性可以采用部件计数法进行预计。然后利用综合法就可以预计系统的可靠性。应该说明的是，目前还没有可用于系统软件模块的具有较高置信度水平的可靠性预计方法。

4.5 维修性

系统的维修性取决于系统各个部件的维修性以及系统的物理结构和功能结构。物理结构影响到存取的难易程度和更换性等。功能结构影响到诊断等的难易程度。

在定量表示一个系统的维修性时，应该把使系统恢复到完全能执行其任务的状态所需采取的各种措施计算在内，包括检测故障、通知维修、论断和排除故障起因、调整和检验等所需的时间。

还应通过核对下列项目的保障措施和覆盖系数，给维修性的定量表示增加定性说明：

——发生故障时的通报方式：灯光、报警信息、报告等；

——访问：便于人员存取和连接测量仪表，模块化程度等；

——诊断：故障直接识别，本身对系统没有影响的诊断工具，远程维修支持装置，统计误差检查和报告；

——修复性/更换性：模块化程度，模块和元件的明确识别，几乎不需要专用工具，更换元件或模块时对其他元件或模块的影响极小；

——检验：维护指导程序，极少量检验要求。

4.6 信任性

系统的信任性取决于由系统元件作为功能实现的忠实性和防护性机理。

忠实性机理是通过一个元件检查其他元件的输出实现的。

防护性机理是通过一个元件检查其他元件的输入实现的。

信任性机理包括：

a) 检验：

——功能的正确执行(例如利用监视器、已知数据进行检验)；

——正确的数据(例如有效性检验、奇偶检验等)；

b) 操作，例如：

——自纠正；

——限制；

——通报操作等。

这些机理可以用来提供忠实性和(或)防护性。

分析信任性机理时，可以采用 8.3.2.2 所述的故障注入技术。

信任性是定性的，某些方面可以定量表示。

4.7 防护性

系统的防护性取决于系统边界上实现的检测和防止不正确的输入或未经许可存取的机理。

防护性是定性的，某些方面可以定量表示。

4.8 忠实性

系统的忠实性取决于在系统的输出元件上实现的检验输出是否正确的机理，同时也取决于系统内部实现的检测和防止系统部件之间错误地传输信号和数据的机理。对于每一个其本身就可被看作是一个系统的相关部件而言，这两种内部机理就是忠实性机理或防护性机理。

忠实性是定性的，某些方面可以定量表示。

5 复查系统要求文件(SRD)

应通过审核系统要求文件，检查文件中是否说明并按 GB/T 18272.2 所述的方式列出了将由系统执行的每一项任务和可信性要求。

如果使命与过程安全有关，并且要求系统执行与安全有关的任务，应检查系统要求的一致性。

可信性评估的有效性完全取决于对有关要求的说明是否全面，以及对故障的认定结果。

为此，应审核系统要求文件，检查文件是否对每一项系统任务明确地说明：

——任务的相对重要性；

——认定任务故障的定义；

——以可信性特性表示的故障的判断依据；

——工作和运行环境。

可信性特性受到人为因素影响时，应对有关情况做适当的说明，如果可能还应定量表示，以便正确评估人为因素的影响。

应按照与每一项独立的任务以及与系统的总使命有关的可信性要求，确定是否已具备必要的信息。

附录 A(提示的附录)列出了为使可信性特性的评定能够进行而应该由系统要求文件提供的各类信息和文件编制格式。

6 复查系统规范文件(SSD)

应通过审核系统规范文件，检查是否按 GB/T 18272.2 所述的方法列出每一项要求完成任务的可信性特性。

尤其应注意查对有关下列内容的信息：

——支持每一项任务的系统功能以及支持这些功能的模块和元件，包括硬件和软件；

——由系统支持的执行各项任务的变通方法及其启动方式；

——系统所具备的信任性机理(安全性和忠实性)以及支持信任性机理的方式；

——支持每一项任务的功能、模块和元件的可靠性和可用性；

——维修性特性；

——工作和环境特性以及对使用模块和元件的限制。

附录 B(提示的附录)列出了为使可信性特性的评定能够进行而应该由系统规范文件提供的各类信息和文件编制格式的导则。

7 评估程序

7.1 概述

评估应按 GB/T 18272.2—2000 第 7 章规定的程序进行。

应明确陈述评估目的，其原则见 GB/T 18272.1—2000 的 4.1。

系统要求文件和系统规范文件提供的信息应该完整、精确，以保证可信性评估的正常进行。如果在评估的某个阶段发现信息有遗漏或不完整，应就有关问题咨询系统要求文件和系统规范文件的起草者，获取所需的详细信息。

GB/T 7289 列出了评估需要考虑的项目一览表。

7.2 分析系统要求文件和系统规范文件

7.2.1 整理文献资料信息

对可信性进行评估，应按 GB/T 18272.2—2000 的 7.2 所述的方法从系统要求文件和系统规范文件中摘录有关信息。

应以定量/定性的方式从系统要求文件中摘录每一项任务所需的可信性特性，注明需要这些可信性时所处的影响条件。

应说明每一项任务的输入、输出和操作。

对于每一个输入，应注明：

——允许状态和相应的允许输出状态；

——非允许状态和要求采取的相应操作措施。

对于每一个输出，应注明：

——允许状态；

——非允许状态和要求采取的相应操作措施。

对于每一项任务的故障，应阐明下列内容：

——造成故障的原因；

——允许发生频率；

——采取的措施；

——至恢复执行任务的允许最长时间；

——如有可能，还要说明 GB/T 18272.1 所述的影响条件。

应将有关系统可信性要求和可信性数据的全部信息汇总，相互对照，编成下列正确简明的说明：

——系统的功能界限；

——系统不符合要求的项目；

——提供执行指定任务的功能以及连接各种功能以支持指定任务的备选数据通道；

——各种功能在系统模块和元件中的分布，及其可信性特性的数据；

——已有的对可信性特性的全部认识及其评估范围。

对系统要求文件和系统规范文件的分析还应包括检查整个系统中备选通道的启动方式，即：

——静态方式，通过改变系统的配置；或

——动态方式，例如借助于信任性机理自动启动或通过键盘操作手动启动。

7.2.2 影响条件

GB/T 18272.1—2000 的 4.4 列出的下列影响条件可对系统的可信性造成影响：

——系统承担的任务，例如系统过载等；

——系统连接的工业过程，例如电噪声；

——系统连接的外部各系统，例如电噪声等；

——提供系统使用的公用设施（气、电等），例如电压变化；

——系统所处的环境，湿度、温度等。

对于可信性的各种特性而言，主要影响条件有下列几个：

a）可靠性：

——公用设施；

——环境；

——服务：由于部件的搬运、储存等造成的影响。

b）维修性：本标准认为维修性是系统本身的固有特性，只会间接受影响，例如因危险条件造成接近受限制。

c）可用性：在考虑使系统维持或恢复到系统能够执行系统任务的状态所需采取的措施时，可用性会受到人为因素和服务条件（备件到货误期、培训、文件编制等）的影响；

d）信任性：信任性的安全性和忠实性机理会受人为因素有意无意的影响，如果这两种机理共用总线或多任务处理器等设施，则会受到系统任务、过程活动突然增多（例如突然出现报警）造成的过程和外部系统的影响。

总之，系统预定工作场所的参比条件发生任何变化都会使系统的正常工作受到影响。

在规定试验项目评定影响条件的影响时，应参阅下列标准：

——GB/T 2423；

——GB/T 2424；

——GB/T 17626。

7.2.3 汇编收集的信息

按上文所述收集来的信息应以一定的方式汇编成册，供设计评估程序时使用。

信息汇编方法的实例见附录 A（提示的附录）和附录 B（提示的附录）。

7.3 设计评估计划

7.3.1 分析系统要求文件和系统规范文件

设计评估计划的第一步工作是分析按 7.2 规定从系统要求文件和系统规范文件中收集的信息。

将系统要求文件与系统规范文件进行比较后，逐一列出每项任务的全部建议的功能、模块、元件以及为达到可信性要求而提供的其他一些手段。

列入此清单的每个项目都是潜在的评估项目。

检查每一个潜在评估项目，确定这些项目的评估深度，使之达到提高置信度水平的要求。

7.3.2 评估项目

按下列条件对整个评估项目进行筛选压缩：

——任务对于使命的重要性；

——在原有经验基础上的现有置信度水平，这可以是系统以往成功执行类似或相同使命、对制造商的了解程度以及用户使用同一类型或类似系统的经验等基础上的置信度水平；

——新型系统的成熟程度，投入运行的参照系统的数量、装置、接口、操作系统和编程语言的标准化

程度。有关标准可以是国际标准、国家标准，也可以是专有标准；

——不同功能的相互依赖程度，接口的数量，同一功能反复用于执行不同任务的次数；

——技术上的制约条件，如尺寸、重量、公用设施的有效性、对试验环境的控制。

7.3.3 评估工作

经过 7.2.3 的筛选压缩，在清单的每一个项目上增加下列内容，就形成一份评估工作清单：

——要求进行的分析和试验的类型；

——进行每一项分析和(或)试验工作所需知识的技能；

——试验可能产生的永久性影响对评估计划的制约；

——经过挑选的可用人员；

——开展分析和试验所需要的工具和设施；

——预计每项分析和试验所需的成本和时间；

——每一项评估工作的优先程度。

按照 7.3.1 和 7.3.2 确定的原则，可能需要考虑几种评估技术，这几种评估技术要能够相互补充。

利用评估工作清单，连同为评估其他特性而制定的类似清单一起，可以形成一份总的系统评估大纲。

7.4 评估大纲

最终确定的评估大纲至少应规定和(或)列出下列要点：

——8.2 所述的系统可信性推断定性分析；

——7.2 所述需要考虑的原则；

——按 7.3.3 要求规定的评估工作；

——需要分析和(或)评定的故障模式及预计产生的影响；

——系统具备的忠实性和安全性机理；

——要求达到的置信度水平；

——评估计划要考虑到试验可能产生的永久性影响。

8 评定技术

8.1 概述

必须选用可以将评定结果与系统要求文件的要求做定性和(或)定量比较的评定技术。

可以选择只需根据系统文件进行分析的评定技术，也可选择需要接触实际系统以实验为依据的评定技术。

由提供选择的评定技术得出的试验结果可以是定量的，也可以是定性的，或者是定量和定性结合的。

本标准推荐了几种评定技术，当然也可以采用其他评定技术，但不管采用何种技术，评估报告都应提供有关这种技术的参考文件。

评估需要考虑的项目可查找 GB/T 7289。下面所述的分析技术是以模型为依据的，不能百分之百保证这种模型能切实代表实际系统。因而还应标明以这种分析技术取得的评定结果的置信度。

系统的可信性还受设计、规范和制造三个阶段中产生的系统错误的影响，系统的软、硬件都会存在这个问题，只有通过细致地检查每一项功能的执行情况才能发现这些错误。

此外，注入假设故障或错误的技术可以提高设计、规范和制造各个阶段所达到的系统最终可信性的置信度，因而很有使用价值。这两种故障注入技术(使用硬件和(或)专门设计的软件)可用于找出假设故障或错误对系统任务的总体影响。

但必须意识到，实际上置信度的提高是有限的，因为能够设计出并付诸实施的试验项目，其数量受所有能够想到并注入系统的可能错误和故障的数量的制约。

8.2 定性评定技术

定性评定的基础是预测分析或试验。

无论是预测分析还是试验，都需要通过分析系统的功能结构和物理结构，确定系统执行任务的方式才能开展评定。

系统的结构可以用功能框图和物理框图、信号流程图、状态图、表格等来描述。

考虑系统所有元件(硬件和软件)的故障模式。确定其对系统任务可信性的影响，以及维修性要求的影响。

可以采用下述一种方法或综合几种方法进行定性分析。

8.2.1 归纳分析法

在组件或元件层次上确定故障模式，分析每一种模式对高一级系统任务可信性的影响。此故障影响即成为高一级层次的故障模式。

这种“自下而上”的分析方法要到最后才能确定各种假设故障模式在系统各个层次上的影响。

GB/T 7826 对这种归纳分析法做了详细说明。

8.2.2 推断分析法

推断分析从系统最高层次的假设故障即任务故障开始，各层次依次进行，直至底层。

逐层分析以确定将导致最高层(即任务层)产生故障的故障模式和相关故障。

沿着功能上的和物理上的路径，重复这种分析直至获取足够的可信性(包括维修性)信息，供评估用。

对于不属于假设事件的故障模式，推断分析不提供任何信息。但对于较复杂的系统，推断分析则非常节省时间。对于比较复杂的系统来说，描述如何认定系统的故障或成功要比认定系统各组件的所有各种可能的故障模式方便得多。

故障树分析(FTA)是一种适用的推断分析法。

8.3 定量评定技术

定量评定技术的依据可以是预测分析和计算也可以是试验。

无论以何种为依据，都必须从分析系统的功能结构和物理结构以及系统执行任务的方式开始进行评定。

系统的结构可以用功能和物理框图、信号流程图、状态图、表格等来描述。

要考虑系统所有元件(硬件和软件)的故障模式。确定故障模式对系统任务可信性的效应，以及维修性要求的影响。

定量评定可以按下列一种方法进行，也可以综合各种方法进行。

8.3.1 预测评定

预测评定以定性分析结果辅以系统元件基本可靠性(故障率)的量化值为依据。在定量表示系统执行任务的故障率时需要采用预测分析法。可靠性方框图法是一种适用的预测分析法。

可靠性方框图几乎可以直接根据系统的功能结构和物理结构绘制。此种方法主要用于成功(两种状态)分析，不能有效处理复杂的修理和维修策略，也不能用于具有多种状态的情况下。

各种数学工具都可用于计算故障率，例如布尔代数、真值表、和(或)通路割集分析等都可供使用。在以定量的方法预测多状态情况下系统执行任务的故障率时，可以采用马尔可夫分析法。

但如若有大量的系统状态需要考虑，则马尔可夫分析法会变得非常复杂，在这种情况下，最有效的是应用马尔可夫分析法计算采用“故障树分析”等其他分析方法推导出的分析模块子集的可靠性数据。

根据现场经验或者采用“部件计数可靠性预测”法计算模块和元件组件的通用数据，可以取得上述分析方法使用的模块和元件的基本量化故障率数据。

在说明影响条件造成的应力强度时，宜采用有关应力模型方法。

部件计数法是以这样一种假设为依据的，即各种组件在功能上是互相串联的(最坏情况下的估计)。

分别列出每一个系统模块和元件的组件，说明每一个组件的类型、其恰当的故障率、影响故障率的因素（部件质量、环境等）以及使用的数量。

在附录D（提示的附录）列出的美国军用标准化手册MIL-HDBK-217，A至F期中列有另一种可供选用的一般故障数据。

对于比较复杂的系统，例如工业过程测量和控制系统，事实上是不可能对可信性的特性做精确的预测评估的。

但对于系统中有足够数量投入使用，能够收集到具有统计意义的现场数据的那些部分，可以对可靠性做出局部的精确预测。

系统的维修性、防护性和忠实性等特性主要取决于设计赋于系统的特点，因此这些特性的存在程度是不能以概率统计的方法加以计算的。必须考虑保证系统安全性和忠实性的元件的可靠性。这些元件的可靠性的评估方法可以与支持系统基本功能的元件和模块的评估方法相同。

8.3.2 评定可信性的试验

8.3.2.1 引言

仅仅通过系统一级的试验来判定一个复杂系统的可靠性和可用性，即不现实也不经济。通常情况下，复杂系统都是独一无二的（样品数为1）。此外，试验的范围必然会受到允许试验时间的严格限制。但对于已投入运行的系统，这类试验则能提供有价值的数据。

由此所取得的实际数据可以用于：

——日后指导改进系统设计和系统结构，重新设计或更换易出故障的设备和软件；

——将预期特性或规定特性与实际数据相比较；

——产生可用于今后可信性预测的现场数据。

确定试验项目时必需遵循的程序可查阅GB/T 15647和有关标准。

对系统进行试验的主要目的是评定系统在出现故障（硬件和软件）、出现未经许可或错误的输入（忠实性和安全性）时的工作状态。

为了观察系统的工作状态，首先应确定一项或一组典型的任务，同时确定每一项任务的被认为属于故障的系统状态（例如输出的状态）。

8.3.2.2 采用故障注入技术的试验

实施故障注入试验之前，应检查系统的技术规范，以便确定：

——为避免故障在系统中传播而采取的忠实性措施；

——为避免故障或未经许可的输入的侵扰而采取的安全性措施；

——系统所具备的诊断特性。

为有效利用时间，应该在定性分析的基础上设计系统试验项目，并尽可能使用系统所具备的和提供给系统的诊断特性。必须注意，在需要由诊断特性提供系统可信性数据的场合，诊断特性本身必须单独接受试验。

在试验系统的忠实性时，可向模块、元件和（或）组件注入故障，然后观察系统是否出现下列情况：

——系统输出故障；

——通报发生故障。

在试验系统的防护性时，可以在系统边界注入故障或者输入未经许可的信息，即不正确的输入、操作和（或）维修工作中的人为错误。

应注意列入若干能同时试验忠实性和防护性的试验项目。故障在系统中的唯一影响是可能会妨碍对输入故障的检测。附录C（提示的附录）列出了若干种故障，可供实施上述试验时使用。

8.3.2.3 环境扰动试验

影响条件的某些扰动能触发防护性机理。

因此，在试验防护性机理时，所选择影响条件的变化应不超出正常值范围。

在选择影响条件时，可参阅 7.2.2。

9 评估的实施与评估报告

评估的实施与评估报告的编写方法应按 GB/T 18272.1—2000 的 5.5 和 5.6 的规定执行。

评估报告还需写明下列要点：

a) 评估计划及必要的变动；

b) 汇总系统要求文件和系统规范文件中的有关数据，例如系统任务、可信性要求、环境条件、工作条件和维修条件等；

c) 对系统的分析；

——系统的物理结构和功能结构，作用于系统各模块、元件和组件的应力，可信性评估各个方面选择模型的依据。

d) 模型适应性

——如果预测需要，模型适应性应考虑精确度要求；

e) 获得数据，例如数学模型的数据来源；

f) 提供计算报告并附计算结果的精确度；

g) 进行的试验：

——有关试验的说明和选择试验项目的依据；

——仿真的故障形式；

——根据定性分析预计的运行情况；

——从定量分析中推导出的预期故障发生频率；

——为了仿真模块、元件或组件的故障，测试系统的忠实性和安全性而注入系统的故障类型，诸如：经输入/输出元件引入的错误，人为错误产生的故障(例如因维修不当造成的不良后果)，由于误用造成的错误(例如使用不合法代码)；

——作用于系统界面的影响条件的性质和等级；

——故障的覆盖范围；

——识别故障时间；

——故障的隔离(故障的清除)；

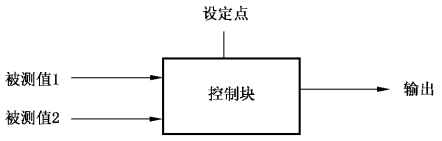
——故障位置测定时间；

——检查在线诊断的正确性，例如是否发生虚假报警，是否能正确识别和区分与过程操作有关的系统故障等；

h) 建议做进一步分析和(或)试验的评估项目清单。

附 录 A
（提示的附录）
系统要求文件中“主从控制”任务的信息和文件格式要求实例

A1 任务简图



A2 界面状态

可能的输入状态：

——被测值 1：＞高限，正常，＜低限

——被测值 2：＞高限，正常，＜低限

——设定点 ：＞高限，正常，＜低限

可能的输出状态：

——输出：全开、冻结、跟踪、全关

A3 可信性（见表 A1）

表 A1 可信性

任务		状态	故障事件		
			预计频率	采取的措施	恢复时间
主从	输入	测量 1			
		＞高	1 次/年	报告/冻结输出	*
		正常	NA	—	—
		＜低	1 次/年	报告/冻结输出	*
		测量 2			
		＞高	1 次/年	报告/冻结最后值	*
		正常	NA	—	—
		＜低	1 次/年	报告/最高输出	*
		设定点 1			
		＞高	1 次/年	报告/冻结最后值	2h
		正常	NA	—	—
		＜低	1 次/年	报告/最高输出	2h
	输出	输出			
		＞高	1 次/年	报告/冻结最后值	2h
		正常	NA	—	—
		＜低	1 次/年	报告/冻结最后值	2h

注

1 测量的输入是否受系统的控制，取决于被评估系统的边界。在实例中，测量是在边界外进行的，因此标出了故障事件的“预计”发生频率这一术语。同样，“恢复时间”不是系统所要考虑的。设定点是由键盘控制的，因此在系统的控制之下。

2 NA＝不用。

3 ＊＝此量值非系统特性。

附 录 B
（提示的附录）
系统规范文件中“主从控制”任务的信息和文件格式要求实例

任务	支持单元			可信性特性				
	功能	模块	元件	可靠性	可用性	维修性	安全性	忠实性
主从	I/O 监视器	I/O 模块	输入卡隔离 输出卡隔离 电源 I/O	1）	1）	1）	2）	2）
	控制	过程模块 1	CPU-PM FbusC DIA PS-PM SysBusC					
		或						
		过程模块 2	CPU-PM FbusC DIA PS-PM SysBusC					
	人机接口	操作站 1	CPU-OPS Mem-card Grd-card SysBusC					
		或						
		操作站 2	CPU-OPS Mem-card Grd-card SysBusC 3）					

1）采用有关确定可信性特性的格式。

2）应参阅“系统规范文件”的说明。

3）表中出现的缩略语为某一制造厂表格中使用的，仅供本表示例之用。

附 录 C
（提示的附录）
信 任 性 试 验

C1 引言

向系统注入故障的试验有助于评估系统（硬件和软件）的信任性。

这些技术，要求试验人员对系统的操作以及系统的物理和功能结构有深入的了解，往往还需要实际接触系统。

这些试验的基本原理是：一个可信的系统，无论其元件出现故障还是受到来自各界面外的干预，都必须能正确地执行其任务。

试验的方法包括制造故障（以试验其忠实性）和（或）引入未经许可的或错误的操作（以试验其防护性），观察由此造成的系统工况（输出状态和（或）发出的信号）。

下列问题与系统的工况有关，需加以考虑：

——出现故障时，输出是否转入或冻结在预定的位置？

——屏幕不能正确工作时，键盘是否能自动锁定？

——通信过载时，系统如何动作？

——注入故障后监视、报警和打印装置是否有信号显示？

在定性分析的基础上协调各项试验，首先从插件板层次开始进行试验，然后逐步转向集成电路插脚这一层次，尽量避免不必要的工作。

引入系统的故障通常都是单一的稳定故障。

注入故障的类型，例如：

——拆除插件板或模块；

——脱开插件板的接头（大多数系统故障是由于接触不良造成的）；

——脱开 IC 插脚或使之表示一个逻辑 0 或 1。

为使试验能正常进行，可能需要采用下列特殊配置：

——带开关的扩充板；

——夹具；

——特殊试验软件。

视评估的深度，这种试验方法可能比较费时，但其优点是易于实施，所需的试验设施相对较便宜。

注：在进行这些试验时，必须注意并采取措施以避免使系统的某些元件受损坏。

C2 注入的故障

GB/T 7826 对系统的潜在故障模式做了分类。

下列条款确定了一部分可导致系统失灵的故障，可供仿真系统故障时使用。

C2.1 由于模块、元件或组件的故障造成的系统故障

——单个电源装置丧失电源；

——备用电源装置（有源和无源装置）丧失电源；

——备用模块及电源模块的初级和次级端丧失电源；

——单个模块和元件丧失电源；

——单个及备用模块和元件之间的通信总线失效；

——模块或元件失效；

——外围设备(显示屏、键盘、打印机、软盘驱动器等)丧失电源;
——与外围设备的通信失效;
——电源线、通信总线、寻址线路、输入/输出线路断开或短路。

C2.2 人为错误造成的系统故障

因维修、重组配置和改进软件不当产生的错误可导致系统故障:
——备用总线电缆混乱;
——模块、元件等的地址设定不正确;
——印制电路板插错位置;
——印制电路板插倒;
——接插件插倒或插反;
——接插件插错位置;
——修理后接插件未插好;
——电源接反;
——预置或起动程序不完整或不正确;
——两次使用同一地址等。

C2.3 不正确或未经许可的输入经人—机接口进入系统导致的系统故障

——呼叫或使用不存在的或不正确的显示、标记码、程序或外围设备;
——因短时间内输入大量指令,在键盘、触屏上造成溢出状态;
——使用不完整的编码呼叫显示和标记等。

C3 观察

注入上述故障后提出下列问题,然后记下问题的答案:

a) 有哪些系统任务受到影响,它们是如何受影响的?
——各个对应模块是否仍然能检测到输入信号的变化?
——各个模块中的输出信号是否响应正确的输入信号?
——提供给操作者的数据显示是否依然正确?
——装置与装置,装置与主计算机、操作站、打印机等之间的通信是否正常?
——模块中是否出现暂时性的操作中断?

b) 系统是否能:
——自动地或在一定时间内报告故障?
——周期性测试后自动报告故障?
——故障是由系统的哪一级报告的(操作站、系统元件)?

c) 系统是否提供保护措施避免故障的发生?
——是否防止故障扩散?
——是否借助备用通路继续工作?
——系统任务是否降级?
——是否借助备用装置继续工作?这样做是否使系统任务降级?
——在系统无法继续正确工作的情况下,输出是否达到预定值?

d) 是否有可能在不影响系统任务的情况下进行在线修理?
——是否通过提供故障部件的明确信息报告故障?
——能否在不影响或不中断系统其他模块或元件工作的情况下更换有缺陷部件?
——经过修理或备用的模块或元件重新插入系统后是否能自动起动并正常工作?

C4 试验结果的分析

为便于分析试验结果，首先要计算引入故障的以下两个百分数：

——系统状态正确；

——信号发送正确。

尽管不能绝对相信这些数据，但用于比较还是有价值的。

在评估可用性时也可以采用类似的方法，自测试的覆盖率可以按自测试测定故障的百分率进行计算。

附 录 D
（提示的附录）
参 考 文 献

GB/T 5080.1—1986 设备可靠性试验 总要求 (idt IEC 60605-1:1978)

GB/T 5080.2—1986 设备可靠性试验 试验周期设计导则 (neq IEC 60605-2:1994)

GB/T 7288—1987 设备可靠性试验 推荐的试验条件 (idt IEC 60605-3:1986)

GB/T 5080.4—1985 设备可靠性试验 可靠性测定试验的点估计和区间估计方法(指数分布) (neq IEC 60605-4:1986)

GB/T 5080.6—1985 设备可靠性试验 恒定失效率假设的有效性检验(idt IEC 60605-6:1989)

GB/T 5080.7—1986 设备可靠性试验 恒定失效率假设下的失效率与平均无故障时间的验证试验方案 (idt IEC 60605-7:1978)

IEC60300-3-1:1991 可信性管理 第3部分：应用指南 第1节：可信性分析技术：方法学指南

USA 军用标准化手册 MIL-HDBK-217，A至F期："电子设备的可靠性预测"

中华人民共和国
国家标准
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
GB/T 18272.5—2000
*
中国标准出版社出版
北京复兴门外三里河北街16号
邮政编码:100045
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行 各地新华书店经售
*
开本 880×1230 1/16 印张 1½ 字数 38 千字
2001年8月第一版 2001年8月第一次印刷
印数 1—2 000
*
书号:155066·1-17724 定价 14.00 元
网址 www.bzcbs.com
*
科目 577—584

GB/T 18272.5-2000