ICS 21.020
K 04

中华人民共和国国家标准

GB/T 9414.5—2018/IEC 60706-5:2007
代替 GB/T 9414.7—2000

维修性　第5部分:测试性和诊断测试

Maintainability—Part 5:Testability and diagnostic testing

(IEC 60706-5:2007,Maintainability of equipment—
Part 5:Testability and diagnostic testing,IDT)

2018-06-07 发布　　2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 9414《维修性》分为以下几个部分：

——第 1 部分：应用指南；

——第 2 部分：设计和开发阶段维修性要求与研究；

——第 3 部分：验证和数据的收集、分析与表示；

——第 5 部分：测试性和诊断测试；

——第 9 部分：维修和维修保障。

本部分为 GB/T 9414 的第 5 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分代替 GB/T 9414.7—2000《设备维修性导则　第四部分：诊断测试》，与 GB/T 9414.7—2000 相比主要变化如下：

—— 规范性引用文件中增加了对 IEC 标准的引用；

——第 4 章修改为“测试性描述和诊断测试”；

——第 5 章修改为“测试性规范”；

——第 6 章修改为“开发过程中的测试性”；

——增加了第 7 章“测试性评估”和第 8 章“测试性文件”。

本部分使用翻译法等同采用 IEC 60706-5:2007《设备维修性　第 5 部分：测试性和诊断测试》。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 2900.13—2008　电工术语　可靠性与服务质量(IEC 60050-191 :1990，IDT)

——GB/T 9414.1—2008　维修性　第 1 部分：应用指南(IEC 60300-3-10:2001，IDT)

——GB/T 9414.2—2012　维修性　第 2 部分：设计和开发阶段维修性要求与研究(IEC 60706-2：2006，IDT)

——GB/T 9414.3—2012　维修性　第 3 部分：验证和数据的收集、分析与表示(IEC 60706-3：2006，IDT)

本部分做了下列编辑性修改：

——修改了标准名称。

本部分由中华人民共和国工业和信息化部提出。

本部分由全国电子电工产品可靠性与维修性标准化技术委员会(SAC/TC 24)归口。

本部分主要起草单位：工业和信息化部邮电工业标准化研究所、北京邮电大学。

本部分主要起草人：夏海轮、武冰梅、曾志民、刘银龙、黄正磊、黄蓉。

本部分所代替标准的历次版本发布情况为：

——GB/T 9414.7—2000。

引　言

测试性是系统或设备的使用和维修中的一个重要特性，对系统或设备的可用性和维修性起举足轻重的作用。诊断测试可以人工进行，也可用具有不同自动化程度的测试设备进行。测试性的优化设计要求设计、使用和维修组织间的密切协作。本部分旨在强调测试性和诊断测试多方面的要求并有助于彼此间的及时协调。

在本部分中，合同对象：系统、设备或功能部件，统称为“产品”需要考虑测试性设计。每个产品需执行其必需的功能，这些功能宜在研发和生产阶段进行校验并在整个寿命周期中得到保持。为保持产品的功能性，在该产品运行的任何时间都要知道每个子功能的功能状况。如果发生失效，宜采取措施确保识别故障并定位产生故障的单元。产品测试性的要求可能看来很简单，但是如果在产品开发开始阶段没有对其考虑，随后的实现将导致工作量的增加和成本的显著提高。如果所有要求在开发开始阶段都能实现，研发工程师不需要大量额外的工作就可以详细说明功能特性“测试性”，从而可以显著地节约成本，例如通过减少检验开发结果的测试步骤数节约成本。经验表明，开发阶段的额外成本和工作可以得到补偿，例如现有的测试设备可用于生产阶段。可靠的故障识别和低廉的运行过程中的维修成本，大大增加了可测产品的市场价值。

由于本部分适用的产品涉及广泛的技术，本部分采用通用方式对有关工艺和技术内容进行撰写。因此，本部分只提供对产品估计的评估依据和实现必需的产品测试性的基本方法。产品的故障识别和故障定位的技术实现是产品开发工程师的任务，该技术的实现依赖于产品开发时的技术水平。因此，所需的测试任务是以硬件形式或者软件形式来实现并不重要，重要的是所有功能都能通过测试路径来检查，且已确定的测试性特征值和给定目标值相符。如果与目标值有偏差，宜采用措施以确保目标值得到满足。这些措施宜在冻结设计前的开发早期阶段进行实施。

维修性　第5部分:测试性和诊断测试

1　范围

GB/T 9414的本部分目的在于:

——为在设计和开发中早期考虑测试性方面的问题提供指南;

——有助于确定有效的测试程序作为运行和维修的组成部分。

本部分适用于包括商用现货在内的所有类型产品,无论是机械、液压、电气还是其他技术。另外,本部分适用于任何产品的开发,使得产品特性是可验证的(可测的)。

本部分的目标是确保在开发初期就定义好与产品测试性相关的先决条件,使得由客户制定的条件在开发过程中落实、记录归档和验证。

本部分还提供了作为产品设计一个完整部分的测试性的实现和评估方法,并建议在产品寿命周期内宜对产品测试性文件不断更新。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

IEC 60050-191　电工术语　可靠性与服务质量(International electrotechnical vocabulary—Chapter 191:Dependability and quality of service)

IEC 60300-3-10　可靠性管理　第3-10部分:应用指南　维修性(Dependability management—Part 3-10:Application guide—Maintainability)

IEC 60706-2　维修性　第2部分:设计和开发阶段要求与研究(Maintainability of equipment—Part 2:Maintainability requirements and studies during the design and development phase)

IEC 60706-3　维修性　第3部分:验证和数据的收集、分析与表示(Maintainability of equipment—Part 3:Verification and collection, analysis and presentation of data)

3　术语和定义、缩略语

3.1　术语和定义

IEC 60050-191界定的以及下列术语和定义适用于本文件。

3.1.1

机内测试　built-in test;BIT

产品内在的能自动识别和定位故障的测试。

3.1.2

机内测试设备　built-in test equipment;BITE

用于实现机内测试功能的硬件和/或软件。

3.1.3

商用现货　commercial off-the-shelf;COTS

标明商用的现成产品。

3.1.4

危害性　criticality

故障的影响程度。

注：危害性用级数来表示，级数越高，故障所引起的预期后果就越严重。

3.1.5

测试深度　depth of test

一个单元或子单元测试级别的说明和描述。

3.1.6

设计层级　design level

在产品分解结构中，对现存的设计要素(功能和/或物理单元)指定的层级。

注：有些情况下，“设计层级”也称作“约定层次”。

3.1.7

诊断正确率　diagnosis correctness

产品的故障在给定条件下能被正确诊断的比例。

3.1.8

诊断测试　diagnostic testing

用来进行诊断的测试程序。

3.1.9

虚警　false alarm

有故障指示时未发现故障的情况。

3.1.10

虚警率　false alarm rate

故障指示中虚警的百分比。

3.1.11

故障识别时间　fault recognition time

出现失效的时刻到故障被识别之间的时间。

3.1.12

故障模拟　fault simulation

为检验诊断能力，在硬件单元中采用非破坏性的干预使故障产生和/或通过软件模拟故障。

3.1.13

功能　function

产品所要求具有的能力。

注：在产品分解结构中，功能总是与指定层级相联系。

3.1.14

功能模型　functional model

描述激励与测量(响应)终端之间相互影响、相互依赖关系的概念性表示。

注：产品开发中的功能模型是显示产品功能，并辅以由开发者制定的测试路径的主要框图。

3.1.15

功能测试　functional test

测试硬件单元的所有指定功能以检验产品能力。

3.1.16

硬件单元　hardware unit

以硬件形式实现功能和/或子功能的设计要素，也可能包含软件部分。

3.1.17

现场可更换单元　line replaceable unit;LRU

可由用户或维修支持方直接在设备上更换的可更换硬件或软件单元。

3.1.18

维修方案　maintenance concept

设计水平和用于产品维修的维修水平间的相互关系。

3.1.19

维修策略　maintenance policy

基于所有者、使用者和客户的目标和策略所提供维修和维修保障的通用方法。

3.1.20

监测　monitoring

在选定的运行模式下,对其功能自动观测,且不影响运行。

3.1.21

运行环境　operational context

产品运行所期望的环境。

3.1.22

参数　parameter

规范功能的物理量。

3.1.23

产品　product

指定的可交付物品或服务。

注1:从可信性角度讲,产品可能是简单的(例如一个器件,一个软件算法),也可能是复杂的(例如一个系统或一个包括硬件、软件、人为因素、辅助设施及活动的综合体)。

注2:产品有自己的生命周期阶段。

注3:product 和 item 有相同的定义。

3.1.24

产品分解结构　product breakdown structure

形象表示产品单元和子单元物理构成的树形结构。

3.1.25

车间可更换单元　shop replaceable unit;SRU

可在用户库房/车间、同等级的维修支持方或在供方车间更换的硬件或软件单元。

3.1.26

信号　signal

表示信息的物理变量。

注:一个信号可由一个或多个参数表示。

3.1.27

规范　specification

在给定等级的产品分解结构下,对产品功能的详细描述。

注:规范一般源自系统需求并且可以验证。

3.1.28

工作说明　statement of work;SoW

详细说明提供的货物和服务的文件。

注:工作说明由客户提出或接受,定义了合同中提出的工作和由承包者提供的工作。因此,工作说明形成了主要技术文件,根据该文件投标者提出他们的出价,承包者执行该工作,客户接受提供的货物和服务。

3.1.29

激励　stimulus

用于触发某种功能的具有确定参数的输入信号。

3.1.30

子功能　sub-function

功能的细分(参见 3.1.13 功能)。

3.1.31

端口　terminal

用于测试产品信号的物理接入点的通称。物理实现或同义的相关术语有：

——插头；

——连接器；

——插头/插头型连接器；

——测试点；

——接口；

——转接口。

注：端口通常是由唯一的标识符来标识。

3.1.32

测试方案　test concept

系统测试性需求分析结果的描述和如何满足需求方法的规定。

3.1.33

测试覆盖率　test coverage

在给定测试规程下能诊断出有故障的功能数与总功能数之比。

3.1.34

测试设备　test equipment

实施测试所需的工具(硬件和/或软件)。

注：测试设备根据测试所涉及的技术分为机内测试设备(BITE)和机外测试设备。

3.1.35

测试规程　test instruction

描述在测试规范中所要求的测试如何实现的文件。

3.1.36

测试路径　test path

从相关联的硬件单元至端口测试步骤的描述。

注：此外,测试路径定义了激励与响应的(功能)关系。

3.1.37

测试序列　test sequence

一系列的测试步骤。

3.1.38

测试规范　test specification

详细说明测试序列、参数和功能的文件。

3.1.39

测试步骤　test step

硬件单元进行测试的最小单位。

3.1.40

测试任务 test task

满足故障识别和定位说明的所有必需测试的总和。

3.1.41

测试性 testability

确定产品在规定条件下能够被测试的程度的设计特性。

3.2 缩略语

下列缩略语适用于本文件。

ATE:自动测试设备(automatic test equipment)

ATS:自动测试系统(automatic testing system)

BIT:机内测试(built-in test)

BITE:机内测试设备(built-in test equipment)

COTS:商用现货(commercial off-the-shelf)

DP:数据处理(data processing)

FL:故障定位(fault localization)

FM:功能监测(functional monitoring)

FME(C)A:故障模式、影响(和危害性)分析[failure mode, effects, (and criticality) analysis]

FR:故障识别(fault recognition)

FT:功能测试(functional test)

FTA:故障树分析(fault tree analysis)

HWE:硬件单元(hardware unit)

LCC:寿命周期费用(life cycle cost)

LORA:修理级别分析(level of repair analysis)

LRU:现场可更换单元(line replaceable unit)

PCB:印刷电路板(printed circuit board)

SoW:工作说明(statement of work)

SRU:车间可更换单元(shop replaceable unit)

SF:子功能(sub-function)

TS:技术规范(technical specification)

4 测试性描述和诊断测试

4.1 概述

在产品设计及其寿命周期的各个阶段内,都考虑产品的测试性有助于对产品进行高效、经济的运行和维护。产品维修方案包括适用的诊断测试方法。测试性和诊断测试的实现是在产品的寿命周期内完成的。

寿命周期费用(LCC)是评价任何设计质量的一个越来越重要的方面。许多顾客除了关心直接采购费用之外,还要求控制与日常使用、维修及后勤保障相关的费用。这些费用主要受产品可靠性、维修性和维修保障特性的影响。在这个意义上,诊断测试技术的应用有可能使 LCC 的一部分费用显著降低。但在确定诊断测试要求时,应考虑 LCC 优化所带来的限制。

本部分适用于产品寿命周期的所有阶段,即:从确定产品需求的设计和开发阶段到制造和安装阶段,最终到运行和维修阶段,见图 1,具体包括:

a) 设计和开发阶段

从产品的概念到实现，产品需求应同其应用领域的具体要求相符，必要的情况下，可经历一些先期阶段。

b) 制造和安装阶段

在此阶段，需要使用当前设备验证诊断技术并评估产品的性能。准备文件并开始对运行和维修人员进行培训。

c) 运行和维修阶段

由于老化，被测设备可能会产生变化。考虑到诊断测试的连续需求，测试设备的测试功能需要延续并更换或升级。在后者情况下，测试设备需要在新开发阶段重新设计。

通过使用本部分，产生产品必要数据/信息的前提条件将得到满足，并且这些前提条件在产品整个寿命周期内可以验证和更新。

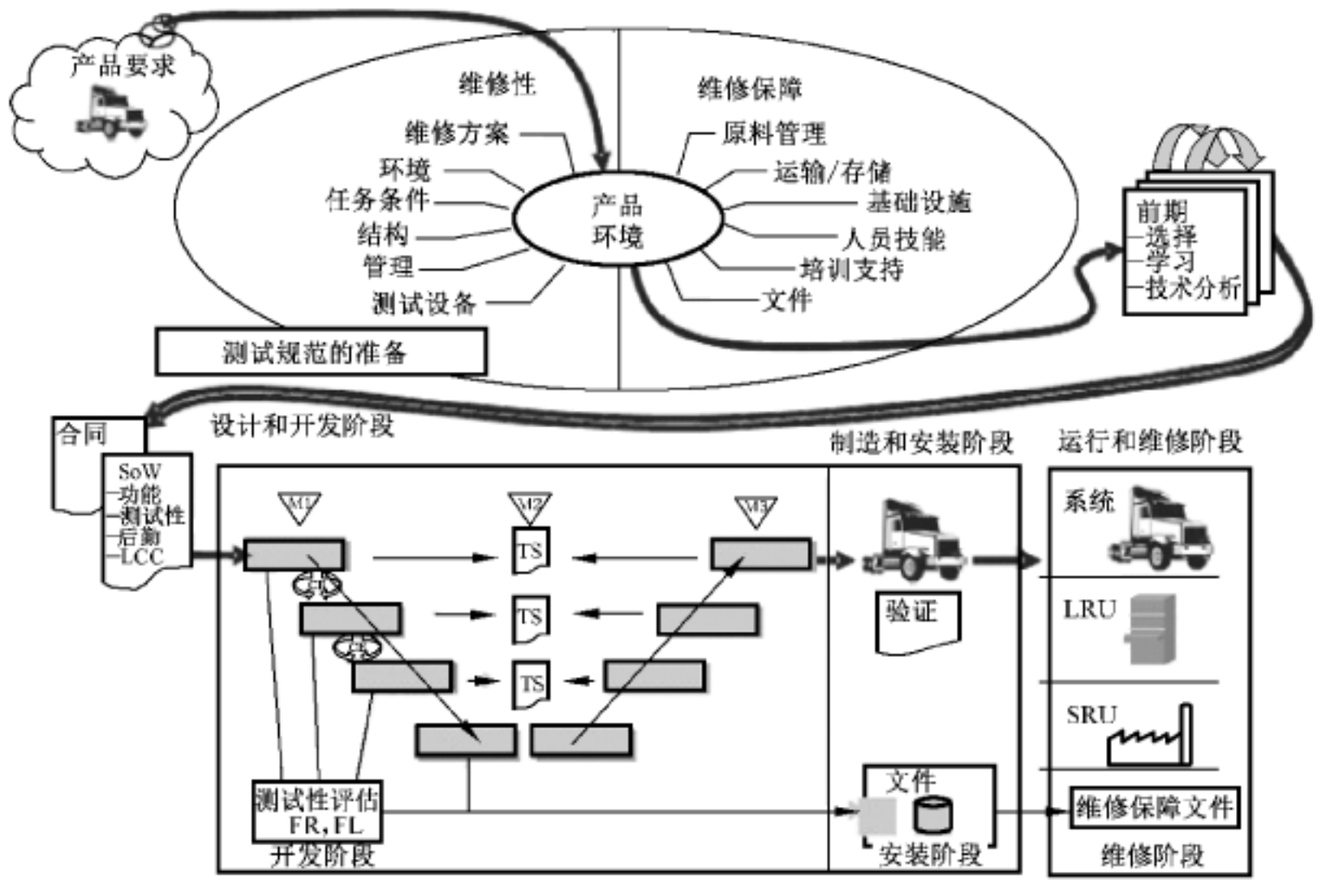
附录 B 给出了根据产品/系统设计如何进行测试性开发、记录归档和验证的例子。

诊断测试包括：

——功能测试，目的是验证功能是否仍然有效。

——状态监测，跟踪设备状态随时间的退化情况。

状态监测同诊断测试的有关概念密切相关，两者密不可分。但是，本部分只包含状态监测的部分内容。



说明：

TS——测试规范；

CE——并行工程；

M1——确认要求；

M2——分析验证；

M3——测试验证。

图 1 寿命周期内的测试性和诊断测试

4.2 测试性目的

设计和开发阶段的测试性与维修性、可用性和安全性密切相关，测试性的主要目的是为每个系统功能解决以下问题：

a) 诊断测试能否监测到功能故障。由于安全性的限制或测试可能具有破坏性(例如:对转子测试超速能力),某些功能是无法进行全面测试的。

b) 测试是否可行。功能故障的危险性、测试费用(测试设备的费用,测试设备维修费用及测试费用)以及使用较好的、较便宜的替代品不一定导致测试经济效益的提高。

注:在a)和b)两种情况下,需采取备选方案来确保这些功能在产品的寿命周期内能够正常运转。同时,这些因素也会影响测试覆盖率。由于不能在系统寿命周期内通过测试来确定系统的运行运转情况,低测试覆盖率也许是有害的,但在好的维修性和维修能力下,测试不是必须的。

c) 在寿命周期的哪个阶段进行系统功能测试。应该在寿命周期的每个阶段都考虑测试能力。比如,功能测试在单元级是可行的,但在系统级测试是不切实际的。这可以通过洗衣机及其排废水功能的例子进行解释。从用户的角度来说,通过预先运行测试来确认功能可以正常运转是有益的(运行阶段测试是无用的)。这个功能的设计不需要使用测试设备来对功能进行测试,这是因为:

1) 抽水机和相关部件的寿命比产品寿命长(其他故障及其维修费用限制了产品的寿命);
2) 能够便捷地使用排除可能故障的维修方法;
3) 能够在单元测试和交付前的系统测试中充分地测试完成排水功能的单元;
4) 哪一个阶段进行测试也会影响寿命周期费用。

d) 测试需要进行到何种深度。测试深度也是一项非常重要的标准,如在上面的例子中,它和维修观念是密切相关的。测试深度指明了区分单元或子单元的标准。例如:系统测试如果不仅能识别需要替换的单元,而且能在几乎不影响费用的情况下识别需要更换的子单元。这就能减小与单元级测试中识别和更换发生故障的子单元相关的测试设备费用。

核实所有开发的功能是测试性设计基本的原则。但需注意,测试覆盖率不必达到100%,因为测试本身在运行过程中可能产生故障,这比非测试故障,如测试或虚警带来的故障更严重。若涉及系统安全,无须所有测试覆盖率都达到100%,因为测试本身可能损害系统安全。在系统运行过程中,测试提供牢靠的保证是很重要的,为了达到这个目的,应精确确定测试覆盖率与100%的偏移量。

无论如何,测试性目的不应和更高等级的目的相冲突,如可用性。

e) 如何管理虚警和“未发现故障”。在故障并不存在的情况下,系统测试可能检测并向用户发送故障报告。这样会引起不必要的调查并最终导致虚警报告。当诊断为“未发现故障”(no fault found)时,也可能导致不必要的维修行为。各种方案的虚警率不能超过已规定标准,且应尽可能地减小至0。为减小虚警和“未发现故障”的发生可引入反馈系统,该系统将不断地评估环境并校准自身以适应部件在已规定标准内的损坏。反复测试消除虚警(测试方案可能因未产生警报而完全改变)会增长测试时间,应尽量避免使用。

当不存在故障时也可能显示故障。这是由于多种原因:

1) 如果在系统中发现了一个故障,且诊断出了发生故障的部件。但拆下该部件对其单独测试并未发现故障后,应检查同故障部件的测试规范相关的系统测试规范;
2) 诊断不足(测试中不能完全识别发生故障的部分);
3) 接口故障(例如,连接故障可导致移除某个单元后重新连接可以消除故障);
4) 欠佳的测试设备包括BITE(例如,发现的故障并不存在);
5) 间歇性故障(劣质部件在某些特定情况下会出现故障);
6) 设计容差累积故障(单元测试没有故障但系统测试有故障)。劣质部件在容许范围的极端情况下,会引起叠加的指标超标;
7) 软件故障(使用不当的测试方法所引起的故障);
8) 维修人员和用户的问题(培训不足、反馈速度、缺乏备件)可能使好的部件产生故障。

在运行及维修过程中,以上所有故障都可能引起不良影响,应尽可能避免。

f) 系统测试能否剪裁。系统测试与确保在给定输入和运行环境下系统能够正常运转有关。测试性需求及故障的定位能力不必规定测试步骤。测试总体功能与可能的后续深入测试能够节省大量时间并在很大程度上提高用户的舒适感。使用 FMECA(参见附录 B)和 FTA 等工具,有助于找到最可能失效的子功能以定义较低层测试的顺序。

4.3 诊断测试的目的

诊断测试的目标是按维修策略所确定的水平为被测设备提供最经济的快速清晰的故障识别方法。好的诊断测试应:

- 提高设备的可用性;
- 降低维修费用;
- 减少间接损坏的风险;
- 提高系统的安全性;
- 优化运行使用。

为实现该目标,诊断系统应:

- 提供置信测试以证实设备对其预定任务的适用性;
- 识别灾变失效和退化失效;
- 能将故障定位至某一失效的功能或 LRU;
- 通过评定耗损状态,发出临近耗损失效的告警;
- 提供设备使用和维修数据。

诊断测试设备的主要应用是:

- 系统运行前的安全性和功能性检测;
- 运行中实施的性能监测;
- 在使用环境中可识别失效组件或 LRU 层次上的设备失效;
- 利用指定的修理设施找出故障的详细位置。

4.4 用于诊断测试的方法

应用于诊断测试的可能方法包括利用从单纯的手动测量、机械特性的评价到全过程和安装的全自动诊断程序,对单个零部件及复杂系统进行测试。广泛采用的诊断方法可分为两类:

——外部诊断:使用的测试设备独立于产品,只在必要时才与之连接。所用的测试设备可能具有通用性,或者是对标准测试设备做一些改进,或者是针对被测设备而专门设计。可能也会包括计算机控制的 ATE(自动测试设备)。

——内部诊断:使用永久性的机内测试设备(BITE),在系统运行时 BITE 能连续地或间断地工作。另外,在系统非正常或非工作状态下,也可能进行专门的测试。

4.5 用于状态监测的方法

许多产品除得益于测试分散故障的诊断测试,还得益于状态监测。状态监测是预防性维修的一部分,它监测产品状态和性能的退化情况。

用于状态监测的方法依设备类型的不同而迥异,可包括:

——振动分析;

——流动性/润滑性分析;

——超声检测;

——热像分析;

——控制系统中置入报警和关机功能。

4.6 测试性的概念

测试性是产品的设计特性,可确保及时高效地评定某个单元的功能能力,并确保识别且必要时定位某个故障。测试性是确保产品维修性的主要因素。

诊断测试是维修方案中描述预防性维修部分的维修行为。测试覆盖率是诊断测试使用的程度。诊断测试包括两步:故障识别(FR)和故障定位(FL)。故障识别确定是否存在故障,故障定位确定故障的具体类型。

诊断测试也需考虑公差链。特定参数通常应规定上限和下限以区分正常运行和故障状态。一个单元性能的上下限可能有严格的限制,但在单元集成时,这些限制受到组成系统的其他单元变化的影响。在为某一测试定义具体的正常/失效偏差前,除考虑公差链,还应考虑进行测试的测试设备的精确性。开发阶段收集的测试结果为方案容差区间提供了预估计(产品功能容许偏差的总合和测试设备的精确性,包括测试设备激励的精确性和测量设备读入数据的精确性)。本部分中无需包括公差链的全部情况。

和功能相关的规范包含测试性。为测试性定义了故障识别和故障定位质量的特性值,它们对产品的基本功能特性有直接的影响。要遵循"待开发的功能必需通过参数值核实"这条规则,应从最开始同时将 FR 和 FL 作为功能性整体的一部分进行开发。这样才能将产品成本限定在预定值内。若后期综合考虑 FR 和 FL,将不仅会导致大量的时间延误,而且会导致产品质量下降和相当高的返工/纠正费用。

5 测试性规范

5.1 概述

诊断测试要求有效地转化为可测量的实际结果的一个关键前提是适当的合同条款。为促进诊断测试方案优化设计、开发和提供,用户应提供对其测试性的确切需求和约束。为此,应向供货方提供下列文件:

——工作说明(SoW)。该文件包含与测试相关的所有功能需求。在该文件中,用户详细说明包括测试性在内的所有期望功能/功能性。

——测试性规范。在该文件中,承包方(开发方)制定出 SoW 中所需运行和测试工程的功能及运行特性的实现方法(硬件,软件)。

5.2 工作说明

工作说明包含用户需求的详细说明而且是形成设计和开发工作的基础。在开发过程中如还能得到其他有用信息,可能进行改进,但更改应得到相互同意,因为这样经常会推延时间和增加费用。这些要求应包含:

——诊断测试的目的(见 4.3);

——运行方案(见 5.3 和表 1);

——维修方案(见 5.3 和表 2);

——经济环境的定性描述(见 4.1);

——首选的方法和解决途径(见 4.4)。

5.3 规范

测试性规范决定了产品的测试性需求,这也可能是开发阶段的要求。测试性规范需详细说明每个

测试阶段及与采用测试规范相关的功能单元。包括：

a) 诊断测试的任务及应用应包含：
   1) 与安全相关的故障清单，要求故障识别率应尽可能地接近100%；
   2) 严重故障清单，要求达到100%测试覆盖率，或者是不进行测试的原因；
   3) 所有其他功能的测试覆盖率或所有功能的整体测试覆盖率下限(需限定测试覆盖率的功能)；
   4) 故障识别时间的最大值；
   5) 故障定位时间的目标值(最大值)；
   6) 诊断正确率的目标值及最小值；
   7) 虚警率的最大值。
b) 测试性设计应包括：
   1) 一般要求；
   2) 详细要求检查清单；
   3) 测试性设计准则。
c) 下列验证的时机及规程：
   1) 测试性验证；
   2) 安全验证。

对不满足以上具体要求的后果应事先予以说明。

测试任务将在5.4.3进行详细说明。应在这一部分确定对可选方案(见5.6)进行评测的重要性。

诊断测试工作与产品的使用和维修过程密切相关。因此，在确定诊断测试要求时，使用和维修方案是应考虑的重要因素，它们应尽可能在系统寿命周期的早期确定，最好在概念和定义阶段。使用方案应首先考虑以使系统能完全满足其使用要求，维修方案应设计成能够以最低费用、最有效地利用资源去满足使用的需要。应始终考虑权衡的程度以实现常有的各种相互对立的要求之间的最佳平衡。

确定使用方案需考虑的各种要素见表1。为了能适当考虑维修环境和使用的限制条件，这些要素的每一项都应有详细规定。

维修方案决定了设计阶段应使用的测试任务、完成测试的人员及使用的测试设备。产品各阶段(开发、生产、运行、维修)的需求都应进行考虑。表2包含维修方案中需考虑的各种要素。

表1 使用方案的要素

要素	可能性		
场所	移动型		
	固定型	可转运	变化场所
			固定场所
		不可转运	
运行模式	持续运行	持续监测	
		间隔时段监测	
		允许中断和中断条件	
	间歇运行，包括间歇性条件		
运行应力条件	欠应力运行		
	标称应力运行		
	过应力运行		

表 1（续）

要素	可能性		
后果	安全性		
	费用		降低利用率
			间接损坏
			维修费用
	修复、紧急措施		
环境条件	机械应力		
	温度应力		
	电应力		
	化学应力		
	其他		
人员	未经培训		
	不同领域的培训		
	已经培训		高等程度
			中等程度
			低等程度
处理	手动		
	半自动		
	全自动		

表 2　维修方案的要素

要素	详细需求内容		
维修任务	预防性	维修	
		诊断测试	
		计划性维修	
	修复性	系统级	故障识别
			故障定位
			修理(更换)
			校准
			功能检查
		零部件级	故障定位
			修理
			校准
			功能检查

表 2（续）

要素	详细需求内容		
维修时间	连续监测		
	预防性维修	间隔	时间周期
			运行
		类型	级别
			定时维修
			视情维修
	修复性维修		
维修场所	固定	维修车间数量	
		维修车间区域分布	
		维修车间技术潜力	
	移动	维修站设备	
		维修站技术潜力	
维修程序	程序		
	资源	硬件	
		软件	
	文档（说明性的或图文的）		硬件的
			软件的
维修保障	库存品	库房数量	
		库房坐落分布	
		库存量	
		储存条件	
	库存品管理	采购	
		供应	
		运输	
维修环境	温度条件		
	其他条件		
维修人员	基本培训	培训部门	
		资格等级	
	专门培训	系统级	
		零部件级	
	进修培训	时间段	
		课程	

5.4 测试性特性

5.4.1 测试性的特征

测试性的特征可以由以下参数描述(其数学表达式参见附录 A):

——故障识别:见 IEC 60050-191;

——故障识别时间:见 3.1.11;

——故障定位:见 IEC 60050-191;

——故障定位时间:见 IEC 60050-191;

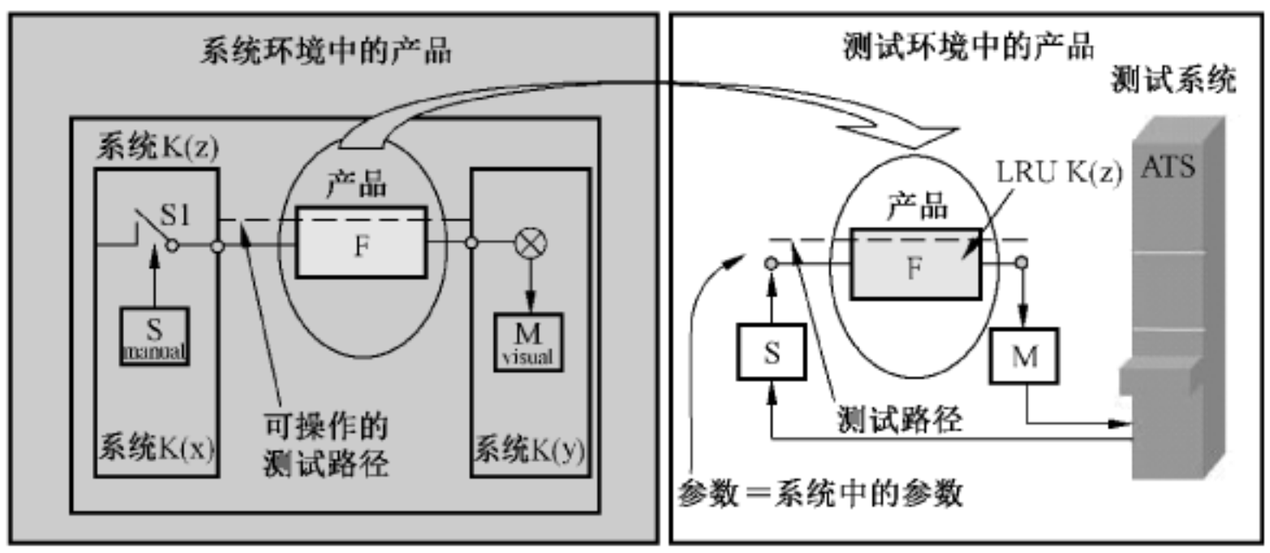
——诊断正确率:见 3.1.7;

——测试覆盖率:见 3.1.33;

——虚警率:见 3.1.10。

5.4.2 运行环境

依据 SoW 中产品的需求,产品可用于不同的运行环境。从测试性角度而言,区分了图 2 所示的规定设计水平条件下的系统环境(运行条件)和所需维修条件相应的测试环境。在测试环境中,产品工作于系统/产品仿真运行。这里,所有测试硬件单元的参数集都应与其所在系统相符合。图 2 表明产品之间是如何联系的。



说明:

S ——激励;

M——测量;

F ——功能。

K(x)、K(y)、K(z) 系统(项目)是结构分解的一部分。

图 2 运行环境

5.4.3 测试任务

5.4.3.1 测试路径

测试的最小单元包含一个测试路径,这个路径起始于至少一个激励,通过一个功能/子功能然后终止于一个与给定值比较的最接近的测量值。

故障识别要求测试路径通过一连串可更换单元的任何功能。

故障定位要求测试路径应该包括可更换单元间物理接口的测试。

测试任务包括故障识别和定位,并且按照表 3 中的各部分进行,其中 A+B+C+D=100%。

表 3　测试任务

部分	测试任务	故障识别给定值示例	故障定位给定值示例
A	运行中的测试(在线测试)	50%	0%
B	在测试条件下的测试,无外部测试设备(离线测试)	50%	95%
C	在测试条件下的测试,有外部测试设备	0%	5%
D	不可测试	0%	0%

表 3 列出的所有测试都可用于故障定位。有故障的可更换硬件单元(LRUs/SRUs)的定位可以通过包含在测试结果中的信息得到,而测试结果通过一系列覆盖不同跨接 LRU/SRU 的测试路径测试得到。功能模型(参见附录 B)提供了所需的信息。在该例中,故障识别的测试只覆盖了 A 和 B 部分,故障定位的测试只覆盖了 B 和 C 部分。

产品设计应规定能依照 SoW 描述的必要条件进行所有测试任务的特征。在允许的条件下,这些特征要被细分为机内测试 BIT(built-in test)和带有必要测试输入的外部测试设备。

5.4.3.2　机内测试

机内测试(BIT)是产品进行自身测试的功能。机内测试功能包含至少一个激励,通过一个功能/子功能的测试路径,以及至少一个包含与给定值对比的度量。需要的机内测试功能数来于 SoW 给出的必要条件,并且依赖于为故障识别制定的给定值。机内测试由硬件部分和软件部分组成。

注:在电子设备中,通过监测某些主要参数就能实现故障检测,比如供电电压,确定信号的能量波形或者频率,离散信号的一致性或者数据校验和。这些都是没有提供外部激励情况下,在线机内测试的特定形式。然而,通过机内测试设备(BITE)可以产生附加的参考信号,允许机内测试将它们和指标值进行比较。

在产品上进行的 BIT 测试构成了全部功能测试的部分测试,并且 BIT 测试可分为在线和离线两类。

在线测试是指在产品运行时连续进行的测试。

执行离线测试前应停止运行。通常这些测试只用于故障定位。

5.4.3.3　通过外部测试设备测试

如果需要外部测试设备且 SoW 允许,则可通过测试输入(如测试连接器)访问产品。外部测试设备的工作原理和机内测试功能的原理相同。因此,要求测试路径从激励开始,经过达到度量点的测试的功能,同时包括对测试结果的评估。

5.5　测试性评估的特征值

要实现本部分所有使用者测试性评估的一致性,需要引入测试性成分的特征值(FR、FL 和测试覆盖率)。这些值与产品无关,它们反映了可测试性产品所需的性能,并且本部分的所有使用者可进行比较。

特征值应提前在 SoW 中做出详细说明,它们是测试性评估的参照点。当进行特征值说明时,也应该考虑维修方案、工程工作及相关费用。如果这些要求已经提供给开发工程师的话,他应能对测试验证和安全验证做出评估。

对由于不符合以上规定要求而造成的后果,应事先予以详细说明。

5.6　选择诊断设计的评价标准

为优选诊断测试方案,应对供选择的诊断设计方案进行对比和评价,并应考虑下列经济准则:

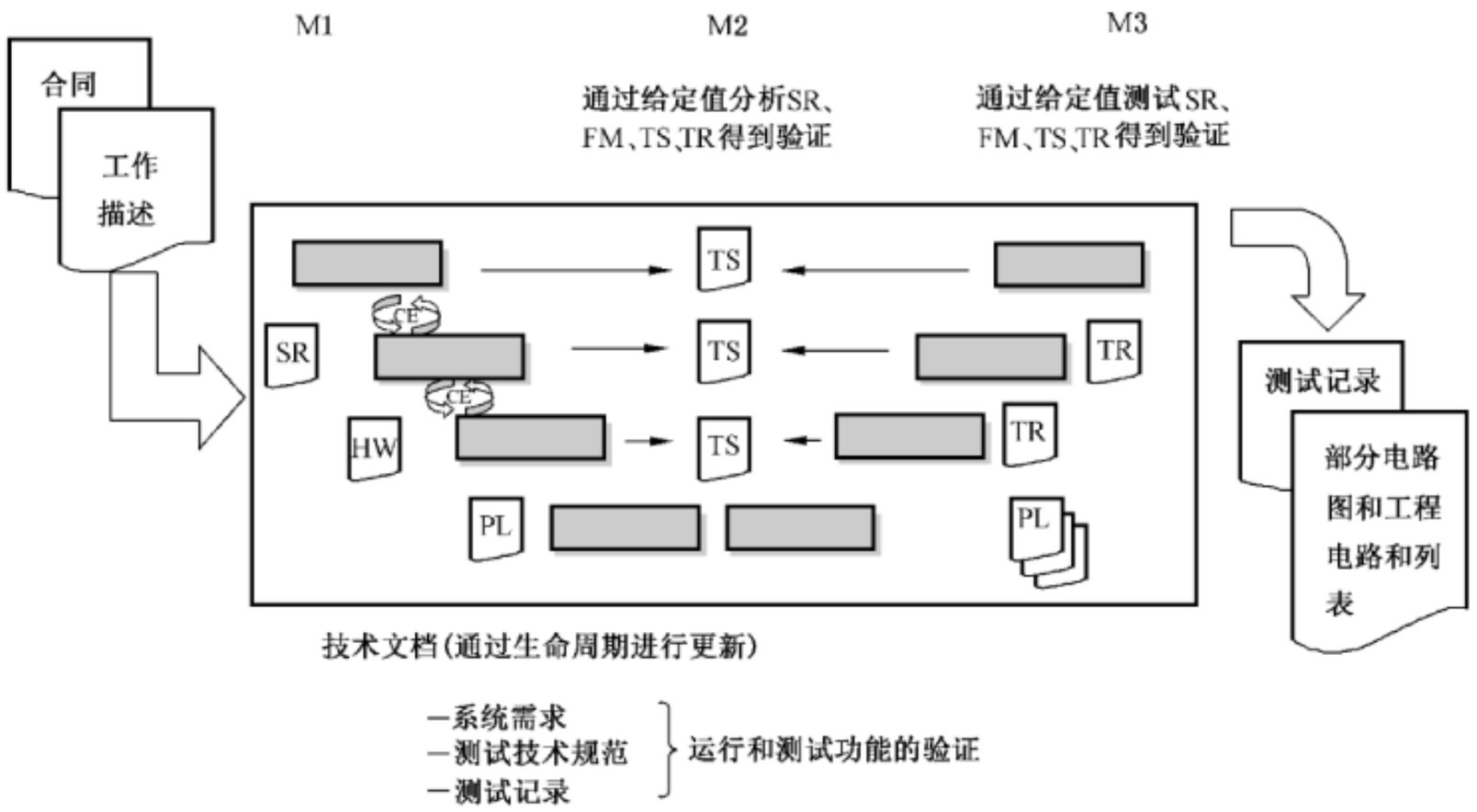
a) 主要费用：
   1) 基于使用性和可用性所需系统的数量；
   2) 开发费用；
   3) 一次性软件费用；
   4) 维修安装的费用。
b) 影响设备单元成本的因素：
   1) 复杂性；
   2) 生产数量；
   3) 冗余等级；
   4) BIT 能力的等级；
   5) 质量标准。
c) 与维修相关的费用：
   1) 预防性及纠正性维修的费用；
   2) 由诊断系统防止间接损坏所节省的费用；
   3) 根据培训水平所考虑的自动化程度；
   4) 预计的设备寿命。
d) 增加运营收益的方法：
   1) 改善处理特性；
   2) 提高可用性，例如故障的快速诊断和修理或利用冗余；
   3) 提高利用率。
e) 其他因素：
   1) 改进的潜力；
   2) 附加硬件、软件的技术和费用对设备安全性、可靠性的影响；
   3) 识别瞬态及间歇失效的能力；
   4) 诊断系统的恢复能力、复位能力；
   5) 采用 BITE 与采用外部测试设备相比的费效增益；
   6) 采用 COTS。

6 开发过程中的测试性

6.1 概要

只要产品运行的所有要求都已制定，就可以开始开发产品了。

产品的成功开发主要是基于对如何进行开发的统一描述。这为相关的需求提供了一个共识，这些需求涉及产品开发、升级和改造。这同样适用于其他附属行为，如质量保证，配置管理和技术项目管理。



说明：

SR ——系统需求；

TS ——测试技术规范；

TR ——测试记录；

PL ——部件清单；

HW——硬件架构；

FM ——功能模型；

M ——节点；

CE ——并行工程。

图 3 V 模型中的开发过程

研发可测试产品时，需要规定三个标志性阶段：

——M1：确认需求并由承包方开始开发；

——M2：通过分析验证对产品测试性进行理论证明；

——M3：通过测试验证对产品测试性进行实际演示。

图 3 表明了在 V 模型中它们是如何和开发过程相关联的。

要开发具有可测试性的产品需要以下步骤：

——检查需求的完整性，必要时要求客户提供任何可能遗漏的需求；

——通过需求分析制定规范；

——根据客户描述的设计水平确定产品；

——进行功能设计(功能/子功能并将其连接起来)；

——进行工程设计(即硬件分配)；

——进行故障识别，必要时进行优化；

——进行故障定位，必要时进行优化；

——准备验证；

——进行验证；

——文件验证。

一旦硬件单元在开发项目中确定，这些单元依照任务的明确描述开启一个新的更深层次设计水平

的开发过程。如果根据给定的硬件单元无法实现某些功能,便会开始一个迭代改进过程。此过程按照之前的标准制定出改进的规范,然后确定一个新的硬件单元。当所有的硬件单元都被确定,直到单独部件,则可以根据任务描述开始集成过程。

应用标准和附带的计算工具可使开发变得相对容易。

6.2 功能分配

测试性的开发过程需要产品中所有的功能和子功能都是可验证的。可通过对硬件单元和相关子功能分配足够的测试步骤来实现。

附录 B 中描述了一种适合于执行测试性要求的程序,它仅是一种基于功能模型的 FMEA 方法。

6.3 测试性工程

6.3.1 测试性设计准则

该工作单元的目的是为实现针对产品建立的诊断测试要求提供方法。这是设计过程中的维修性部分,这方面在 IEC 60300-3-10 和 IEC 60706-2 中均有涉及。基于此,应考虑以下测试性设计准则:

——划分出具有明确安排和清晰接口定义的功能组和功能单元,并尽可能使物理和电气划分与结构相协调以便于诊断、维修和后勤的优化调整。

——应优先采用功能、组件和设计元素,通过简单合适的诊断测试程序容易衡量和评估它们的状态和转换行为。

——测量规程应考虑到它们适用于维修并与已有或预定的外部设备适配,还应考虑测量设备的物理和电气的可达性。

——自测试程度应与 IEC 60300-3-10 中描述的修复分析级别(LORA)一致。

——应提供测试点并适当地标记,特别是需要外部测试设备的测试。

——在最终确定产品测试标准前,应严格定义失效定义和评分标准。

——初始化:系统或设备应设计成具有严格定义的初始状态以开始故障定位过程。一旦失效,初始化应能自动和反复地进行。

——执行测试规程和施加外部激励对零部件本身、相关设备或整个系统应无有害影响。

——所有总线系统都应具有测试可达性。

——在适用的场合下,应设计实用的诊断应用软件并编制相应的文档,以便于维修人员验证。

6.3.2 测试性设计

一旦决定了在硬件单元中实现何种功能,该硬件单元等级应达到产品的设计等级。它们的划分是有层次的(自上而下)。等级数取决于产品/系统复杂度及其技术设计。为简单化/标准化,从零部件到系统每个设计等级都进行分级(K1…Kn)。可能需要引入更高的系统等级,但仅接受连续编号(如系统4,系统 5 等)。

在工程设计过程中,将功能/子功能分配给硬件单元。此时,应考虑以下因素:

a) 最少的接口数(子功能是分离的情况)。

b) 功能组合(SF 与相关更高等级功能的联合)。

c) 只使用标准化接口(如,总线)。必要情况下,采用独立的测试总线。

测试性设计应结合系统寿命期间涉及的各个测试阶段,包括:

1) 生产阶段;

2) 贮存阶段;

3） 试运行阶段；

4） 运行阶段；

5） 运行后阶段；

6） 维修活动；

7） 报废阶段。

为取得一个经济的产品测试性方案，应该单独且综合地考虑每个测试阶段。还应考虑有些系统的多重作用或用于不同场景，会导致其实现不同功能单元的功能，而且对这些单元应采取类似的考虑。

6.3.3 商用现货(COTS)的使用

使用 COTS 的前提条件是它们符合 SoW 规定的要求，从而符合所有和运行范围有关的要求，包括：测试性、维修性和工作阶段需要的文件。在商用现货产品不符合 SoW 规定的测试性要求情况下，研发工程师应对系统补充缺少的测试性功能。

由于主承包方可能不是 COTS 供应方，因此双方需要通过协作进行评估。必需的测试是确保 COTS 符合为主承包方产品规定的运行及环境要求。还可能需要 COTS 供应方提供运行和环境的特性数据以及测试结果来证实声称的可靠性和维修性。除此之外，可能有必要要求供应商提供生产过程中不损害所设计的可靠性和维修性特性的证据，这个证据可能包括取样测试结果或给出在具有高水平加工能力控制下的关键过程控制图。

6.4 测试性研发过程

6.4.1 后勤支持

产品的计划维修支持应由客户在 SoW 中详细说明，以便研发工程师可以确定后勤支持(例如：更高优先级机内测试功能)的结果。如果将要开发的产品包括可更换的标准硬件单元如：灯、保险丝、滤波元件等，那么客户也应在 SoW 中确定后勤支持(见图 4 和表 4)。

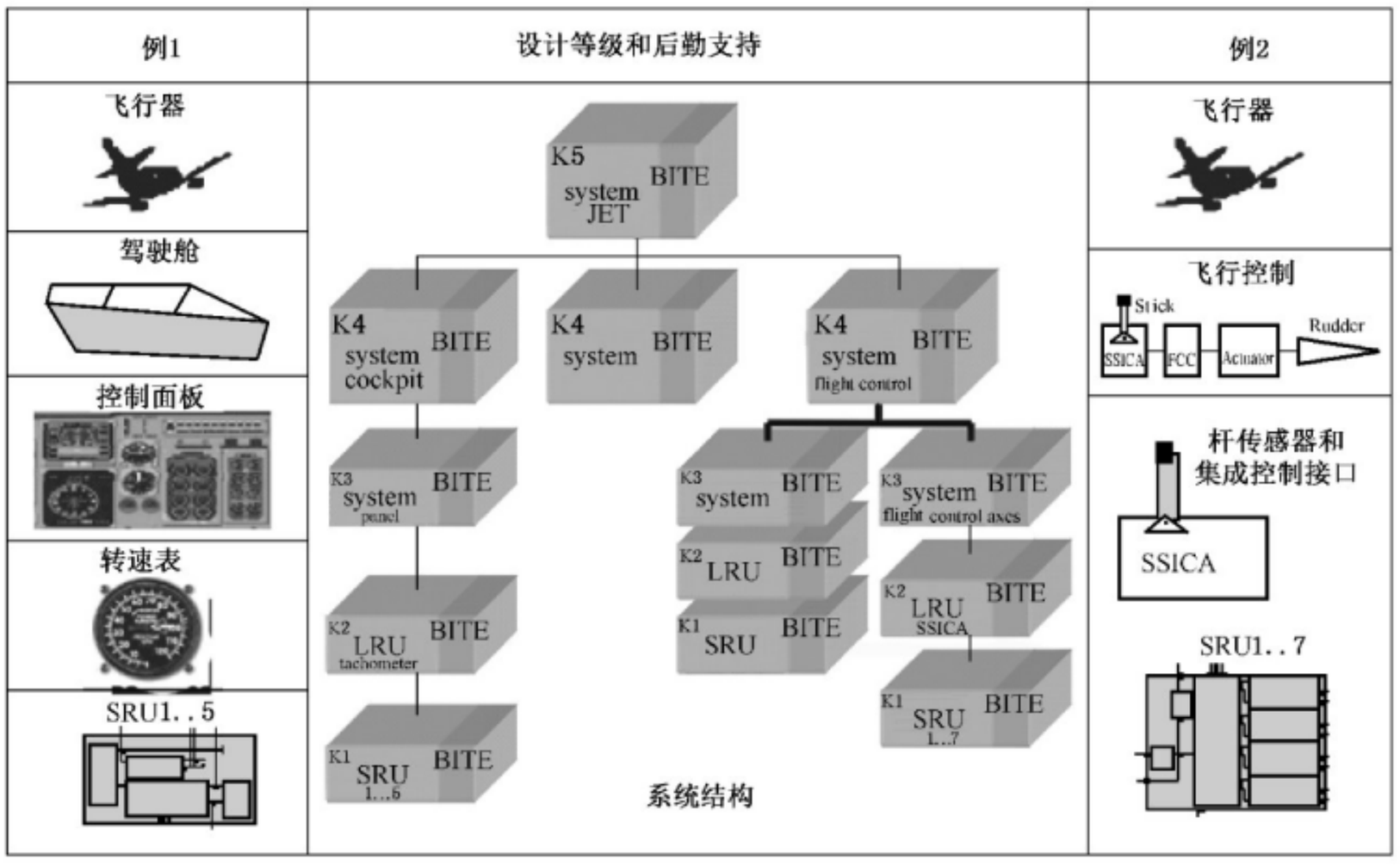


图 4 设计水平和后勤支持(以飞行器为例)

表 4　后勤支持示例

设计水平	后勤支持	示例
K5		飞行器
K4		驾驶舱,飞行控制系统
K3		控制面板,飞行控制轴
K2	现场可更换单元	转速表,杆传感器和接口控制组件
K1	内场可更换单元	插槽卡,PCB 板

6.4.2　可用性和诊断测试

在设计和开发阶段,根据相关的初期权衡研究的结果,应将测试性指标及特性包含到设计中。对诊断测试技术的专门考虑可以提高产品的维修性,减少不可用时间,从而提高可用性和利润并降低总体费用。

对存在固有耗损特性的产品,通过诊断测试过程可以明显减少预防性维修的费用,特别是可以优化维修间隔期、必要的预防性维修工作项目及资源。如果像大多数固态电子系统那样不存在耗损,则预防性维修的费用几乎可以忽略,而最大的费用影响因素是主费用,该项费用主要取决于达到的可用性。因为不可用时间的主要部分是故障识别和定位时间,将诊断重点放在这些要素上是最有效的。

7　测试性评估

7.1　概述

验证工作的目的是先运用理论再通过实际手段来证明诊断测试要求已得到满足。其方法和程序与维修性参数验证中所应用的很类似(IEC 60706-3)。所考虑的验证方案应包括下列内容:

——分析验证;

——测试验证。

7.2　分析验证

分析验证的要素有:

——文件评审:从完整性、准确性及易用性等方面对第 5 章中要求提供的文件进行评审;

——分析:该活动包含产品的分析研究及其测试性特征的评估,可按附录 B 进行评估。

7.3　测试验证

对产品硬件进行测试验证。如果 SoW 中要求测试验证,那么应在开发结果验收阶段进行,测试规范为验证提供了依据。通过对硬件单元的非破坏性干预,必要情况下,和/或软件模拟实现故障仿真,但这需要实际证据来支持。对非可测性功能,应为证实设计的适合性提供证据。

关于测试性验证的更多信息参考附录 B。

8　测试性文件

保证诊断方案的所有文件都以标准化的形式提供是重要的,以使相关信息有利于系统的运行和维护人员使用。文件的编制应考虑使用和维修的运行环境、维修方案、技能等级及所进行的培训程度。测试性文件的详细信息参考附录 B。

附 录 A
（资料性附录）
故障识别和故障定位的特性计算

A.1 符号

m 硬件单元的数量
n 端口的数量
h 运行过程的故障识别
k 测试条件下的故障识别
l 端口的故障定位
$v1$ 故障定位于一个硬件单元
$v2$ 故障定位于两个硬件单元之一
$v3$ 故障定位于三个硬件单元之一
A 运行中测试(在线测试)
B 在测试条件下的测试,无外部测试设备(离线测试)
C 在测试条件下的测试,有外部测试设备
D 预防性维修(维修性测试)

A.2 运行过程的故障识别

符号 h_i 表示在运行过程中端口 i 的故障可以识别。
$h_i=1$:运行过程中端口 i 可以故障识别;
$h_i=0$:运行过程中端口 i 不可以故障识别;
$\sum_{i-1}^{n} h_i$ =运行过程中可以识别故障的端口数量。
因此,运行过程中故障识别的特性表示如下:

$$FR_{(A)}=\frac{\sum_{i=1}^{n} h_i}{n}\times 100\%$$

A.3 测试条件下的故障识别

符号 k_i 表示在测试期间端口 i 的故障可以被识别。
$k_i=1$:在测试期间在端口 i 可以故障识别;
$k_i=0$:在测试期间在端口 i 不可以故障识别;
$\sum_{i=1}^{n} k_i$ =在测试期间故障可以被识别的端口数量。
因此,在测试期间故障识别的特性表示为:

$$FR_{(A+B+C+D)}=\frac{\sum_{i=1}^{n} k_i}{n}\times 100\%$$

记录最优的测试路径是测试部分 A 的一部分(在线测试)。

为了使费用的有效利用,考虑子功能的失效率(λ)有助于最优化在线测试期间故障识别的必要测试路径的数量。

FR=依据子功能失效率的故障识别(A 部分)

SF=子功能

P_{SFi}=子功能 i 的可测端口数

$\sum P_{SFi}$=子功能 i 的所有端口数

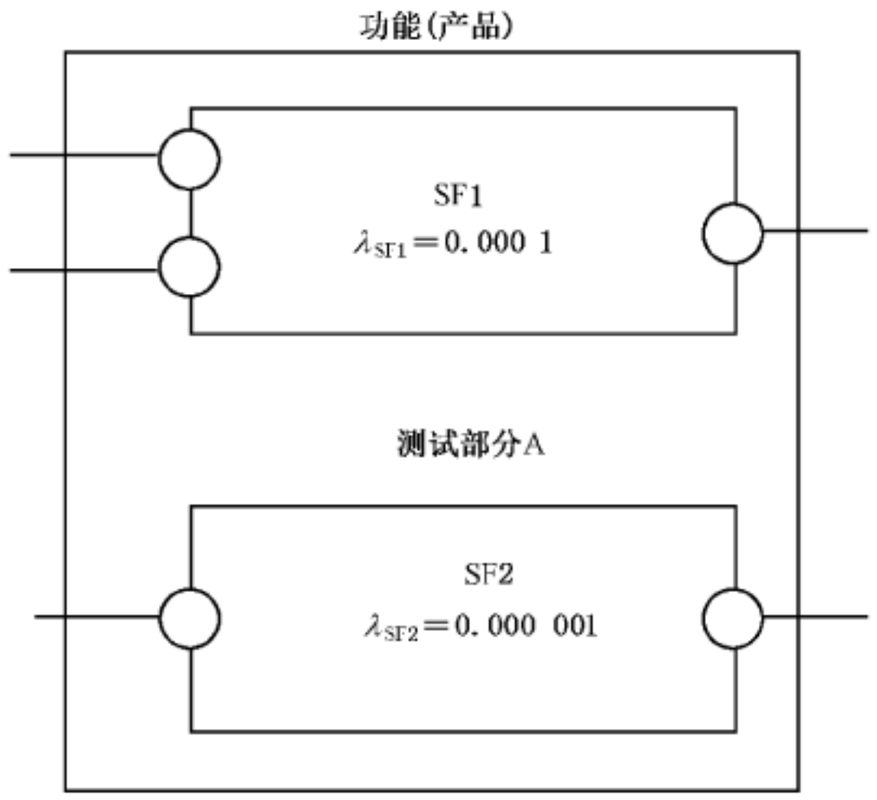
λ_{SFi}=子功能 i 的失效率

$\sum\lambda_{SFi}$=所有子功能的失效率总和

公式:

$$FR=\sum_{i=1}^{n}\frac{P_{SFi}}{\sum P_{SFi}}\times\frac{\lambda_{SFi}}{\sum\lambda_{SFi}}\leqslant 1$$

例如:



$P_{SF1}=3$ $\lambda_{SF1}=0.000\ 1$

$\sum P_{SF1}=3$ $\lambda_{SF2}=0.000\ 001$

$P_{SF2}=2$ $\sum\lambda_{SF}=0.000\ 101$

$\sum P_{SF2}=2$

$$FR=\left(\frac{3}{3}\right)\times\left(\frac{0.000\ 1}{0.000\ 101}\right)+\left(\frac{2}{2}\right)\times\left(\frac{0.000\ 001}{0.000\ 101}\right)\leqslant 1$$

$$FR=(1)\times(0.99)+(1)\times(0.009\ 9)\leqslant 1$$

FR=(0.99)×100%+(0.009 9)×100%

FR=(SF1)99%+(SF2)1%=100%

结果:

子功能 SF2 失效的概率大约为 1%。因此测试这个子功能可以转化为测试 B 或者 C 部分,从而最小化对 A 在线测试的测试耗费。

故障定位

符号 l_i 表示一个故障可以定位在端口 i。

$l_i=1$:故障定位在端口 i;

$l_i=0$:故障没有定位在端口 i;

$\sum_{i=1}^{n} l_i$ = 可以定位故障的端口数。

因此,在端口的故障定位的特性为

$$FL = \frac{\sum_{i=1}^{n} l_i}{n} \times 100\%$$

符号 $v1_j$ 表示一个故障可以被明确地定位在硬件单元 j 上。

$v1_j = 1$:在硬件单元 j 上明确地有故障定位;

$v1_j = 0$:在硬件单元 j 上明确地没有故障定位;

$\sum_{j=1}^{m} v1_j$ = 可以明确定位故障的硬件单元数。

因此,在一个硬件单元上的故障定位的特性为:

$$FL_{v1} = \frac{\sum_{j=1}^{m} v1_j}{m} \times 100\%$$

符号 $v2_j$ 表示一个故障可以被定位在两个硬件单元中的一个上,其中的一个硬件单元是单元 j。

$v2_j = 1$:故障定位在硬件单元 j 或者另外一个硬件单元上;

$v2_j = 0$:在硬件单元 j 和另外一个硬件单元上没有故障定位;

$\sum_{j=1}^{m} v2_j$ = 故障可以定位在两个硬件单元其中之一的情况数。

因此,故障定位在两个硬件单元的其中之一上的特性表示如下:

$$FL_{v2} = \frac{\sum_{j=1}^{m} v2_j}{m} \times 100\%$$

A.4 诊断正确率和测试识别比

A.4.1 符号

借助 5.4.3.1 的注释,下面的符号已被确定。值 A、B、C、D 是子集 A′、A″、B′、B″、C′、C″、D′和 D″的极限值。

A	运行中测试	(在线测试)
A′	产生正确诊断的在线测试	($\lim A' = A$)
A″	实际提供的在线测试	($\lim A'' = A$)
B	在测试条件下的测试,无外部测试设备	(离线测试)
B′	产生正确诊断的离线测试	($\lim B' = B$)
B″	实际提供的离线测试	($\lim B'' = B$)
C	在测试条件下的测试,有外部测试设备	(外部测试)
C′	产生正确诊断的外部测试	($\lim C' = C$)
C″	实际提供的外部测试	($\lim C'' = C$)
D	预防性维修	(维修测试)
D′	产生正确诊断的维修测试	($\lim D' = D$)
D″	实际提供的维修测试	($\lim D'' = D$)

其中 A 是 lim A′的值。

A.4.2 诊断正确率

根据测试性设计的基本原理，应有

$$A+B+C+D=100\%$$

（见 5.4.3.1），例如，所有可能的故障都在测试任务的 A、B、C、D 四部分的其中之一被诊断。正确诊断部分用如下公式表示：

$$A'+B'+C'+D'\leqslant 100\%$$

因此，诊断正确率 D_c 可以用比率表示为

$$D_c=\frac{A'+B'+C'+D'}{A+B+C+D}\leqslant 1$$

A.4.3 测试识别比

在测试任务的 A、B、C、D 任一部分中能被识别出的故障，用如下公式表示：

$$A''+B''+C''+D''\leqslant 100\%$$

因此，测试识别比 T_c 可以用比率表示为

$$T_c=\frac{A''+B''+C''+D''}{A+B+C+D}\leqslant 1$$

附 录 B
（资料性附录）
可测产品的开发步骤

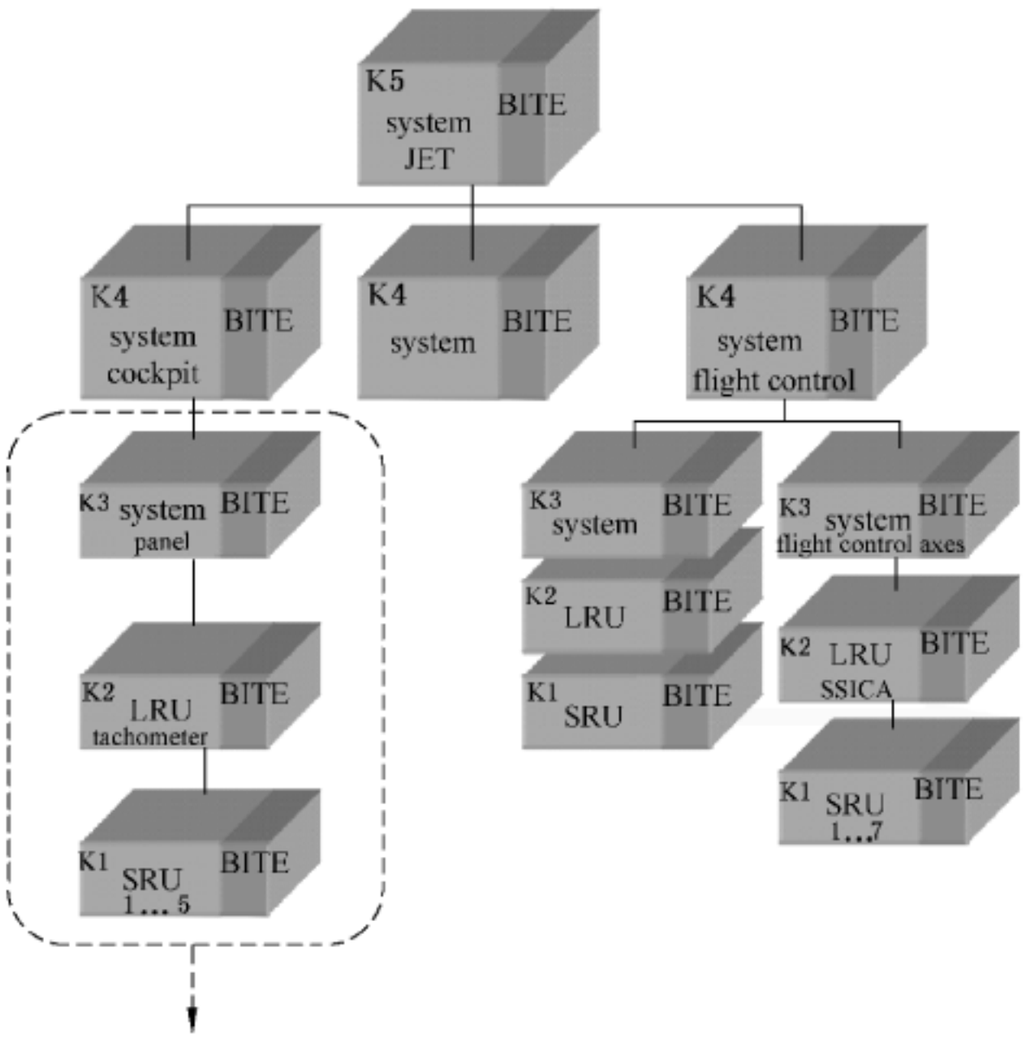
B.1 需求分析

B.1.1 SoW 的需求分析

利用本部分中给出的导则，分析 SoW 中所包含的需求，以确定它们是完整的，明确的。
对于那些表达不明确的需求，应该咨询顾客，并在 SoW 中重新精确地描述。
一旦客户和承包方达成一致并接受 SoW，在此基础上签订该合同。

B.1.2 将要开发产品的分类

以接受的 SoW 为基础（见图 B.1），决定将要开发产品的基本数据（名称、产品号、版本、设计等级）。
基于 SoW 需求确定将要开发产品的设计等级（例如设计等级 K4）。
来自 SoW，用于可更换硬件单元的后勤配置（LRU/SRU）。



产品基本数据		
产品号：样品	分类号：12345678	版本：01
设计等级：K3 系统		

图 B.1 确定基本数据的示例

基本数据已被确定。

B.2 功能设计

B.2.1 列出功能和子功能

在开发开始阶段,生成一个符合需求功能的产品功能细目分类,该需求功能是基于已接受的 SoW。

列出源于 SoW 的功能表。

将这些功能分解为独立的、可在所涉及的等级(见表 B.1)范围内实现的子功能。

规则:列出将进行开发的所有子功能(SF)。

表 B.1 “系统规范”文件的数据

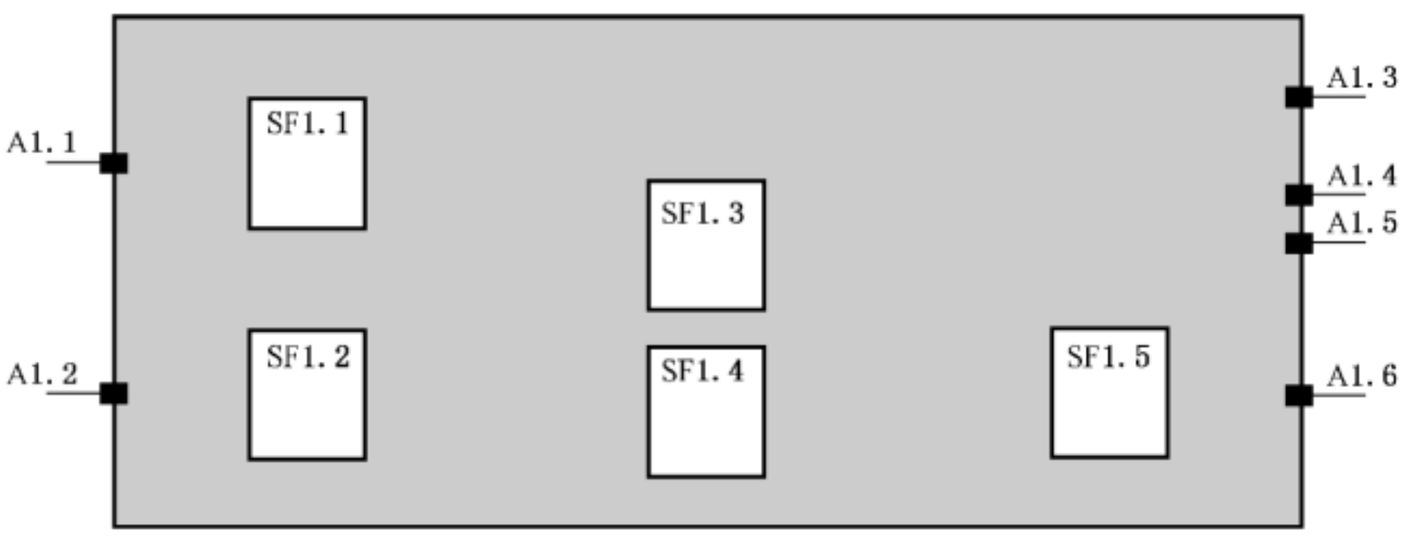
产品号:样品 分类号:12345678 版本:01

设计等级:K3 系统

功能	子功能
功能 1	SF1.1 SF1.2 SF1.3 SF1.4 SF1.5
功能 2	在示例中未涉及
功能 3	在示例中未涉及

B.2.2 功能和端口的建模

利用“系统规范”文件中的数据进行产品子功能和端口的建模(见图 B.2)。



说明:

A1.1 ——端口 1.1;

SF1.1——子功能 1.1。

图 B.2 子功能和端口的模拟

为了精确定义功能模型,通过规定功能链将已确定的子功能相互连接起来(见图 B.3)。

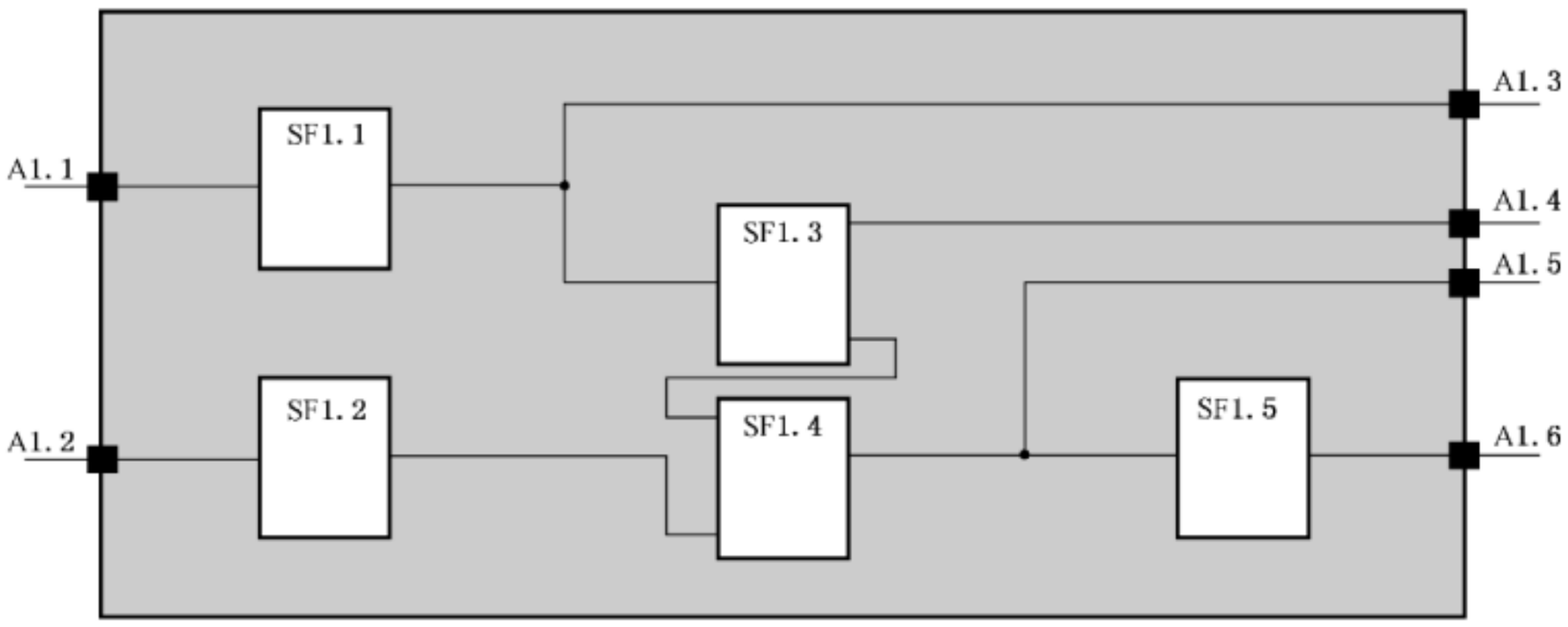


图 B.3　表示子功能间功能端口的功能模型

准则:功能模型表示出子功能的前后功能关系。

功能模型是子功能和端口的分配。

B.2.3　与功能相关参数的确定

B.2.3.1　“系统规范”文件的数据

利用“系统说明”文件中的数据来确定所有子功能(SF)的参数。这些参数可以定量地描述子功能(可在子功能端口测量)并且提供子功能已经实现的证据。

根据将起作用的参数可确定相应的端口(子功能端口)。

而后,在研究的等级限定下,根据起作用的子功能参数确定相应的端口。

测试说明中说明配置给子功能的参数。

规则:每一个子功能应由至少一个或者多个参数决定。

表 B.2　“测试规范”文件的数据(参数的功能分配)

产品号:样品　分类号:12345678　版本:01

设计等级:K3 系统

功能	子功能	激励参数	激励端口	测量参数	测量端口
功能 1	SF1.1	Stim 1.1	A1.1	Meas 1.1	A1.3
		Stim 1.2	A1.1	Meas 1.2	A1.3
		Stim 1.3	A1.1	Meas 1.3	A1.3
	SF1.2			Meas 2.1	
	SF1.3	Stim 1.4	A1.1	Meas 3.1	A1.4
	SF1.4	Stim 1.5	A1.2	Meas 4.1	A1.5
		Stim 1.5	A1.2	Meas 4.2	A1.5
	SF1.5	Stim 1.6	A1.2	Meas 5.1	A1.6

激励/测量参数见图 B.5。

B.3 工程设计

B.3.1 功能模型、系统规范

一旦产品的功能结构已经完成，对于将实现功能的硬件可用下面的步骤检验：

——通过系统规范中后勤和组织的要求，确定产品细目分类的结构；

——确定用设计元素（硬件单元）表示的产品功能/子功能的分解；

——选出应该容易替换（与后勤有关的约束条件）的硬件单元；

——插入已确定的硬件单元来确认功能模型；

——从由子功能和硬件单元限制条件组成的子功能链集合中取得各自的端口。

在功能模型中给出硬件零部件端口的标号（例如 A1.5：图 B.4 中的端口 5）。

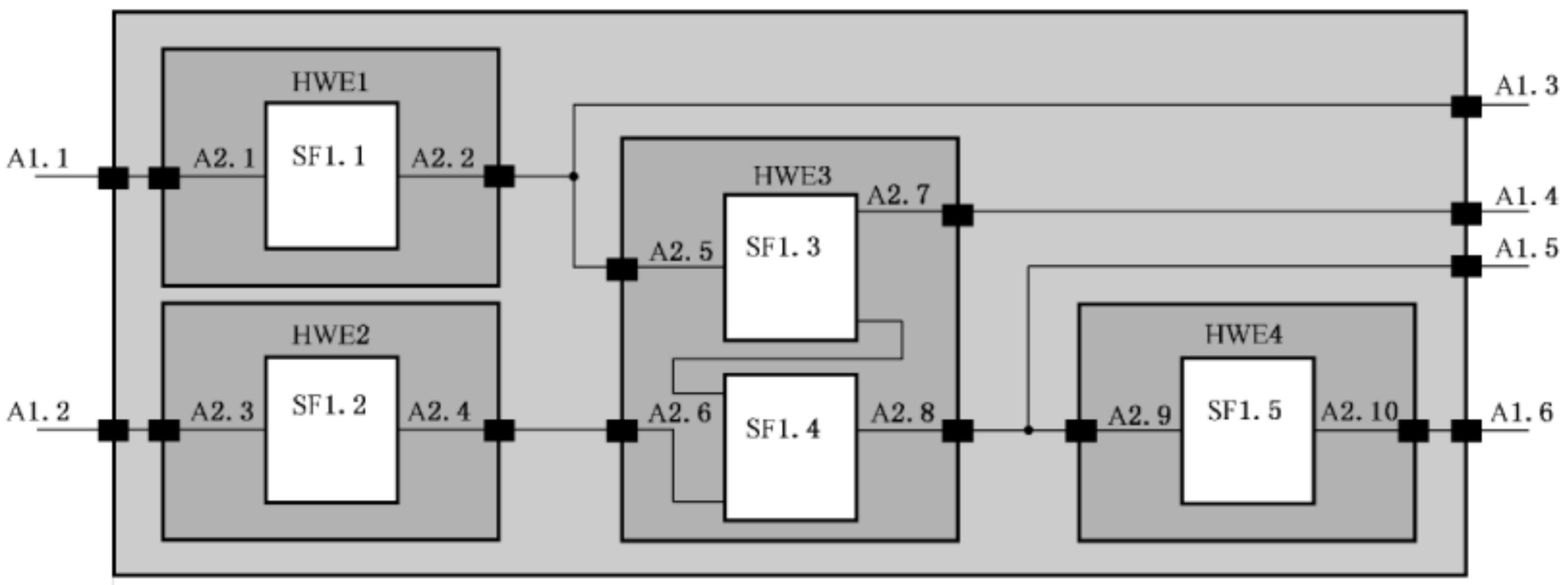


图 B.4 加入硬件零件的功能模型

将已定义的硬件单元分配到一个与系统规范中的后勤要求相符合的后勤等级（LRU、SRU）中。

表 B.3 加入硬件单元和后勤配置的数据表

产品号：样品　分类号：12345678　版本：01
设计等级：K3 系统

功能	子功能	硬件单元	后勤支持	激励参数	激励端口	测量参数	测量端口
功能 1	SF1.1	1	LRU	Stim 1.1	A1.1	Meas 1.1	A1.3
				Stim 1.2	A1.1	Meas 1.2	A1.3
				Stim 1.3	A1.1	Meas 1.3	A1.3
	SF1.2	2	LRU			Meas 2.1	
	SF1.3	3	LRU	Stim 1.4	A1.1	Meas 3.1	A1.4
	SF1.4	3	LRU	Stim 1.5	A1.2	Meas 4.1	A1.5
				Stim 1.5	A1.2	Meas 4.2	A1.5
	SF1.5	4	LRU	Stim 1.6	A1.2	Meas 5.1	A1.6

B.4 测试性的开发

B.4.1 测试步骤的确定

为了研发所需的测试性,需要确认子功能的参数。

为测试某个参数,需要执行测试步骤。

对于有一个或几个输入(同时地),在输出端为每个参数分配测试步骤。

在一个测试步骤中,在功能输入端施加一个特定的激励参数,在输出端进行测量并对参数进行验证。

将测试步骤明确地编号。

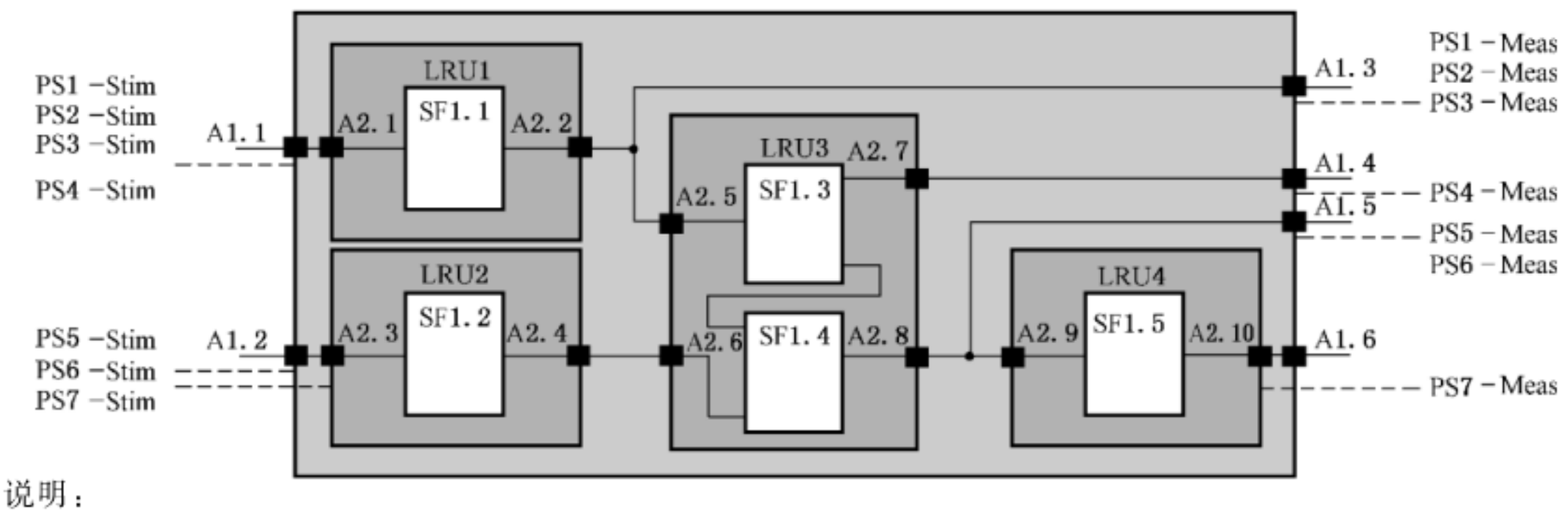
规则:一个测试步骤应分配到每一个具有在测试中受等级限制的端口的参数上。

表 B.4 包括测试步骤的数据表

产品号:样品 分类号:12345678 版本:01
设计等级:K3 系统

功能	子功能	硬件单元	后勤支持	测试步骤	激励参数	激励端口	测量参数	测量端口
功能 1	SF1.1	1	LRU	PS1	Stim 1.1	A1.1	Meas 1.1	A1.3
				PS2	Stim 1.2	A1.1	Meas 1.2	A1.3
				PS3	Stim 1.3	A1.1	Meas 1.3	A1.3
	SF1.2	2	LRU				Meas 2.1	
	SF1.3	3	LRU	PS4	Stim 1.4	A1.1	Meas 3.1	A1.4
	SF1.4	3	LRU	PS5	Stim 1.5	A1.2	Meas 4.1	A1.5
				PS6	Stim 1.5	A1.2	Meas 4.2	A1.5
	SF1.5	4	LRU	PS7	Stim 1.6	A1.2	Meas 5.1	A1.6

有些参数在测试中受单元结构限制不能直接分配给测试步骤,这样的参数仅可以通过整体功能的其他测试步骤间接测量得到。在例子中所示,参数 Meas 2.1 是通过测试步骤 5～7 间接测量得到的。



说明:

A1.1 ——端口 1.1;

SF1.1 ——子功能 1.1;

PS1-Stim ——第一步测试的激励;

PS1-Meas——第一步测试的测量。

图 B.5 显示激励源和测量点的功能模型

B.4.2 测试路径的确定

所有的子功能均位于测试步骤的激励源和测量点之间，并且对相关测试路径的测试性能产生影响。

规则：应将一个测试路径分配到每一个测试步骤。

在相同的激励端口情况下，如果在同一端口上有多个需要验证的参数，几个必要的测试步骤可以合并到一个测试路径中（见表 B.5：测试步骤 1～3 被合并到测试步骤 1 中）。

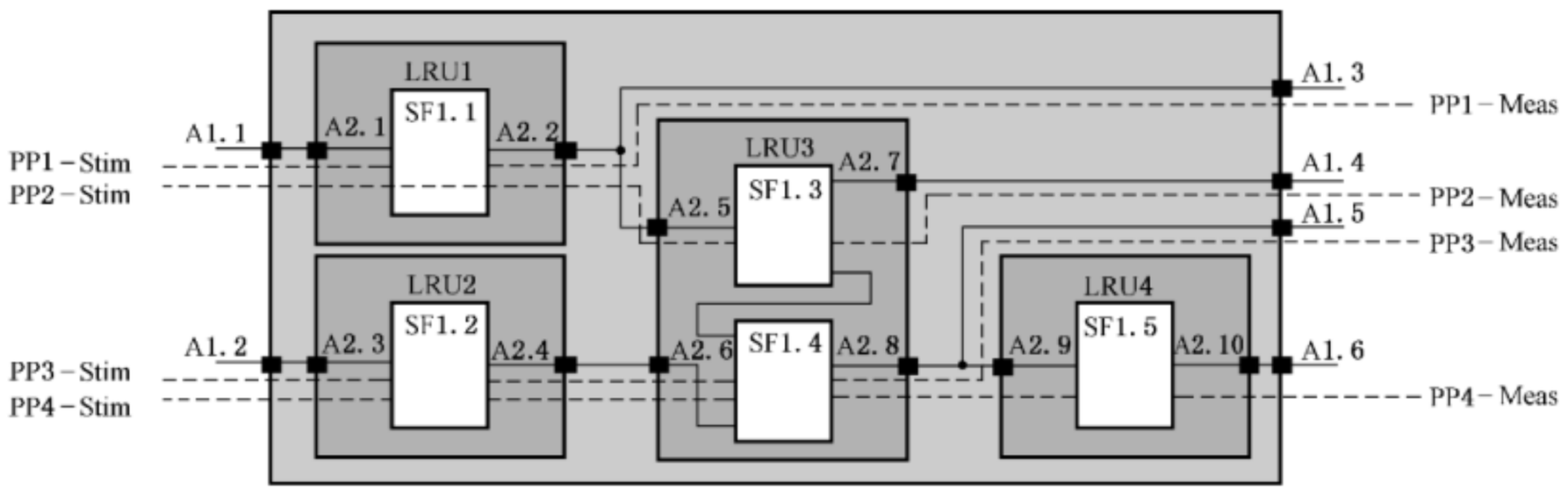
所有测试路径应明确地编号。

表 B.5 扩展包括测试路径的数据表

产品号：样品　分类号：12345678　版本：01

设计等级：K3 系统

功能	子功能	硬件单元	后勤支持	测试路径	测试步骤	激励参数	激励端口	测量参数	测量端口
功能 1	SF1.1	1	LRU	PP1	PS1	Stim 1.1	A1.1	Meas 1.1	A1.3
				PP1	PS2	Stim 1.2	A1.1	Meas 1.2	A1.3
				PP1	PS3	Stim 1.3	A1.1	Meas 1.3	A1.3
	SF1.2	2	LRU					Meas 2.1	
	SF1.3	3	LRU	PP2	PS4	Stim 1.4	A1.1	Meas 3.1	A1.4
	SF1.4	3	LRU	PP3	PS5	Stim 1.5	A1.2	Meas 4.1	A1.5
				PP3	PS6	Stim 1.5	A1.2	Meas 4.2	A1.5
	SF1.5	4	LRU	PP4	PS7	Stim 1.6	A1.2	Meas 5.1	A1.6



说明：

A1.1　——端口 1.1；

SF1.1　——子功能 1.1；

PP1-Stim　——测试路径 1 的激励；

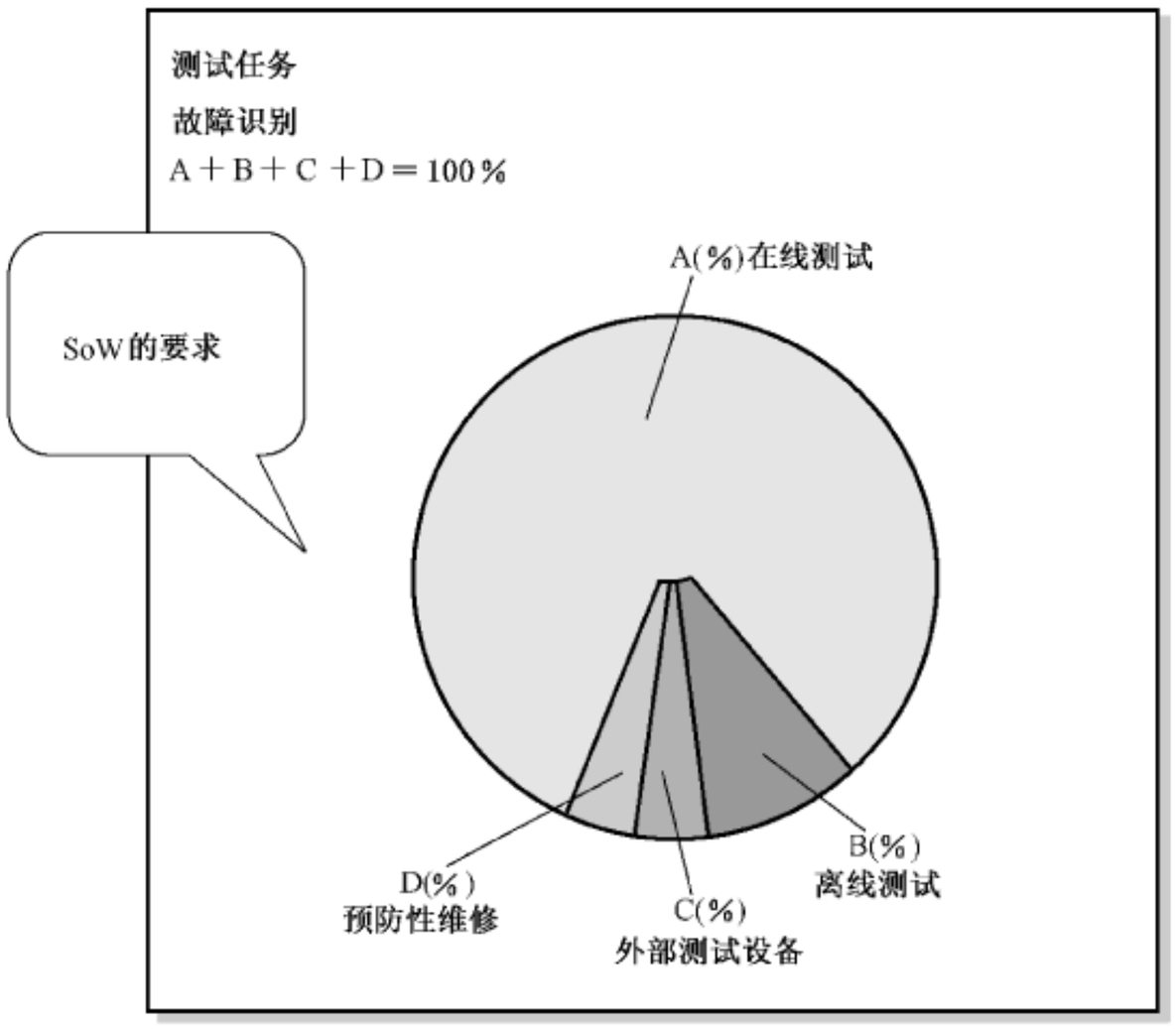
PP1-Meas　——测试路径 1 的测量。

图 B.6 显示测试路径的功能模型

在图 B.6 中，功能模型和数据表扩展到包括了测试路径。

B.4.3 测试任务各部分的分配

用图 B.7 所示的测试方法实现故障识别。



说明：

A 部分(％)——运行过程的测试(在线测试)；

B 部分(％)——在测试条件下无外部测试设备的测试(离线测试)；

C 部分(％)——在测试条件下有外部测试设备的测试；

D 部分(％)——预防性维修(硬件单元的预防性更换)。

图 B.7　测试任务

各独立的测试路径被分配到以功能模型为基础的相应部分(A、B、C、D)，并且将各路径加进数据表中(见表 B.6)。

表 B.6　扩展为包括测试任务各部分的数据表

产品号：样品　分类号：12345678　版本：01 设计等级：K3 系统										
功能	子功能	硬件单元	后勤支持	测试路径	测试步骤	测试任务部分	激励参数	激励端口	测量参数	测量端口
功能 1	SF1.1	1	LRU	PP1	PS1	Section B	Stim 1.1	A1.1	Meas 1.1	A1.3
				PP1	PS2	Section B	Stim 1.2	A1.1	Meas 1.2	A1.3
				PP1	PS3	Section B	Stim 1.3	A1.1	Meas 1.3	A1.3
	SF1.2	2	LRU						Meas 2.1	
	SF1.3	3	LRU	PP2	PS4	Section A	Stim 1.4	A1.1	Meas 3.1	A1.4
	SF1.4	3	LRU	PP3	PS5	Section C	Stim 1.5	A1.2	Meas 4.1	A1.5
				PP3	PS6	Section C	Stim 1.5	A1.2	Meas 4.2	A1.5
	SF1.5	4	LRU	PP4	PS7	Section A	Stim 1.6	A1.2	Meas 5.1	A1.6

在表 B.6 中，测试规范中的数据被扩展到包括测试任务部分。

B.5 故障识别的评估

B.5.1 故障识别率计算的方法

加入更多的项目栏以扩展数据表。

这些项目栏包含所有硬件单元端口的标号。

确定端口和硬件单元的数量并把这个数量加入到相应的总数栏中(见表 B.7 中 10 个端口和 4 个硬件单元)。

表 B.7 确定端口和硬件单元的数量

硬件单元端口	LRU1	LRU2	LRU3	LRU4	Σ 端口	Σ 硬件单元
	2.1 2.2	2.3 2.4	2.5 2.6 2.7 2.8	2.9 2.10	10	4

对于每一个测试路径,将这个路径所覆盖的端口标上“×”。

在一个测试路径中,对那些涉及超过一次的测试步骤,仅考虑一次。

表 B.8 显示端口和路径关系的矩阵

硬件单元端口			LRU1		LRU2		LRU3				LRU4		Σ 端口	Σ 硬件单元
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4
	测试步骤	测试路径												
	PS1	PP1	×	×	—	—	—	—	—	—	—	—		
	PS2													
	PS3													
	PS4	PP2	×	×	—	—	×	—	×	—	—	—		
	PS5													
	PS6	PP3	—	—	×	×	—	×	—	×	—	—		
	PS7	PP4	—	—	×	×	—	×	—	×	×	×		

B.5.2 运行过程中故障识别(FR)性能的特征值

在数据表中,确定所有的测试路径是从测试工作的“运行过程测试”部分“A”获得入口(见表 B.6)。这些测试路径有助于在线测试。

利用这部分数据,确定运行过程中故障识别性能的特征值。

要检查每个端口至少被一条测试路径覆盖。如果在一个特定端口的项目栏中至少有一个“×”,则在“通过 A 可识别的故障?”一行中给这个端口填上“1”。

例如:测试路径 2(PP2)通过端口 A2.5(见表 B.9)。由于测试路径 2 经过端口 A2.5,所以在这个端

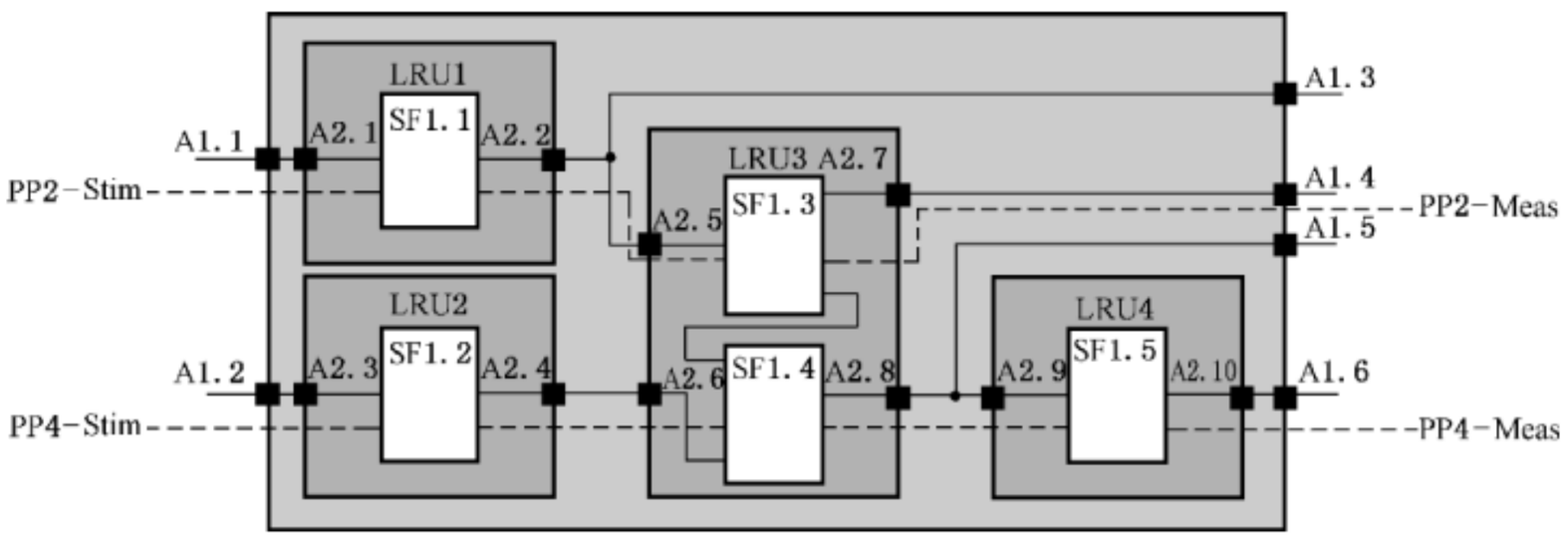
口发生的故障可以识别。

将所有可识别故障的端口数填入总数栏中。

表 B.9　运行过程(A)故障识别性能特征值的确定

硬件单元 端口			LRU1		LRU2		LRU3				LRU4		Σ 端口	Σ 硬件单元	特征值
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$
	测试 步骤	测试 路径													
	PS1 PS2 PS3	PP1	×	×	—	—	—	—	—	—	—	—			
	PS4 PS5	PP2	×	×	—	—	×	—	×	—	—	—			
	PS6	PP3	—	—	×	×	—	×	—	×	—	—			
	PS7	PP4	—	—	×	×	—	×	—	×	×	×			
经过 A 的故障可识别吗			1	1	1	1	1	1	1	1	1	1	10		100%

从已加入所有测试路径的功能模型中，提取出那些被分配到测试工作的“运行过程测试”部分(“A”)的所有路径(见图 B.8)。



说明：

A1.1　　——端口 1.1；

SF1.1　　——子功能 1.1；

PP2-Stim ——测试路径 2 的激励；

PP2-Meas——测试路径 2 的测量。

图 B.8　显示 A 的测试路径的功能模型

运行过程中故障识别性能的特征值 $FR_{(A)}$ 由子功能和/或已选测试路径经过端口与实际端口的比决定(见下面公式)。

$$FR_{(A)}=\frac{\text{A 的测试路径通过的子功能终端的数量}}{\text{子功能的实际终端的数量}}\times 100\%$$

将已确定的特征值记录在数据表中。

例:部分 A 测试路径(PP2 和 PP4)经过适于子功能 SF1.1～SF1.5 的端口 A2.1～A2.10。

$$FR_{(A)}=\frac{\text{测试路径通过的子功能的 10 个终端}}{\text{子功能的 10 个实际的终端}}\times 100\%=100\%$$

B.5.3 测试条件下的故障识别(FR)性能的特征值

在测试条件下,所有部分测试任务(部分 A+B+C+D)可以用于故障识别。

利用这个数据的数量,确定测试条件下故障识别的特征值。

要检查每个端口至少被一条测试路径覆盖。如果在一个特定端口的项目栏中至少有一个“×”,则在“经过 A+B+C+D 部分的故障可识别吗?”行中给这个端口填上“1”。

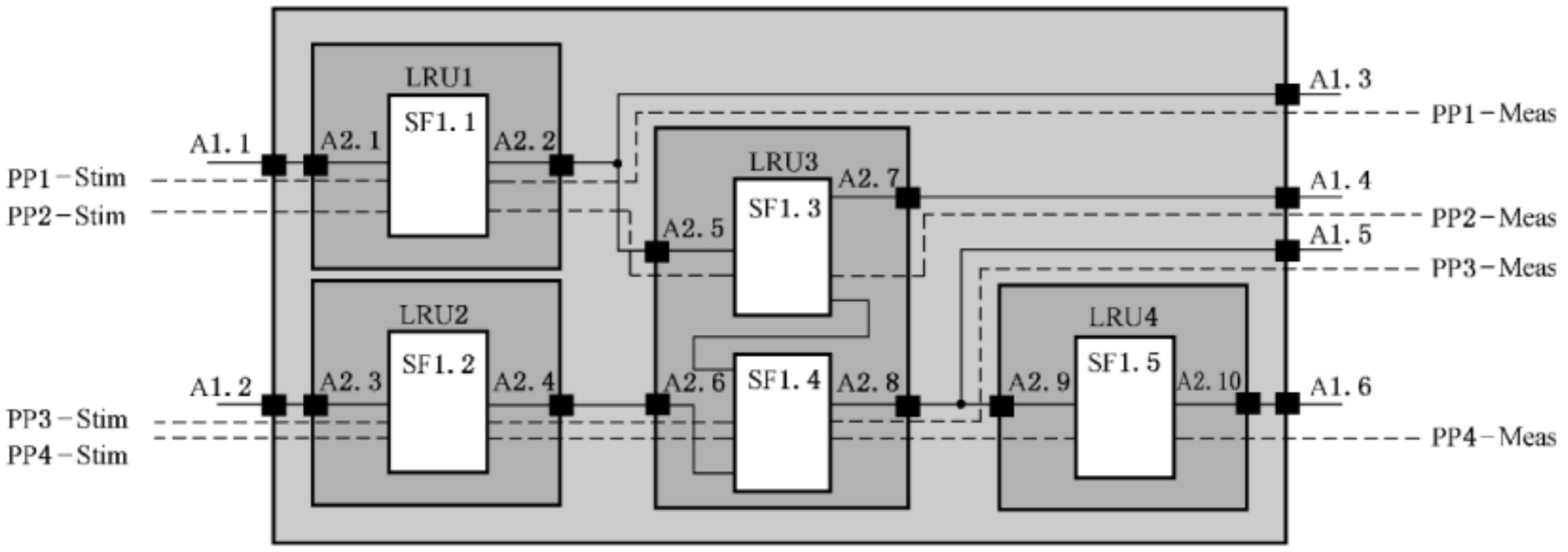
例如:测试路径 2(PP2)通过端口 A2.5(见表 B.10)。由于测试路径 2 经过端口 A2.5,所以在这个端口发生的故障可以被识别。

将所有可识别故障的端口数填入总数栏中。

表 B.10 测试条件下(A+B+C+D)故障识别(FR)性能特征值的确定

硬件单元 端口			LRU1		LRU2		LRU3				LRU4		Σ 端口	Σ 硬件 单元	特征值	
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$
	测试 步骤	测试 路径														
	PS1 PS2 PS3	PP1	×	×	—	—	—	—	—	—	—	—				
	PS4 PS5	PP2	×	×	—	—	×	—	×	—	—	—				
	PS6	PP3	—	—	×	×	—	×	—	×	—	—				
	PS7	PP4	—	—	×	×	—	×	—	×	×	×				
经过 A 部分的故障可识别吗			1	1	1	1	1	1	1	1	1	1	10		100%	
经过 A+B+C+D 的故障可识别吗			1	1	1	1	1	1	1	1	1	1	10			100%

将所有的测试路径加入到功能模型中。



说明：

A1.1 ——端口 1.1；

SF1.1 ——子功能 1.1；

PP1-Stim ——测试路径 1 的激励源；

PP1-Meas ——测试路径 1 的测量结果。

图 B.9 显示 A+B+C+D 部分测试路径的功能模型

在测试条件下故障识别(FR)性能的特征值由测试路径经过的端口与实际端口的比决定(见下面公式)。

$$FR_{(A+B+C+D)}=\frac{\text{A+B+C+D 部分中测试路径经过的子功能终端数量}}{\text{实际的子功能终端}}\times 100\%$$

将已确定的特征值记录在数据表中。

例：A+B+C+D 的测试路径通过适于子功能 SF1.1～SF1.5 的端口 A2.1～A2.10(PP1～PP4)。

$$FR_{(A+B+C+D)}=\frac{\text{测试路径的 10 个子功能终端}}{\text{10 个实际的子功能终端}}\times 100\%=100\%$$

B.6 故障定位评估

B.6.1 故障定位的计算方法

故障定位评估根据下面的覆盖矩阵实现(见表 B.11)。

表 B.11　覆盖矩阵

硬件单元			LRU1		LRU2		LRU3				LRU4		Σ	Σ	特征值		
端口			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	端口 10	硬件单元 4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	
	测试步骤	测试路径															
	PS1	PP1	×	×	—	—	—	—	—	—	—	—					2^0
	PS2																
	PS3																
	PS4	PP2	×	×	—	—	×	—	×	—	—	—					2^1
	PS5																
	PS6	PP3	—	—	×	×	—	×	—	×	—	—					2^2
	PS7	PP4	—	—	×	×	—	×	—	×	×	×					2^3
			3	3	12	12	2	12	2	12	8	8					

每行的测试路径被赋予 2^0 与 2^n 之间的二进制编码。

将表征端口的列表示为二进制码(“×”代表“1”;“—”代表“0”),并以十进制数填入编码行。

因此对于表 B.11 中的每一个端口可以计算出表 B.12 中的编码值。

表 B.12　端口编码

硬件单元	LRU1		LRU2		LRU3				LRU4	
端口	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10
编码	3	3	12	12	2	12	2	12	8	8

表征硬件单元端口列的编码用来核对所有剩余硬件单元的编码。

如果当前考虑的端口编码只出现一次,则在该端口的“可准确定位?”一行填入“1”。

例如:将端口 A2.5 的编码(2)和其他硬件单元端口的编码比较,如硬件单元 1 的端口编码(3 和 3),硬件单元 2 的端口编码(12 和 12)及硬件单元 4 的端口编码(8 和 8)。由于端口 A2.5 的编码仅出现一次,因此如果发生故障,该端口可以被准确定位。

将可准确定位的端口总数输入总数域(见表 B.13)。

表 B.13　总数域

编码	3	3	12	12	2	12	2	12	8	8				
可准确定位吗	1	1	—	—	1	—	1	—	1	1	6			
可准确定位的硬件单元 $FL_{(L1)}$	1									1		2		

如果一个硬件单元的所有端口都可以定位，那么在各硬件单元的“可准确定位硬件单元”行中输入“1”。

例如：可以根据下面图 B.10 和图 B.11 的示例更明确地解释故障定位方法。

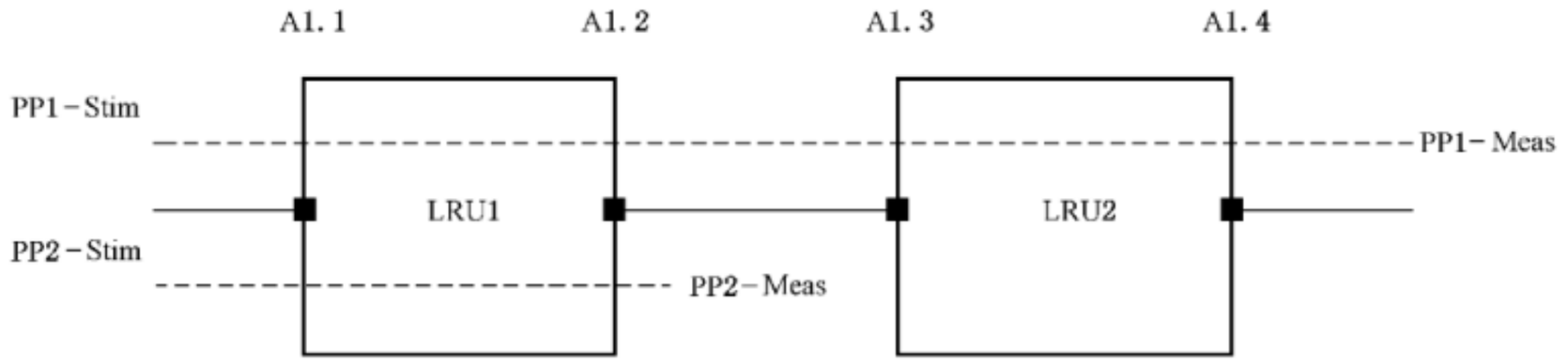


图 B.10　例 1 的功能模型

由这个功能模型得出下面的矩阵表 B.14。

表 B.14　例 1 的故障定位矩阵

	LRU1		LRU2		Σ 端口	Σ 硬件单元	特征值	
	A1.1	A1.2	A1.3	A1.4	4	2	FL	
PP1	×	×	×	×				2^0
PP2	×	×	—	—				2^1
编码	3	3	1	1				
可准确定位	1	1	1	1	4		100%	
可准确定位硬件单元		1		1		2	100%	
结合两个硬件单元可定位						0	0%	
结合 n 个硬件单元可定位						0	0%	

通过所选择的测试路径能保证对该端口准确地故障定位。

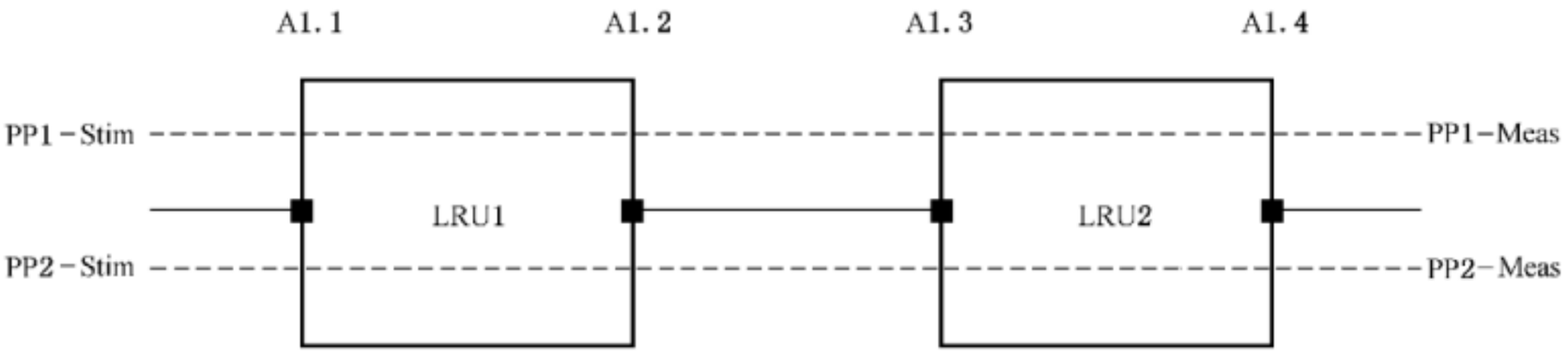


图 B.11　例 2 的功能模型

由该功能模型可得出下面的矩阵表 B.15。

表 B.15　例 2 的故障定位矩阵

	LRU1		LRU2		Σ 端口	Σ 硬件单元	特征值	
	A1.1	A1.2	A1.3	A1.4	4	2	FL	
PP1	×	×	×	×				2^0
PP2	×	×	×	×				2^1
编码	3	3	3	3				
可准确定位	—	—	—	—	0		0%	
可准确定位硬件单元	—		—			0	0%	
结合两个硬件单元可定位	1		1			2	100%	
结合 n 个硬件单元可定位						0	0%	

通过所选择的测试路径不能保证对该端口准确的故障定位。

B.6.2　故障定位性能的特征值

以上所证明的原则也适用于故障定位(FL)性能特征值的确定(见表 B.16)。

表 B.16　确定故障定位(FL)性能的特征值

硬件单元端口			LRU1		LRU2		LRU3				LRU4		Σ 端口	Σ 硬件单元	特征值			
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	FL	
	测试步骤	测试路径																
	PS1	PP1	×	×	—	—	—	—	—	—	—	—						2^0
	PS2																	
	PS3																	
	PS4	PP2	×	×	—	—	×	—	×	—	—	—						2^1
	PS5																	
	PS6	PP3	—	—	×	×	—	×	—	×	—	—						2^2
	PS7	PP4	—	—	×	×	—	×	—	×	×	×						2^3
译码			3	3	12	12	2	12	2	12	8	8						
可准确定位			1	1	—	—	1	—	1	—	1	1	6				60%	

故障定位(FL)性能的特征值取决于所有能被用于故障定位的端口数(定位行为“1”)与所有端口数的比率。

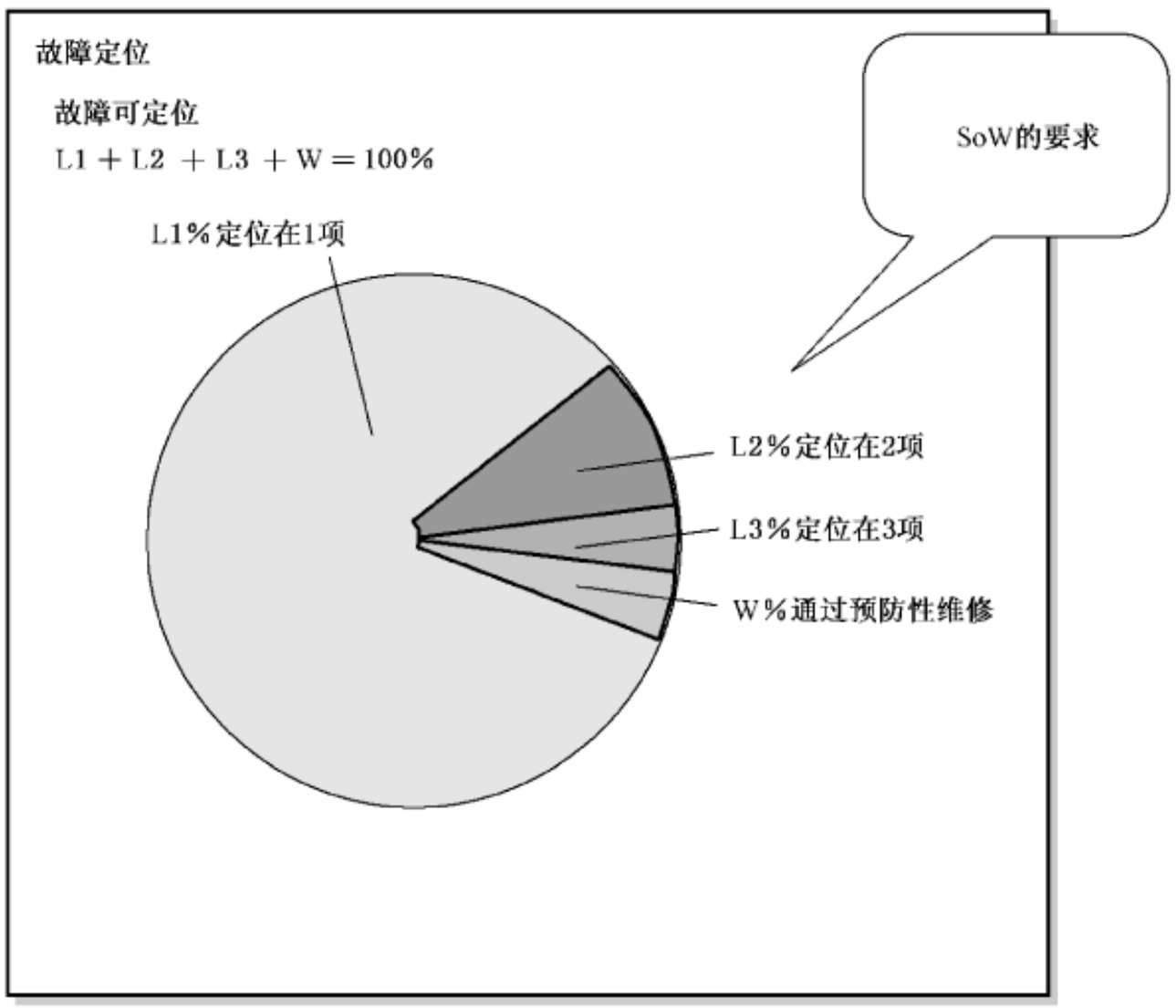
$$FL=\frac{可用于故障定位终端数}{子功能的所有终端数}\times 100\%$$

在本例中，FL=60%。

B.6.3 故障定位(硬件单元)与准确性之间的关系

可根据所有端口“可定位”行是否为“yes”，对每个硬件单元进行评估。

为确定允许硬件单元故障定位的不确定程度，应该以系统规范为准。



说明：

L1(%)——可准确定位硬件单元；

L2(%)——涉及 2 个硬件单元可定位；

L3(%)——涉及 3 个硬件单元可定位；

W(%)——预防性维修(硬件单元的预防性更换)。

图 B.12 故障定位比例

将适当数目的行(“可定位到 n 个硬件单元”的每种情况)增补到表 B.17。

在这个例子中，SoW 规定一个故障允许最多涉及三个硬件单元。

假如硬件单元的所有端口在“可定位”行中被给出“yes”的评估，那么在“一个硬件单元可以定位”行中输入“1”。

在每个“可定位”行输入为“no”的列中，该硬件单元与故障可能有关。

表 B.17　硬件单元可定位性的确定

硬件单元 端口			LRU1		LRU2		LRU3				LRU4		Σ 端口	Σ 硬件 单元	特征值			
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	FL	
	测试 步骤	测试 路径																
	PS1 PS2 PS3	PP1	×	×	—	—	—	—	—	—	—	—						2^0
	PS4 PS5	PP2	×	×	—	—	×	—	×	—	—	—						2^1
	PS6	PP3	—	—	×	×	—	×	—	×	—	—						2^2
	PS7	PP4	—	—	×	×	—	×	—	×	×	×						2^3
编码			3	3	12	12	2	12	2	12	8	8						
可准确定位			1	1	—	—	1	—	1	—	1	1	6				60%	
可准确定位硬件单元 $FL_{(L1)}$			1								1			2			50%	
涉及两个硬件单元可定位 $FL_{(L2)}$				1		1								2			50%	
涉及三个硬件单元可定位 $FL_{(L3)}$														—			0%	

一个、两个或三个硬件单元相对于测试情况下同一等级硬件单元总数的可识别性百分比分配可用下式计算。

$$FL_{HWE(Ln)}=\frac{\text{涉及 } n \text{ 个单元的可定位硬件单元数}}{\text{硬件单元总数}}\times 100\%$$

在本例中：

——$FL_{HWE(L1)}=50\%$；

——$FL_{HWE(L2)}=50\%$；

——$FL_{HWE(L3)}=0\%$；

——$FL_{HWE(W)}=0\%$。

B.6.4　提高故障定位性能特征值的方法

可以通过不同的措施改进故障定位：

- 为进行测试，通过引进额外的子功能和/或端口改变设计(参见图 B.13，端口 A1.7)；
- 通过规定适当的测试和仿真数据增加测试路径(参见表 B.18，测试路径 PP5)。

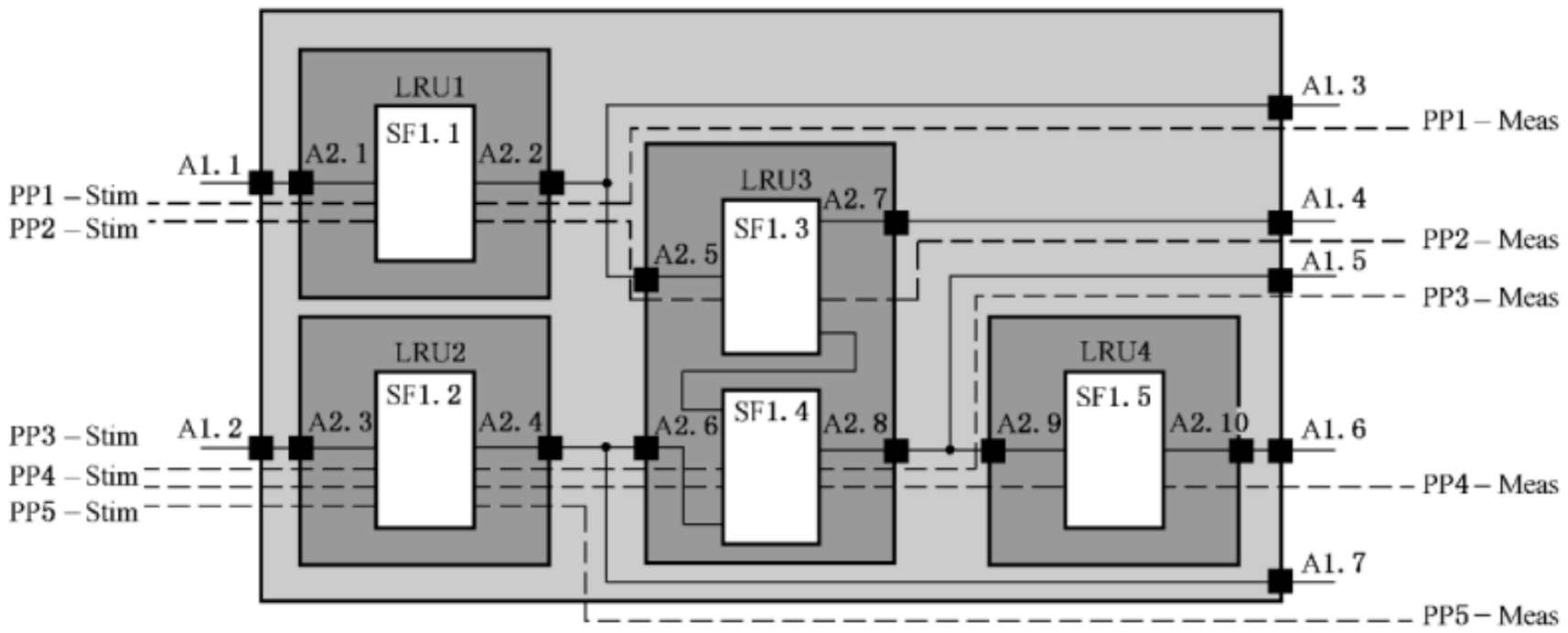


图 B.13　包含额外的激励和测量点的功能模型

表 B.18　扩充至包含测试路径 PP5 的数据表

名称:样本　　项目号:12345678　　版本:02 设计等级:K3 系统										
功能	子功能	硬件单元	后勤配置	测试路径	测试步骤	测试任务部分	激励参数	激励端口	测量参数	测量端口
功能 1	SF1.1	1	LRU	PP1	PS1	section B	Stim 1.1	A1.1	Meas 1.1	A1.3
				PP1	PS2	section B	Stim 1.2	A1.1	Meas 1.2	A1.3
				PP1	PS3	section B	Stim 1.3	A1.1	Meas 1.3	A1.3
	SF1.2	2	LRU	PP5	PS8	section C	Stim 1.7	A1.2	Meas 2.1	A1.7
	SF1.3	3	LRU	PP2	PS4	section A	Stim 1.4	A1.1	Meas 3.1	A1.4
	SF1.4		LRU	PP3	PS5	section C	Stim 1.5	A1.2	Meas 4.1	A1.5
				PP3	PS6	section C	Stim 1.5	A1.2	Meas 4.2	A1.5
	SF1.5		LRU	PP4	PS7	section A	Stim 1.6	A1.2	Meas 5.1	A1.6

表 B.19　硬件单元定位性的确定,包含增加的测试路径 5

硬件单元端口			LRU1		LRU2		LRU3				LRU4		Σ端口	Σ硬件单元	特征值			
			2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	2.10	10	4	$FR_{(A)}$	$FR_{(A+B+C+D)}$	FL	
	测试步骤	测试路径																
	PS1	PP1	×	×	—	—	—	—	—	—	—	—						2^0
	PS2																	
	PS3																	
	PS8	PP5	—	—	×	×	—	—	—	—	—	—						2^1
	PS4	PP2	×	×	—	—	×	—	×	—	—	—						
	PS5																	2^2
	PS6	PP3	—	—	×	×	—	×	—	×	—	—						2^3
	PS7	PP4	—	—	×	×	—	×	—	×	×	×						2^4
编码			5	5	26	26	4	24	4	24	16	16						
可准确定位吗			1	1	1	1	1	1	1	1	1	1	10				100%	
可准确定位的硬件单元 $FL_{(L1)}$			1		1		1				1			4			100%	
涉及两个硬件单元可定位 $FL_{(L2)}$														—			0%	
涉及三个硬件单元可定位 $FL_{(L3)}$														—			0%	

一个、两个或三个硬件单元相对于测试情况下同一等级硬件单元总数的可识别性百分比分配可用下式计算。

$$FL_{HWE(Ln)}=\frac{\text{涉及 } n \text{ 个单元的可定位硬件单元数}}{\text{硬件单元总数}}\times 100\%$$

在本例中:

——$FL_{HWE(L1)}=100\%$;

——$FL_{HWE(L2)}=0\%$;

——$FL_{HWE(L3)}=0\%$;

——$FL_{HWE(W)}=0\%$。

B.7　测试性验证

B.7.1　验证执行

承包方应当给出故障识别和定位已完成的指示证据。

由于测试性是系统必需的要求,因此应在开发验收测试阶段提供证据。

可以通过两种不同的方式提供验证:

——分析验证

通过在设计审查期间的理论分析，并采用和产品当前测试说明相关的可测性记录表来验证。可在产品寿命周期内的任何点反复进行验证，例如在生产中或者结合一些规范变化后等。

——测试验证

如果 SoW 需要产品硬件进行测试验证，那么将在开发结果的验收期间进行，并且由测试规范提供验证的基础。

假如预定值不能获得验证，那么将与客户商议进行矫正，或者修改合同。

B.7.2 验证方法

通过示范进行验证，根据下面的准则选择测试路径：

——任务重要度-包括相应的安全性-测试路径

这些路径是依据系统规范中的要求进行定义的。在所有现存的测试路径中，应对关系到任务重要度高的(例如，依据 FMECA)那些进行验证。对这些测试路径故障识别的实现是一个基本需求。

——基于失效的测试路径(Lambda)

为了验证，在 SoW 中客户需要多种与失效相关的测试路径，那么需要知道 LRU/SRU 的期望故障率。分配给 LRU 的产品失效率的细目分类由开发方定义，也可能以规范的形式由客户和/或开发商自己制定，这些依赖于失效率的评估。

——路径的随机选择

从没有被验证的测试路径中，选择并验证若干统计确定的路径。

在验证纪录中记下选择的测试路径。

以包含根据以上提供的标准选择出的测试路径的验证纪录为基础，为测试性提供证据。

通过在一个硬件单元上模拟故障提供验证，该硬件单元是相关测试路径覆盖的硬件单元之一。

表 B.20 验证记录

标号：样本　　项目码：12345678　　版本：01 设计等级：K3 系统									
功能	子功能	硬件单元	测试路径	测试步骤	1/MTBF λ	是否危急	是否仿真	标准	参数的偏差是否被识别
功能 1	SF1.1	LRU1	PP1	PS1 PS2 PS3	1/1 000		Yes	高 Lambda	
	SF1.2	LRU2			1/9 000				
	SF1.3	LRU3	PP2	PS4	1/2 500		No		
	SF1.4	LRU3	PP3	PS5 PS6	1/2 000		Yes	随机的	
	SF1.5	LRU4	PP4	PS7	1/1 500	Yes	Yes	致命故障	

作为结果，记录由参数偏差构成。假如确定了参数的偏差，那么这些文档中的测试路径要与在系统中实行的测试路径一致。

验证记录确保文档化的测试性与在系统中实行的相一致。不准许有偏离。

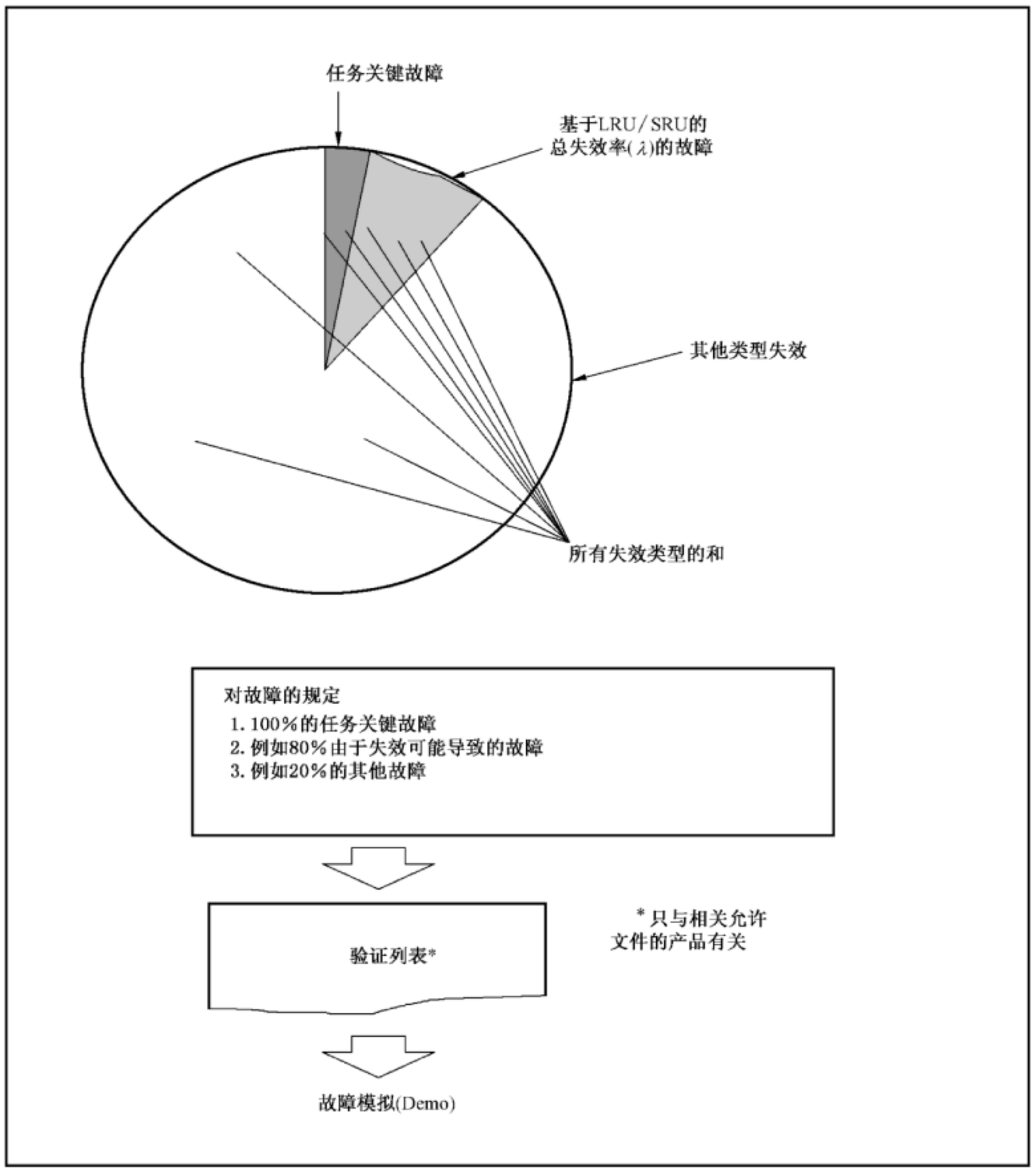


图 B.14　为验证选择标准

B.8　文件

B.8.1　概述

描述测试性的中心文件是功能模型。

功能模型中存储的所有信息基于文件系统规范、测试规范和扩展方框图，并在整个产品寿命周期内更新。

这些文件和功能模型应该存储在一个数据模块中，即所有的信息包应存储在一个公用的源数据库(CSDB)中，并能通过数据模块代码进行寻址。

B.8.2 系统规范(参见表 B.21 的例子)

“系统规范”文件包含将被实现的功能的书面描述。

表 B.21 “系统规范”的例子

标号:样本	项目码:12345678 设计等级:K3 系统	版本:01
功能	子功能	
功能 1	SF1.1 SF1.2 SF1.3 SF1.4 SF1.5	
功能 2	例子中未研究	
功能 3	例子中未研究	

B.8.3 测试规范

“测试规范”包含用于实现必需功能所需的参数。

表 B.22 “测试规范”的例子

标号:样本		项目码:12345678 设计等级:K3 系统		版本:01						
功能	子功能	硬件 单元	后勤 配置	测试 路径	测试 步骤	测试任务 部分	激励 参数	激励 端口	测量 参数	测量 端口
功能 1	SF1.1	1	LRU	PP1	PS1	Section B	Stim 1.1	A1.1	Meas 1.1	A1.3
				PP1	PS2	Section B	Stim 1.2	A1.1	Meas 1.2	A1.3
				PP1	PS3	Section B	Stim 1.3	A1.1	Meas 1.3	A1.3
	SF1.2	2	LRU						Meas 2.1	
	SF1.3	3	LRU	PP2	PS4	Section A	Stim 1.4	A1.1	Meas 3.1	A1.4
	SF1.4	3	LRU	PP3	PS5	Section C	Stim 1.5	A1.2	Meas 4.1	A1.5
				PP3	PS6	Section C	Stim 1.5	A1.2	Meas 4.2	A1.5
	SF1.5	4	LRU	PP4	PS7	Section A	Stim 1.6	A1.2	Meas 5.1	A1.6

B.8.4 扩展的框图(参见图 B.15)

这是一个包含测试路径的扩展框图。以明确的方式标识测试路径。为了展示特定测试路径的需要,可能使用几个相同的框图。

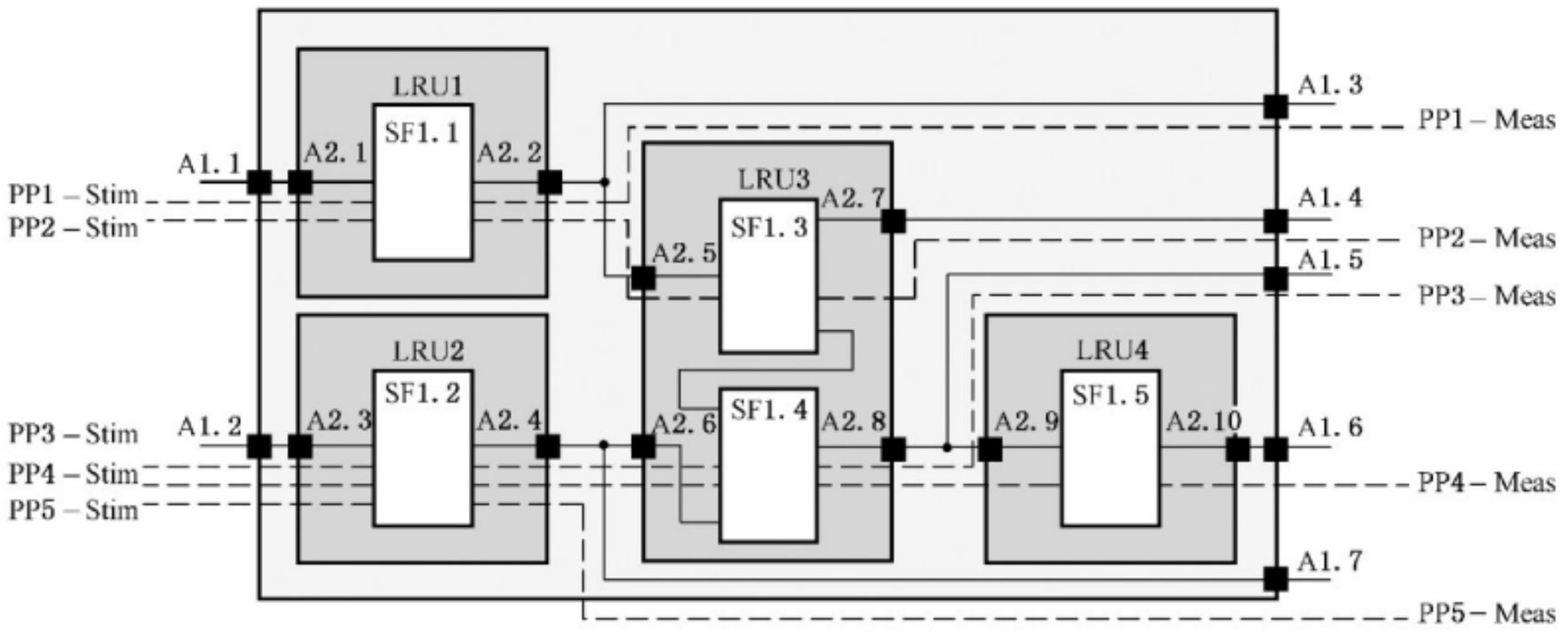


图 B.15 以扩展框图呈现的功能模块

完整的框图为诊断测试提供所有的基本信息。根据被测试系统的大小,诊断测试可以通过计算机和基于使用像表 B.22 这样的数据表的软件工具进行运行,而手工诊断测试将主要使用详尽的扩展框图。

B.8.5 验证记录

以包含将要验证的测试路径的验证记录为基础提供测试性证据。

验证记录包含如表 B.23 所示的信息。

表 B.23 验证记录

标号:样本	项目码:12345678	版本:01							
	设计等级:K3 系统								
功能	子功能	硬件单元	测试路径	测试步骤	1/MTBF λ	是否危急	是否仿真	标准	参数的偏差是否被识别
功能 1	SF1.1	LRU1	PP1	PS1	1/1 000		Yes	高 Lambda	
	SF1.2	LRU2		PS2	1/9 000				
	SF1.3	LRU3	PP2	PS3	1/2 500		No		
	SF1.4	LRU3	PP3	PS4	1/2 000		Yes	随机的	
				PS5					
				PS6					
	SF1.5	LRU4	PP4	PS7	1/1 500	Yes	Yes	致命故障	

验证在产品硬件上执行。如果 SoW 要求这种验证，那么将在开发结果的验收期（参见图 3 中的 M3）内执行。再次强调，测试规范将为验证提供依据。通过对硬件零件非破坏性的干预，必要时，和/或通过软件模拟进行仿真。

参 考 文 献

[1] IEC 60300-1:2003 Dependability management—Part 1:Dependability management systems

[2] IEC 60300-2:2004 Dependability management—Part 2:Guidelines for dependability management

[3] IEC 60300-3-2 Dependability management—Part 3-2:Application guide—Collection of dependability data from the field

[4] IEC 60300-3-3 Dependability management—Part 3-3:Application guide—Life cycle costing

[5] IEC 60300-3-11 Dependability management—Part 3-11:Application guide—Reliability centred maintenance

[6] IEC 60300-3-12 Dependability management—Part 3-12:Application guide—Integrated logistic support

[7] IEC 60300-3-14 Dependability management—Part 3-14:Application guide—Maintenance and maintenance support

中 华 人 民 共 和 国
国 家 标 准
维修性 第5部分：测试性和诊断测试
GB/T 9414.5—2018/IEC 60706-5：2007
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2018年6月第一版
*
书号：155066·1-60016

GB/T 9414.5-2018