指导性文件

GD28-2023

中 国 船 级 社

船舶设备与系统可靠性验证指南

2023

2023 年 7 月 1 日生效

北 京

目　录

前　言

根据中国船级社《智能船舶规范》的要求，智能航行系统的场景感知系统和自主航行系统的设备和部件应具有充分的可靠性，以最大程度降低故障发生的几率。近年来，随着国产配套设备不断发展，船舶智能化水平不断提高，低碳零碳战略下新能源的应用带动了新设备和系统层出不穷，业界对于船舶设备和系统的可靠性关注程度也逐步增强。

基于上列规范要求和业界需求，中国船级社制定了本指南，规定了船舶设备与系统可靠性测试和验证的基本方法和一般要求，为船东、设备与系统生产商、计算机软件及嵌入式系统开发方、检测和试验机构提供指导。

本指南针对船舶设备与系统所处的环境特点，规定了船舶环境参数分类及其严酷度分级，提出了不同严酷度下的环境试验要求，并给出了确定设备与系统可靠性验证综合环境条件的建议性方法。本指南分别介绍了设备、计算机软件和嵌入式软件的试验目的、试验环境、试验内容和试验方法。

基于设备、计算机软件和嵌入式软件的可靠性验证试验结果，本指南还提供了船舶设备与系统可靠性评估与计算要求，给出了常用可靠性模型及其可靠性指标计算方法。

本指南由中国船级社编写和更新，通过网页 http://www.ccs.org.cn 发布，本指南使用相关方对于指南的意见可反馈至 rd@ccs.org.cn。

第 1 章　通　则

1.1　适用范围

本指南规定了设备与系统可靠性测试和验证的基本方法和一般要求，为船东、设备与系统的生产商、软件及嵌入式系统开发方、检测和试验机构提供指导。

本指南定位为技术文件层次中的“指南”，是对规范进行解释以及新的技术在船舶和海上设施方面应用的非强制性技术文件。

1.2　一般说明

可靠性验证是通过产品的工作或模拟工作的各种试验来评价其是否满足预先规定的可靠性指标。通过对试验获得的各种数据进行统计、推断，得到相应的可靠性指标参数，进一步判断能否达到规定的要求。

1.3　船舶设备与系统的可靠性验证

根据船舶设备与系统特点，本指南接受的设备与系统可靠性验证方式包括三种：现场试验、实验室试验和仿真试验。

设备与系统的环境适应性和可靠性验证试验剖面应满足本指南第 4 章要求。

设备可靠性验证试验应满足本指南第 5 章要求。

计算机软件可靠性验证试验应满足本指南第 6 章要求。

嵌入式软件可靠性验证试验应满足本指南第 7 章要求。

系统可靠性评估应满足本指南第 8 章要求。

如遇到无法应用本指南第 5 至 8 章对船舶设备与系统可靠性进行验证的情况，可采用失效模式及影响分析（FMEA）/失效模式、影响及危害性分析（FMECA）或故障树（FTA）中的一种方法，对设备与系统的失效模式、后果及风险结果进行分析，作为验证可靠性的依据。FMEA、FMECA 或 FTA 的具体应用方法，可参见中国船级社《船舶综合安全评估应用指南》和 IEC 60812:2018。

船舶设备与系统可靠性验证由中国船级社进行，或由中国船级社认可的第三方试验验证机构进行，并通过中国船级社的见证、审核。开展设备与系统可靠性验证的第三方试验验证机构，应满足中国船级社《船用产品试验检测机构认可指南》第 1 篇第 2 章的相关要求。依据本指南通过可靠性验证的船舶设备与系统，由中国船级社签发符合性证明，具体详见本指南第 9 章要求。

第 2 章　规范引用文件

2.1　一般说明

下列参考文件对于指南的应用是不可缺少的。凡是注明版本号的引用文件，仅引用版本适用。凡是不注明版本号的引用文件，其最新版本适用于本指南。

引用文件　　表 2.1

序号	版本号	中文名称	对应的国际标准
1	-	中国船级社《钢质海船入级规范》及其修改通报	-
2	-	中国船级社《智能船舶规范》	-
3	-	中国船级社《智能设备检验指南》	-
4	-	中国船级社《电气电子产品型式认可试验指南》	-
5	-	中国船级社《船舶综合安全评估应用指南》	-
6	GB/T5080.1-2012	可靠性试验 第 1 部分：试验条件和统计检验原理	IEC60300-3-5:2001 Dependability management- Part3-5: Application guide - Reliability test conditions and statistical principles
7	GB/T5080.2-2012	可靠性试验 第 2 部分:试验周期设计	IEC 605-2:1994 Equipment reliability testing - Part2: Design of test cycles
8	GB/T 2423 系列	电工电子产品环境试验	IEC 60068-2: Environmental Testing-Part2
9	GB/T 11804-2005	电工电子产品环境条件 术语	-
10	GB/T 14597-2010	电工产品不同海拔的气候环境条件	-
11	GB/T 14092.3-2009	机械产品环境条件 高海拔	-
12	GB/T 4796-2017	环境条件分类：环境条件分类及其严酷程度	IEC 60721-1-2002 Classification of environmental conditions-Part 1: Environmental parameters and their severities
13	GB/T 4797.1-2018	环境条件分类 大自然环境条件：温度和湿度	IEC60721-2-1-2013 Classification of environmental conditions-Part2-1: Environmental conditions appearing in nature - Temperature and humidity
14	-	环境条件分类 第 3 部分：环境参数组及其严酷程度的分类 导言	IEC 60721-3-0-2020 Classification of environmental conditions - Part 3-0: Classification of groups of environmental parameters

序号	版本号	中文名称	对应的国际标准
			and their severities - Introduction
15	GB/T 4798.6-2012	环境条件分类　环境参数组分类及其严酷程度分级:船舶环境	IEC 60721-3-6-1987 Classification of environmental conditions. Part 3: Classification of groups of environmental parameters and their severities. Introduction. Ship environment
16	GB/T 20159.6-2008	环境条件分类 环境条件分类与环境试验之间的关系及转换指南：船用	IEC TR 60721-4-6: 2003 Amendment 1 - Classification of environmental conditions - Part 4-6: Guidance for the correlation and transformation of environmental condition classes of IEC 60721-3 to the environmental tests of IEC 60068 - Ship environment
17	GB/T 6994-2006	船舶电气设备：定义和一般规定	IEC 60092-101:2018 Electrical installations in ships - Part 101: Definitions and general requirements
18	GB/T 37079-2018	设备可靠性 可靠性评估方法	IEC 62308:2006 Equipment reliability - Reliability assessment methods
19	GB/T 34986-2017	产品加速试验方法	IEC 62506:2013 Methods for product accelerated testing
20	GB/T 38634-2020	系统与软件工程 软件测试	ISO /IEC/IEEE 29119-2015: Software and systems engineering- Software testing
21	GB/T 29832.1-2013	系统与软件可靠性 第 1 部分：指标体系	-
22	GB/T 29832.2-2013	系统与软件可靠性 第 2 部分：度量方法	-
23	GB/T 29832.3-2013	系统与软件可靠性 第 3 部分：测试方法	-
24	GB/T 11457-2006	信息技术 软件工程术语	-
25	GB/T 28171-2011	嵌入式软件可靠性测试方法	-
26	GB/T 22033-2017	信息技术 嵌入式软件术语	-
27	GB/T 30093-2013	自动化控制系统可靠性技术评审程序	-
28	-	可靠性、可用性、维护性和维护支持术语的数学表示式	IEC 61703-2016 Mathematical expressions for reliability, availability, maintainability and maintenance support terms
29	GB/T 14093.6-2009	机械产品环境技术要求 海洋环	-

序号	版本号	中文名称	对应的国际标准
		境	
30	GB/T 7826-2012	系统可靠性分析技术 失效模式和影响分析（FMEA）程序	IEC 60812:2006 Analysis techniques for system reliability-Procedure for failure mode and effects analysis(FMEA)
31	GB/T 37981- 2019	可信性分析技术 可靠性框图法和布尔代数法	IEC61078: 2006 Analysis techniques for dependability -Reliability block diagram and boolean methods

第 3 章　术语及缩略语

3.1　术语

3.1.1　产品 item

本指南的产品指船舶设备与系统，其中系统中的软件系统包含计算机软件和嵌入式软件及其组合。

3.1.2　故障 fault

故障是因内在状况丧失按照要求执行的能力。

3.1.3　可靠性 reliability

可靠性是产品在规定的条件和规定的时间区间内完成规定功能的能力。

3.1.4　使用寿命　useful life

使用寿命是产品从首次使用直到由于运行和维修不具备经济性或遭到废弃，不再满足用户要求的时间区间。

注 1：“首次使用”不包括先前产品移交给最终用户的测试活动。

3.1.5　可靠度（量度）reliability (measure)

本指南中可靠度（量度）简称为可靠度，即在产品给定的条件下在时间区间（t_1，t_2）内按照要求执行的概率。

注 1：给定的条件包括影响可靠性的各种因素，如：运行模式、应力水平、环境条件和适用的维修等。

注 2：通常假设在给定的时间区间的起始时刻，产品处于按照要求执行的状态。

注 3：当 t_1=0 和 t_2=t，则 R (0, t) 可简化为 R (t) ，并称为产品的可靠度函数或产品的生存函数。更详细的描述可参见 IEC61703: 2016。

3.1.6　环境适应性 environmental suitability

环境适应性是产品在其寿命期预计可能遇到的各种环境作用下能实现其所有预定功能、性能和（或）不被破坏的能力。它要求产品要在使用中遭遇恶劣的极端气候、力学和生物化学等环境中不受损坏并正常发挥作用，一般认为能适应极端环境的产品也一定能适应常规环境。

3.1.7　环境参数 environmental parameter

环境参数是描述环境因素的物理、化学和生物特性的一个或多个参数，如温度、湿度和加速度等。例如：环境因素振动是由振动类型（正弦的或随机的）、加速度和频率等参数来描述的。

3.1.8　环境参数组及其严酷等级 group of environmental parameters and their severities

环境参数组及其严酷等级是用于特定用途或特定目的的一组环境条件特性值。

3.1.9　（工作参数或环境参数的）严酷度 severity (of operation or environmental parameter)

严酷度表示每一工作参数或环境参数的量值。它可以确定作用于产品的应力水平。

3.1.10　可靠性试验 reliability test

可靠性试验是对产品可靠性量度或性质进行测量（测定）、验证或比较的试验。

3.1.121 可靠性验证试验 compliance test

可靠性验证试验是用于证明产品的特性或性能是否符合其规定可靠性要求的试验。

3.1.12　可维修产品 repairable item

产品失效后，在给定的条件下能重新恢复到执行要求功能的状态，称为可维修产品。

注 1：“给定的条件”可以包括技术的、经济的和其他方面的考虑。

注 2：产品在某些条件下是可以维修的，但在其他条件下是不可维修的。

3.1.13 **不可维修产品** non-repairable item

产品失效后，在给定的条件下不能重新恢复到执行要求功能的状态，称为不可维修产品。

注 1：“给定的条件”可以包括技术的、经济的和其他方面的考虑。

注 2：产品在某些条件下是不可维修的，但在其他条件下是可以维修的。

3.1.14 **可维修性** maintainability

可维修性指假设给定的维修活动从 t=0 时开始，在规定的条件下使用指定的程序和资源，在时间区间（t_1, t_2）内完成该活动的概率。

注 1：当 t_1=0 和 t_2= t 时，M（0, t）简化为 M (t) 并称为维修度函数。

3.1.15 **寿命试验** life test

寿命试验是为验证产品在规定条件下的使用寿命或贮存寿命所进行的试验。

3.1.16 **试验方案** test plan

试验方案是试验人员执行试验的指南。它包括统计试验方案（受试产品信息、故障产品处理方式以及试验结束准则），并进一步规定试验条件、试验设施和操作程序、观测、试验报告以及试验数据的分析。

3.1.17 **鉴别比** discrimination ratio

比率 D(D >1)，表征试验方案区分可接受可信性量度和不可接受可信性量度的能力。鉴别比是试验方案的优良指数。

3.1.18 **（瞬时）失效率**（instantaneous）failure rate

设产品在时刻 t 处于可用状态，在时间区间(t, t+Δt)内出现失效的条件概率与区间长度 Δt 之比，当 Δt 趋于 0 时的极限为失效率（如果存在）。

3.1.19 **（瞬时）失效强度**（instantaneous）failure intensity

可维修产品在时间区间(t, t+Δt)内的平均失效数与区间长度 Δt 之比，当 Δt 趋于 0 时的极限为失效强度（如果存在）。即失效强度为单位时间内出现的失效次数。

3.1.20 **硬件** hardware

硬件是用于处理、存储或传送计算机程序或数据的物理设备。

3.1.21 **软件** software

软件是与计算机系统的操作有关的计算机程序、规程和可能相关的文档。

3.1.22 **软件可靠性** software reliability

软件可靠性包括两方面含义：一是在规定条件下，在规定的时间内软件不引起系统失效的概率。该概率是系统输入和系统使用的函数，也是软件中存在的缺陷的函数。如果有缺陷存在，系统输入将确定是否会遇到已存在的缺陷。二是在规定的时间周期内、规定条件下，程序执行所要求功能的能力。

3.1.23 **软件成熟性** software maturity

软件成熟性指为避免由软件自身存在的故障而导致软件失效的能力，可采用以下几个指标来度量：

失效度用于度量软件发生和解决失效的程度，主要包括失效密度、失效解决率等；

故障度用于度量发现和排除软件自身存在故障的程度，主要包括故障密度、潜在故障排除率等；

测试度用于度量软件已被测试的程度，主要包括测试覆盖率、测试通过率等；

有效度用于度量软件运行的有效程度，主要包括平均失效间隔时间、有效服务时间率、累计有效服务时间等。

3.1.24 **软件容错性** software (error) tolerance

软件容错性指在出现故障或违反规定接口的情况下，软件维持规定性能级别的能力，可

由以下几个指标来度量：

正常运行率用于度量软件为保持正常运行所作努力的程度，主要包括避免宕机率、避免失效率等；

抵御误操作率用于度量软件为抵御误操作所作努力的程度。

3.1.25 **软件易恢复性** software recovery

软件易恢复性指在失效发生的情况下，软件重建规定的性能级别和恢复直接受影响的数据的能力，可由以下几个指标来度量：

重启成功度用于度量宕机后软件可重新使用的程度，主要包括平均宕机时间、平均恢复时间等指标。

修复成功度用于度量异常发生后软件可修复的程度，主要包括易修复性、修复有效性等。

3.1.26 **嵌入式系统** embedded system

嵌入式系统是植入应用对象内部，起信息处理或控制作用的专用计算系统。

3.1.27 **嵌入式软件** embedded software

嵌入式软件是满足嵌入式系统应用环境特殊要求的软件。

3.1.28 **内部安装** internally mounted

内部安装是指产品系统安装于能防止环境影响的隔间内，使产品系统与外部环境完全隔绝。

3.1.29 **外部安装** externally mounted

外部安装是指产品系统安装在外面，不能防止外部环境的任何影响。

3.1.30 **可靠性确认测试** reliability validation test

可靠性确认测试是为了确认在给定统计置信度下，对嵌入式软件当前的可靠性水平是否满足用户需要而进行的测试，即确认是否满足所规定的可靠性目标。

3.1.31 **级联** cascaded

直接由初始行为产生的行为，例如：级联偏离、级联失效、级联偏差。

3.1.32 **仿真试验** simulation test

基于船舶设备与系统应用场景，针对如避碰、感知等算法功能所进行的计算机虚拟测试和试验。

3.1.33 **实验室试验** lab test

指具有一定资质和能力的实验室，进行的规定类型的检测/测试。

3.1.34 **现场试验** field test

现场试验是指测试场试验或实船应用环境试验。

3.1.35 **剖面** profile

产品经历的事件和环境的时序描述，如任务剖面为产品在完成规定任务这段时间内所经历的事件和环境的时序描述。

3.1.36 **耐久性** Durability

设备的耐久性是指设备在规定的使用、储存与维修条件下，达到极限状态之前完成规定功能的能力，一般用寿命参数衡量。寿命参数包括首次大修期限、使用寿命、大修间隔期限、总寿命、储存寿命和可靠寿命等。

3.2 缩略语

下列缩略语适用于本指南：

MTBF：平均失效间隔时间（Mean Time Between Failures）；

MTTF：平均失效前时间（Mean Time to Failure）；

MTTR：平均修复时间（Mean Time to Repair）；

FI/FIO：可证明失效强度与失效强度目标之比。

第 4 章　船舶环境参数分类及其严酷度分级与可靠性验证综合环境条件

4.1　一般说明

环境适应性主要表征产品使用寿命期中，在可能遇到的各种环境包括极限环境内的生存能力。可靠性则表征产品使用寿命期中在典型环境下，其能正常工作的能力。本指南中规定，进行产品可靠性验证需要结合相应的船舶环境条件，并对产品适用环境严酷度等级予以标明。本指南将产品通过环境适应性试验作为可靠性验证的前置要求。

4.2　船舶环境参数分类及其严酷度分级要求

本指南给出的严酷度被超出的概率很低，仅将可能影响产品的结构完好性和功能特性的严酷条件包括在内。不同的部位，在某一段时间内可能会有不同的出现率，例如机器处所集控台和驾驶台的振动环境存在差异，同一时间会出现不同的出现率。对任何环境参数都应考虑其出现率，应用时应作为补充规定，详见 IEC60721-3-0 2021。

4.2.1　一般引用要求

本指南分别给出了气候环境条件（K）、生物环境条件（B）、化学活性物质（C）、机械活性物质（S）和机械环境条件（M）等级。对于具体产品，应建立一组完整的等级，如：6K2/6B2/6C2/6S1/6M4。

最低等级 6K1/6B1/6C1/6S1/6M1 的组合适用于安装在有气候防护（如水密）部位的产品和系统，并在正常使用时承受相应的环境条件。最高等级 6K5/6B2/6C3/6S3/6M4 的组合适用大部分航行环境条件比较严酷的产品和系统。各环境条件的等级标志说明详见 4.2.2 至 4.2.6，环境条件对照表见附录 1。

最极端的气候类型，例如极端寒冷和极端干热，一般只在两极和内陆区域发现，因此未包括在本指南内。但船舶在内陆水域（河流、湖泊）航行时，可能会承受此类极端气候类型。如需承受极端气候类型，则气候环境条件采取一事一议的方式确定。

对于青海湖水域以及西藏自治区内河水域（包括雅鲁藏布江水系和内陆河湖水系）以及其他高海拔航区还应考虑高海拔环境条件要求，电工产品相关要求参见 GB/T 14597-2010，机械产品相关要求参见 GB/T 14092.3-2009。

4.2.2　气候环境条件分级要求

气候环境条件分为下列七个等级标志：

6K1，6K1 包括安装在完全有气候防护、供热和通风等部位的各种产品在升温后的情况，不包括机舱和装有大散热设备部位的产品，该产品也不暴露在透过玻璃或其他透明材料的太阳辐射下。

6K1 包括湿热和稳态湿热的气候类型，也包括一切水域内浸在水中的产品，水温特别高的水域除外，例如阿拉伯海湾水域。

6K2，除 6K1 所包括的条件外，6K2 还包括了除寒冷外一切气候类型中各种有加温和通风条件的部位在升温前和升温过程中的情况。对通风部位来说，6K2 也包括了湿热和稳态湿热的气候类型。这些产品可承受潮湿、加热元件的热辐射，以及透过玻璃或其他透明材料的太阳辐射。6K2 还包括了水温特别高的各水域内浸在水中的产品。

6K3，除 6K2 所包括的条件外，6K3 还包括安装在机舱内，以及紧靠发热量大的设备的

各种产品。6K3 也包括靠近装卸货物时要临时开启的门、梯口部位的各种产品。

6K4，除 6K3 所包括的条件外，6K4 还包括除寒冷气候类型外承受太阳辐射、雨和水流影响的非通风部位，以及除寒冷气候类型外其他一切气候类型中无气候防护的产品，但不包括航行于降雨量异常和有飓风的水域。

6K4 还包括安装在机器发热部位上的产品、承受直接的太阳辐射和水流影响的产品，但不包括大浪的冲刷。

6K5，除 6K4 所包括的条件外，6K5 包括在寒冷气候类型中，安装在有气候防护但不加温的部位和无气候防护部位的产品，还包括安装在冷藏舱内和航行于降雨量异常或有飓风水域情况下无气候防护部位的各种产品，以及承受大浪冲刷的各种产品。

6K6 等级表示湿热的露天气候条件(热带湿热气候类型,如热带雨林地区)。

6K7 等级表示干热、亚干热和极端干热的露天气候条件(热带干热气候类型,如沙漠)。

4.2.3 生物环境条件分级要求

生物环境条件分为下列两个等级标志：

6B1，6B1 包括航行于无特殊动物、植物危害水域的船舶上的各种装置，以及安装在其他船舶结构不可能霉变或遭受动物危害的舱室内的各种装置。

6B2，除 6B1 所包括的条件外，6B2 还包括航行于可能霉变或遭受动物危害水域的船舶上无防护的各种装置。

4.2.4 化学活性物质分级要求

化学活性物质分为下列三个等级标志：

6C1，6C1 包括不暴露于盐雾、发动机废气和邻近工业污染源排放物，且有完全气候防护的各种装置;也包括航行于内陆淡水水域的船舶甲板上对发动机废气有防护措施的各种装置，且航线附近水域无排放大量空气污染物的工业区。

6C2，除 6C1 所包括的条件外，6C2 还包括暴露于盐雾和发动机废气，有完全气候防护的各种装置。

6C3，除 6C2 所包括的条件外，6C3 还包括无气候防护的各种装置，以及航行于排放大量空气污染物的工业区附近水域船舶上的各种装置。

4.2.5 机械活性物质分级要求

机械活性物质分为下列三个等级标志：

6S1，包括对沙、尘和烟灰侵入有防护措施的各种装置。

6S2，除 6S1 所包括的条件外，6S2 还包括可能进行积尘甲板清扫的无气候防护和有气候防护部位的各种装置，也包括处于锅炉排气(烟灰)中的各种部位。

6S3，除 6S2 所包括的条件外，6S3 还包括了各种无气候防护的装置，其中包括航行于沙漠附近的船舶上各种装置。

4.2.6 机械环境条件分级要求

机械环境条件分为下列四个等级标志：

6M1，仅包括非机动船上的装置。

6M2，除 6M1 所包括的条件外，还包括载重量大于 1000 吨机动船舶上的装置，但不包括载重量小于 20000 吨的船舶尾部装置。6M2 不包括直接与装载或者与往复机械相连接的装置。

6M3，除 6M2 所包括的条件外，还包括载重量不大于 1000 吨机动船舶上的装置和载重量小于 20000 吨的船舶尾部装置，也包括直接装载系统、集装箱导轨和起货机相连接的装置，以及挖泥船上的装置。

6M4，除 6M3 所包括的条件外，6M4 还包括直接与往复机械相连接的装置。

4.3 不同严酷度环境试验要求

产品环境试验应在试验进程期间，明确规定产品处于何种环境，明确在试验前、试验中及试验后应测量的性能参数，以及失效判据，对应不同严酷度环境条件下的试验要求可参见IEC TR 60721-4-6: 2003 和中国船级社《电气电子产品型式认可试验指南》（2015）。已通过中国船级社接受的第三方检测和试验机构或根据特别情况商定进行的环境试验，无需重复进行环境试验，应根据 4.2.1 节要求标明产品已通过环境试验所对应的环境严酷度，具体环境条件和试验之间的转换关系可参见 IEC TR 60721-4-6: 2003。

4.4 可靠性验证剖面要求

4.4.1 寿命剖面要求

寿命剖面是对船舶设备与系统在从接收到寿命终结或退出使用这段时间内所要经历的各种事件和状态（包括环境条件、工作方式及其延续情况）的一种时序描述。寿命剖面涉及寿命期内的每个重要事件，例如贮存运输、试验与检验、备用与待命状态、运行使用或任务，以及其他可能事件。寿命剖面是确定产品将会遇到的环境条件的基础。

4.4.2 任务剖面要求

任务剖面是对船舶设备与系统在完成规定任务这段时间内所要经历的全部重要事件和状态的一种时序描述，是寿命剖面的一部分。一种产品或系统可用于执行单一功能，也可用于执行多项功能。因此，任务剖面可以有一个或多个。任务剖面是决定产品或系统在使用中将会遇到的主要环境条件的基础，取决于产品或系统的使用要求。

4.4.3 环境剖面要求

环境剖面是产品在贮存、运输、使用中将会遇到的各种主要环境参数和时间的关系图，应根据任务剖面绘制。每个任务剖面对应于一个环境剖面，因此环境剖面可以是一个或多个。

4.4.4 试验剖面要求

试验剖面是直接供试验用的环境参数与时间的关系图，按照一定的规则对环境剖面进行处理后得到的。试验剖面还应考虑任务剖面以外的环境条件，例如开阔水域自主航行和停泊的温度环境。对设计用于执行一种功能的产品，试验剖面与环境剖面和任务剖面之间呈一一对应关系，对设计用于执行多项功能的产品，则应按照一定的规则将多个试验剖面合并为一个综合试验剖面。本指南在附录 2 提供了综合试验剖面的示例。

4.5 可靠性验证试验综合环境条件要求

若船东或目标船舶设备与系统有试验条件的规定，则试验条件按照已有规定确定。若船东或者目标船舶设备与系统无其他规定，则可靠性验证试验应在电压输入、温度、振动、湿度和其他有关试验条件的综合作用下进行，试验条件的量值应根据产品的目标任务剖面和工作环境剖面确定。

为了尽量逼真地模拟产品在使用中所处的实际环境，应优先使用实测应力（特别是温度和振动），也可使用估计应力，应力的获取也可以通过仿真试验或计算。在无法有效获取上列应力的情况下，可根据产品使用安装位置和环境参照使用本指南 4.5.1、4.5.2、4.5.3 提供的应力。

(1) 实测应力

实测应力是指根据产品在实际使用中执行典型任务剖面时，在受试产品安装位置附近测得的数据，经过分析处理后确定的应力。

(2) 估计应力

估计应力是根据处于相似位置，具有相似用途的产品在执行相似任务剖面时测得的数据，经过分析处理后确定的应力。只有在无法得到实测应力的情况下方可使用估计应力。

(3) 参考应力

当无法确定实测应力和估计应力时，可采用本指南提供的参考应力要求。

在规定船舶设备与系统靠性验证试验的综合环境条件时，应考虑产品在船上的安装位置和船舶类型，例如安装在甲板、上层建筑和桅杆区的无遮蔽产品，往往会经受更为严酷的环境应力；为了包括最坏的贮存和运输环境，在进行综合环境试验时，应增加冷浸和热浸环境；对于工作任务剖面为多雨环境条件的产品，在设计其验证试验剖面时还应考虑淋雨影响；对于安装于机舱及燃料舱和含易挥发油性货物货舱位置的产品，还应考虑油雾影响。

船舶设备与系统按其在船舶上的安装位置和环境分为以下三类：

(1) 外部安装的产品；

(2) 内部无温控舱室安装的产品；

(3) 内部有温控舱室安装的产品。

4.5.1 外部安装的产品

4.5.1.1 电应力和工作循环要求

电应力包括产品的通断电循环、规定的工作模式及工作周期、规定的输入标称电压及其最大允许偏差。工作循环期间，输入电压应在图 4.5.1.1(1)所示的几个等级之间变化。若船东或者客户方无其他规定，则输入电压的范围应为标称电压的 6%~10%或者符合有关规范的规定。受试产品在标称电压和室温完成性能测量后，应按图 4.5.1.1(1)和图 4.5.1.1(2)分别施加最低和最高电压并进行工作循环。产品在冷浸和热浸期间不通电，在其他时间内有 10%的随机时间处于断电状态。

4.5.1.2 振动应力要求

振动应力量值和剖面应按产品的现场使用类别、产品的安装位置和预期使用情况确定。在确定实际振动应力时，至少应考虑以下因素：振动类型、频率范围、振动量值，施加振动的方向和方式。

应按图 4.5.1.1(1)和图 4.5.1.1(2)的安排，在随机抽取的 25%工作循环内施加振动应力。振动频谱应该符合图 4.5.1.2 的规定。试验在使用要求或者用户合同规定的某一轴向进行。振动程序如下：

(1) 每 24h 随机抽取 6h 施加振动应力，并以 3h 为一个振动循环。

(2) 施加航行及运输随机频谱时按以下规定进行随机振动；

① 频率范围：10Hz~200Hz；

② 量级（总均方根值 r.m.s）:10m/s^2；

③ 持续时间：22min。

注：本指南所提及的温控包括温度控制装置及温控器，温度控制装置是将温度控制在限定范围内的装置，温控器是将感应温度和控制加热器功率的器件合并在一起的装置或组合。

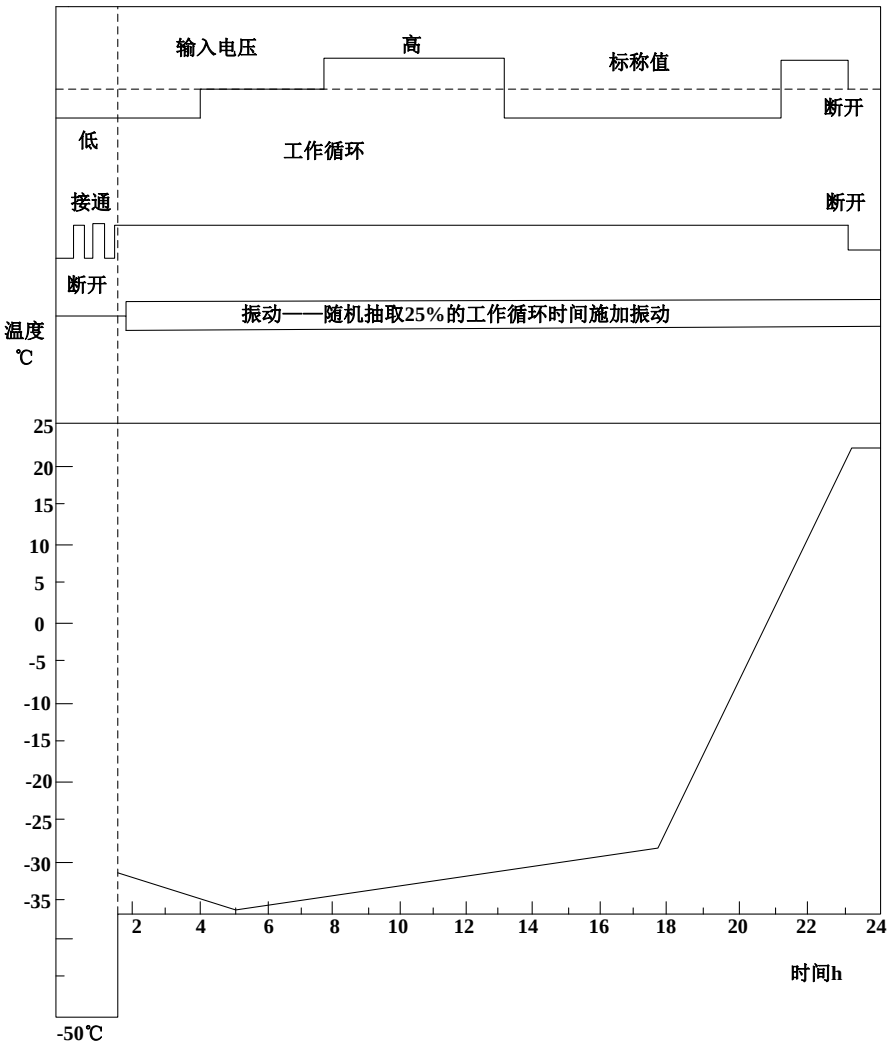


图 4.5.1.1(1) 外部安装产品的合成试验剖面（冷循环）

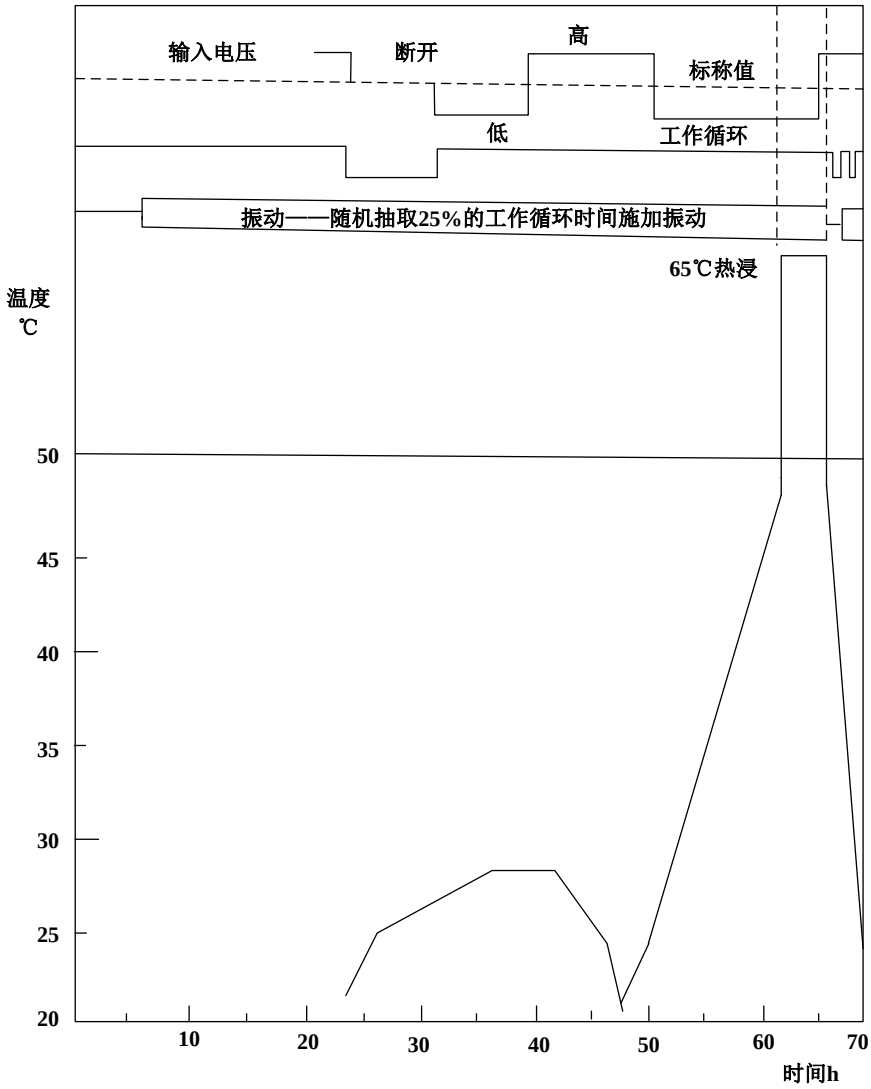


图 4.5.1.1(2) 外部安装产品的试验剖面（热循环）

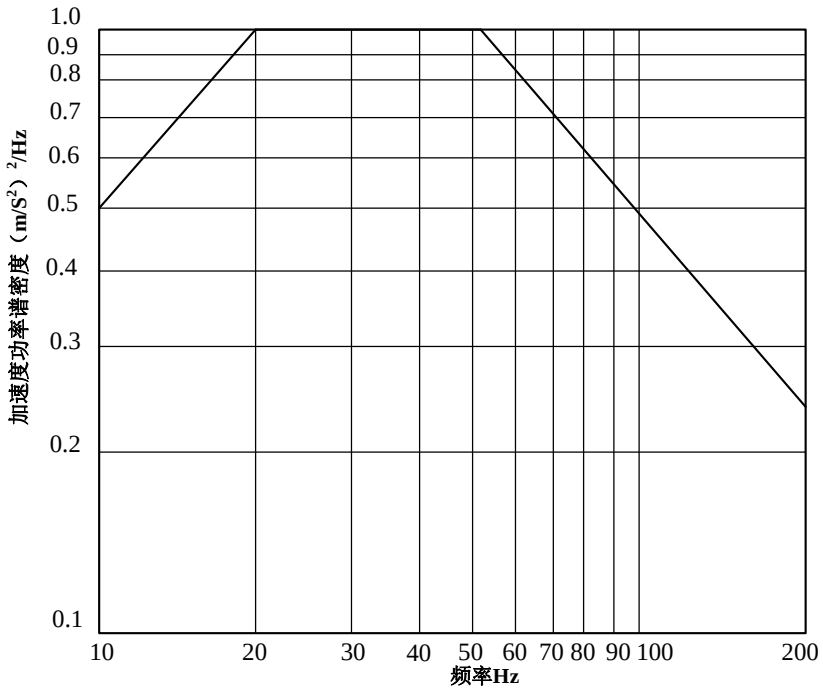


图 4.5.1.2 航行及运输途中随机频谱

4.5.1.3 温度和湿度应力要求

试验循环期间根据需要，在适当阶段喷入水蒸汽，调节湿度应力，以模拟使用中经历的环境条件。温度应力应真实地模拟受试产品在使用中经历的实际环境。确定温度应力时，至少考虑以下因素：起始温度（热浸、冷浸）、工作温度（范围、温度变化率和持续时间）、每一个任务剖面的温度变化情况，冷却气流（设备功耗、拥挤情况及冷却空气流动情况），同时应考虑受试产品的实际应用环境，避免过载导致受试件损坏。

外部安装的产品，其温度和湿度剖面按以下规定，所有相对湿度的容差应为±5%：

(1) 从 22℃和 25%~75%的相对湿度开始将温度尽快降到-50℃,在-50℃（冷浸)下保持 1.75h（不通电)后将温度升到-32℃,冷浸仅在前 3 个循环中进行；
(2) 在 3.5h 内将温度缓慢降到-34.5℃；
(3) 在 13h 内将温度缓慢升到-28℃；
(4) 在 5h 内将温度升到 22℃；
(5) 使温度保持在 22℃，将相对湿度在 1h 内调到 25%~75%；
(6) 在 2h 内将温度升到 25℃，相对湿度升到 95%；
(7) 在 10h 内将温度缓慢升到 29℃，使相对湿度继续保持在 95%,保持 5h；
(8) 在 5h 内将温度缓慢降到 25℃，使相对湿度继续保持在 95%；
(9) 在 2h 内将温度降到 22℃，相对湿度降到 25%~75%；
(10) 在 2h 内将温度升到 25℃，相对湿度调到 65%；
(11) 在 12h 内将温度缓慢升到 48℃，相对湿度降到 25%；
(12) 将温度尽快升到 65℃（热浸)，相对湿度升到 95%，保持 2h（不通电)后将温度降到 48℃，热浸仅在前 3 个循环进行；
(13) 在 6h 内将温度缓慢降到 22℃，相对湿度降到 25%~75%；
(14) 再重复步骤到（6）到（13）五次；
(15) 返回步骤（1），并重复以上循环直至到所要求的试验持续时间。

4.5.2 内部无温控舱室安装的产品

内部无温控舱室安装的产品，其完整的试验剖面见图 4.5.2(1)和图 4.5.2(2)。

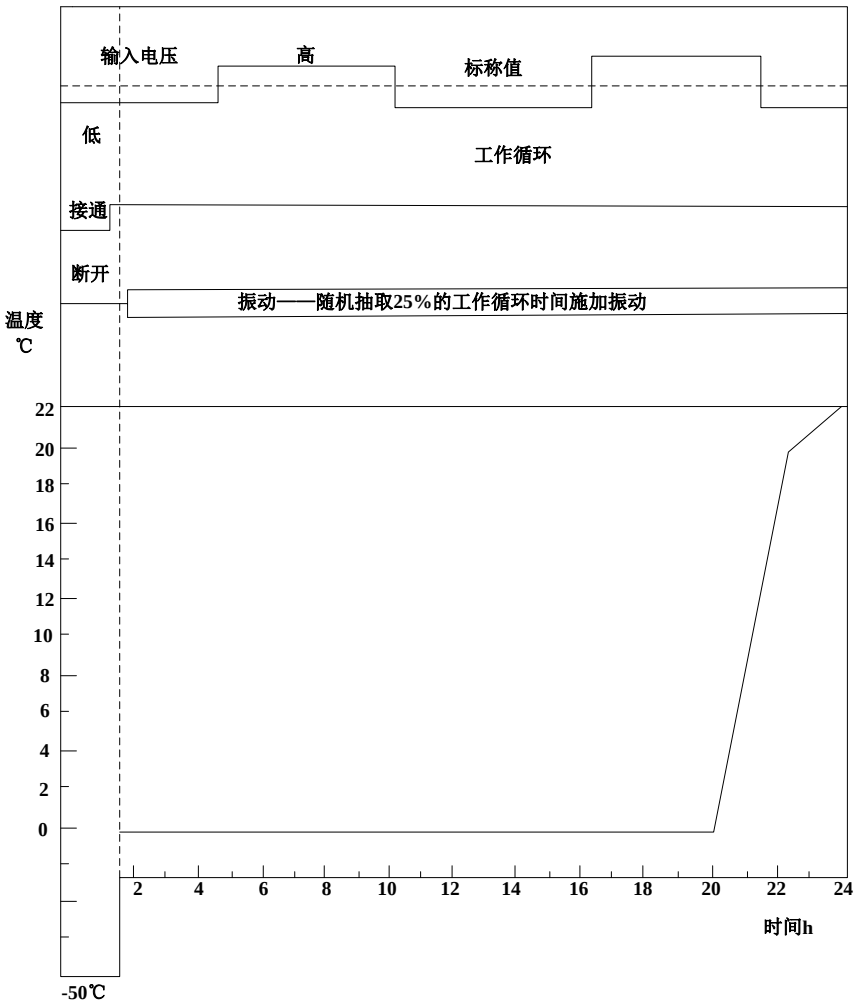


图 4.5.2(1) 无温控内部安装产品试验剖面（冷循环）

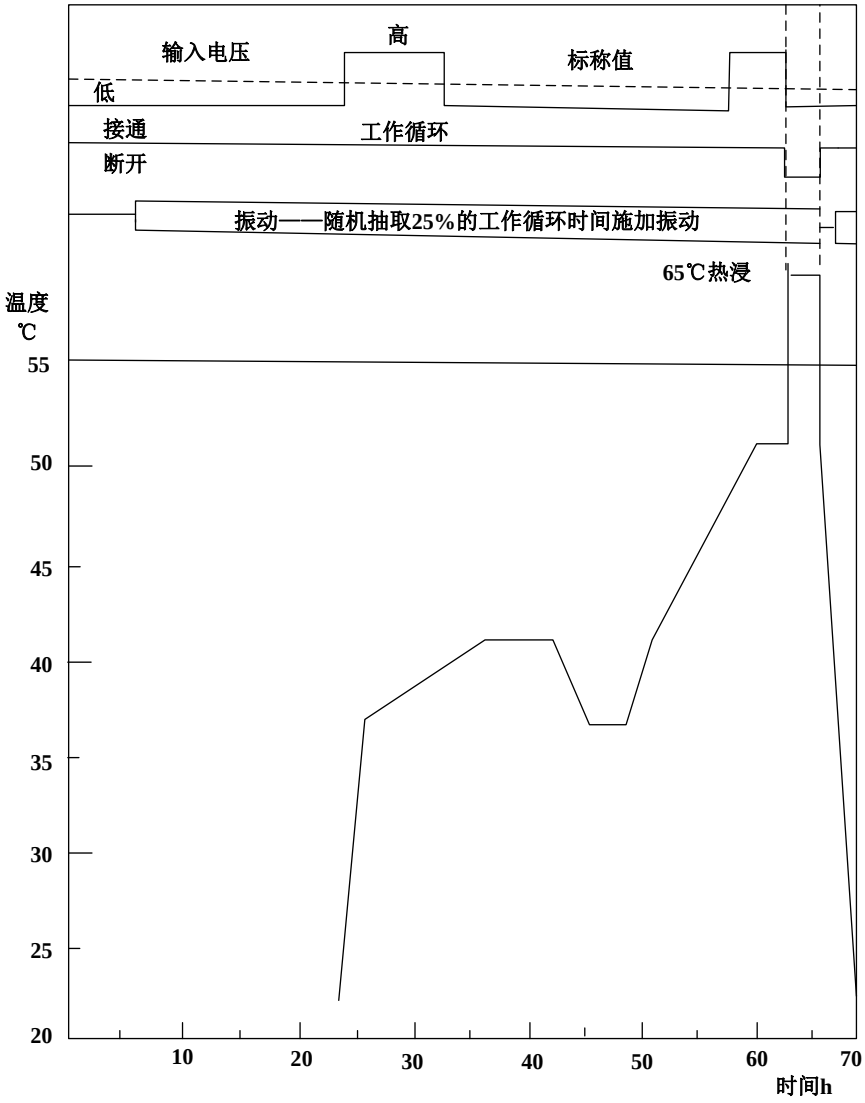


图 4.5.2(2) 无温控内部安装产品的试验剖面（热循环）

4.5.2.1 电应力和工作循环要求

参见 4.5.1.1 的要求。

4.5.2.2 振动应力要求

参见 4.5.1.2 的要求。

4.5.2.3 温度和湿度应力要求

内部无温控舱室安装的产品，其温度和湿度剖面按以下规定，所有相对湿度的容差应为±5%。

(1) 从 22℃和 25%~75%的相对湿度开始，将温度尽快降到-50℃，在-50℃（冷浸)下保持 1.75h（不通电)后将温度尽快升到 0℃，冷浸仅在前 3 个循环中进行；

(2) 在 0℃保持 19.5h 后，在 2h 内将温度升到 19℃；

(3) 在 1h 内分别将温度和相对湿度调到 22℃和 25%~75%；

(4) 在 2h 内分别将温度和相对湿度调到 37℃和 50%；

(5) 在 10h 内分别将温度和相对湿度缓慢调到 41℃和 48%，并保持 5h；

(6) 在 5h 内分别将温度和相对湿度调回到 37℃和 50%；

(7) 在 2h 内使温度保持在 37℃，将相对湿度下降到 43%；

(8) 在 2h 内分别将温度和相对湿度调到 41℃和 33%；

(9) 在 9h 内分别将温度和相对湿度缓慢调到 50℃和 21%,并保持 4h；

(10) 将温度迅速升到 65℃（热浸)，相对湿度升到 95%，保持 2h（不通电)后，将温度尽快降到 50℃，热浸仅在前 3 个循环进行；

(11) 在 5h 内分别将温度和相对湿度缓慢调回到 22℃和 25%~75%；

(12) 再重复步骤（4）到（11）五次；

(13) 返回到步骤（1），并重复以上循环直至达到所要求的试验持续时间。

4.5.3 内部温控舱室安装的产品

内部温控舱室安装的设备，其完整试验剖面见图 4.5.3(1)和图 4.5.3(2)。

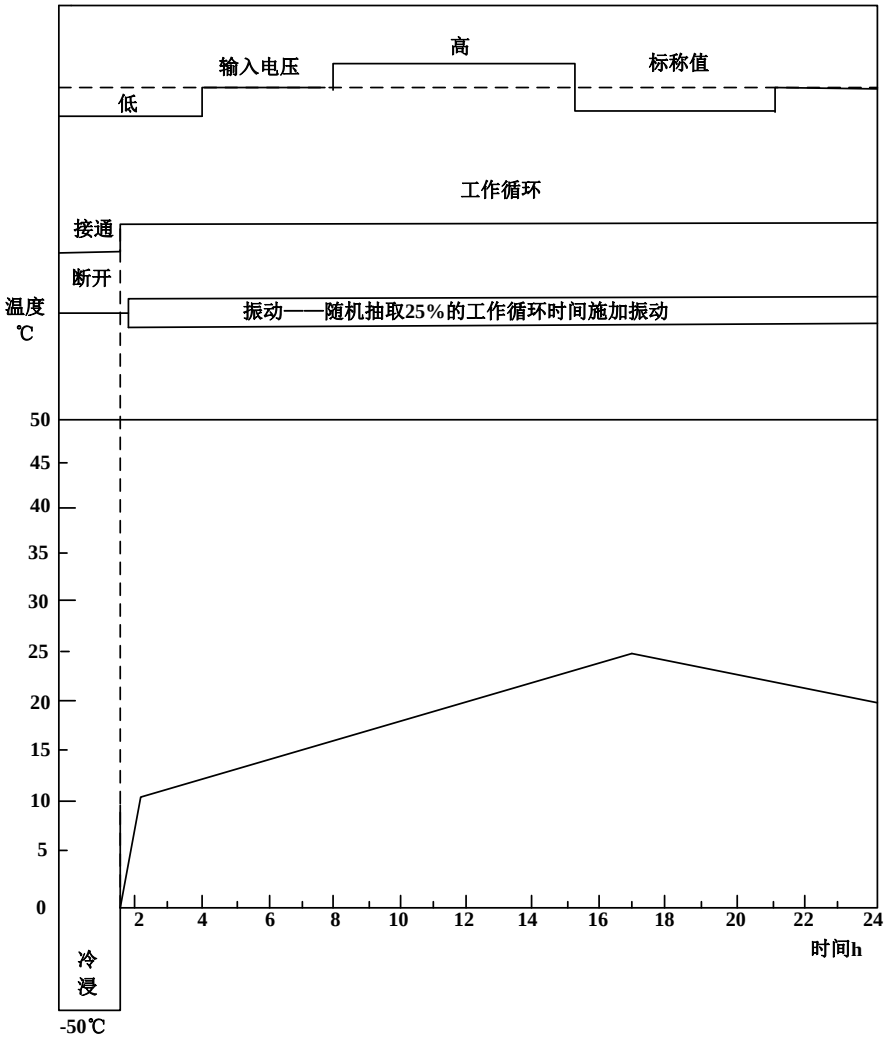


图 4.5.3(1) 内部舱室安装产品（有温控）的试验剖面（前部分）

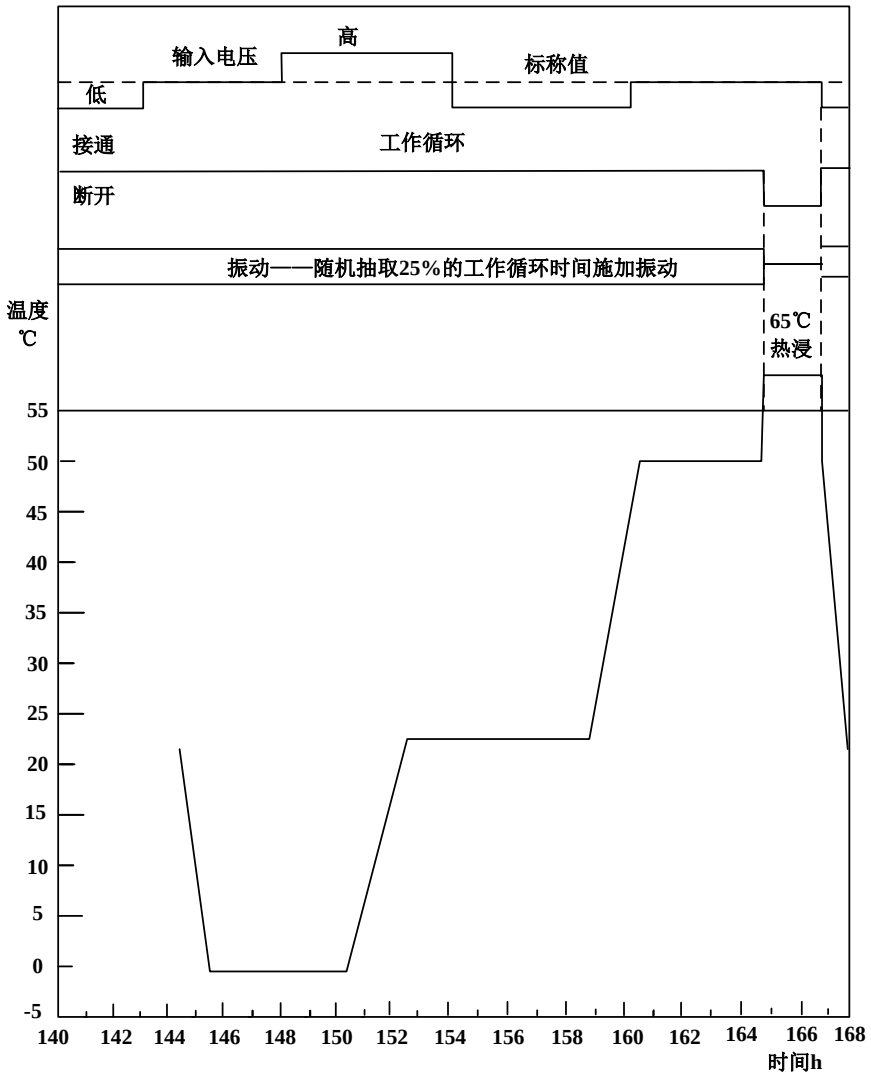


图 4.5.3(2) 内部舱室安装产品（有温控）的试验剖面（后部分）

4.5.3.1 电应力和工作循环要求

参见 4.5.1.1 的要求。

4.5.3.2 振动应力要求

参见 4.5.1.2 的要求。

4.5.3.3 温度和湿度应力要求

内部温控舱室安装的产品，其温度和湿度剖面按以下规定，所有相对湿度的容差应为±5%。

(1) 从 22℃和 25%~75%的相对湿度开始，尽快将温度降到-50℃（冷浸)，相对湿度调到 25%，保持 1.75h（通电)后，在 0.25h 内将温度升到 10℃，并使相对湿度调到 75%，冷浸仅在前 3 个循环中进行；

(2) 在 15h 内分别将温度和相对湿度缓慢调到 25℃和 30%；

(3) 在 7h 内分别将温度和相对湿度缓慢调到 22℃和 30%；

(4) 再重复步骤（1）到（3）五次；

(5) 在 1h 内将温度降到 0℃，并保持 5h；

(6) 在 2h 内分别将温度和相对湿度调到 22℃和 46%，并保持 7h；

(7) 在 2h 内分别将温度和相对湿度调到 50 和 21%，保持 4h 后将温度尽快升到 65℃（热浸)，保持 2h（不通电)后，将温度快速下降到 5℃，热浸仅在前 3 个循环进行；

(8) 在 1h 内分别将温度和相对湿度调到 22℃和 25%~75%；
(9) 返回到步骤（1），重复此循环直至达到所要求的试验持续时间。

第 5 章　船舶设备可靠性验证

5.1　一般说明

本章适用于不含计算机系统的电气类、电子类、机械类、气动类、液压类和材料类等设备。

5.2　试验目的

一般情况下，对于有可靠性指标要求的新研制或改进设备，特别是关键性或技术含量较高的设备，应进行可靠性验证试验。基于试验数据，验证设备的特性或性能是否符合其规定的可靠性要求。

验证试验的结果是“接收”（符合）或“拒收”（不符合）。验证试验基于统计假设检验理论，假设针对设定的概率模型的参数。对验证试验，应根据下列两个特征之一确定试验方案和判定标准，进而通过决策风险和鉴别比来确定。一是对规定试验次数或在规定试验时间内，可接受的关联失效数（可接收数可以为零）；二是对规定关联失效数，可接受试验次数与可接受试验时间的比值（规定关联失效数可以为零）。

对应决策风险，包括生产方风险和使用方风险两部分。生产方风险是当设备具有规定的可接受可靠性值时而被拒收的概率（第Ⅰ类风险），使用方风险是当设备具有规定的不可接受可靠性值时而被接收的概率（第Ⅱ类风险）。为尽量减少设备的第Ⅰ类风险和第Ⅱ类风险，对生产方来说应确保设备的可靠性优于规定的可接受值，对使用方也同理。鉴别比与可靠性度量指标相对应，可以选择成功率/失败率，失效率和失效强度。统计方案类型和比较具体可参考 GB/T 5080.1-2012，试验方案可参考 GB/T5080.5-1985 和 GB/T5080.7-1985。

5.3　试验环境

通常使用具有代表性，能代表定型设备的技术状态，体现出设计和制造水平的设备进行验证试验。试验方式可选择实验室试验或现场试验。

进行验证试验时，应尽可能模拟实际的使用条件，包括环境条件、工作条件和维护条件。环境的相关要求见本指南第 4 章。

试验应在验船师参加或中国船级社接受的公认独立第三方检测和试验机构或根据特别商定的情况下进行。

5.4　试验内容

试验内容主要包括统计试验方案设计、试验剖面设计和试验实施三个方面。

统计试验方案、试验条件、试验设施和操作程序、观测、试验报告以及试验数据分析都应包含在试验方案中。其中，适用的可靠性指标和可接受值，检验分布假设的有效性，抽取试验样品的产品母体和具体的抽样方法，为监测产品、维修设备和试验程序的控制试验运行而配备的试验设备，当受试产品和试验设施发生故障时应采取的措施等应详细说明。

对产品可靠性验证试验的任何要求均应包含或规定在产品合同或产品技术规范中。

5.5　试验方法

5.5.1　统计试验方案

试验方案应描述受试产品的数量、故障设备处理的方式（维修、替换、撤离）以及试验

结束的准则，有两种基本的试验方案，在试验中产品可以进行有替换或无替换/维修或不维修。

(1) 截尾序贯试验

在截尾序贯试验期间，按事先拟定的接受、拒收和截尾时间，对产品进行连续地或短间隔地监测，并将累计的相关试验时间和关联失效数与确定是否接收、拒收或继续试验的判据进行比较。

(2) 定时/定数截尾试验

在定时/定数截尾试验期间，事先规定试验截尾时间/截尾的故障数，对受试产品进行连续地或短间隔地监测，直至累计相关试验时间超过预定的相关试验时间（接收）或发生了预定的关联失效数（拒收）。

试验方案的选择应基于统计学考虑。用时间度量可靠性指标的电子产品、部分机电产品及复杂的功能系统，适用于指数分布，而二项分布适用于以成功率为可靠度指标的成败型产品。如以上均不适用，还可考虑其他分布，如 Weibull 分布。

5.5.2 试验剖面设计

试验剖面设计见本指南第 4 章第 4.4 节和第 4.5 节。

5.5.3 试验流程

可靠性验证试验流程，见图 5.5。对产品可靠性验证试验的具体要求，参见 GB/T 5080.1-2012 中[5.1.2]。试验数据收集和分析要求，参见 GB/T 5080.1-2012 中[7]和[8]。

5.6 寿命试验

按照获得期望信息所需要的时间和所用的试验条件，寿命试验可分为常态寿命试验和加速寿命试验。对于可靠性水平高的设备，常态寿命试验的时间通常较长。为缩短设备上市周期、降低设备成本，满足人们对经济、高效试验方法的需求，通常用加速试验来解决。

按照增加应力的方式，加速寿命试验可以分为恒定应力加速寿命试验、步进应力加速寿命试验、序进应力加速寿命试验等。对于寿命指标具备可加速性的设备，加速寿命试验可参照 GB/T 34986-2017 附录 E 进行，试验输出为可靠度参数或寿命指标。部分设备的寿命指标不具备可加速性，如开关的寿命次数、折页板开合次数等，应进行常态寿命试验。试验方法见本章第 5.5 节。

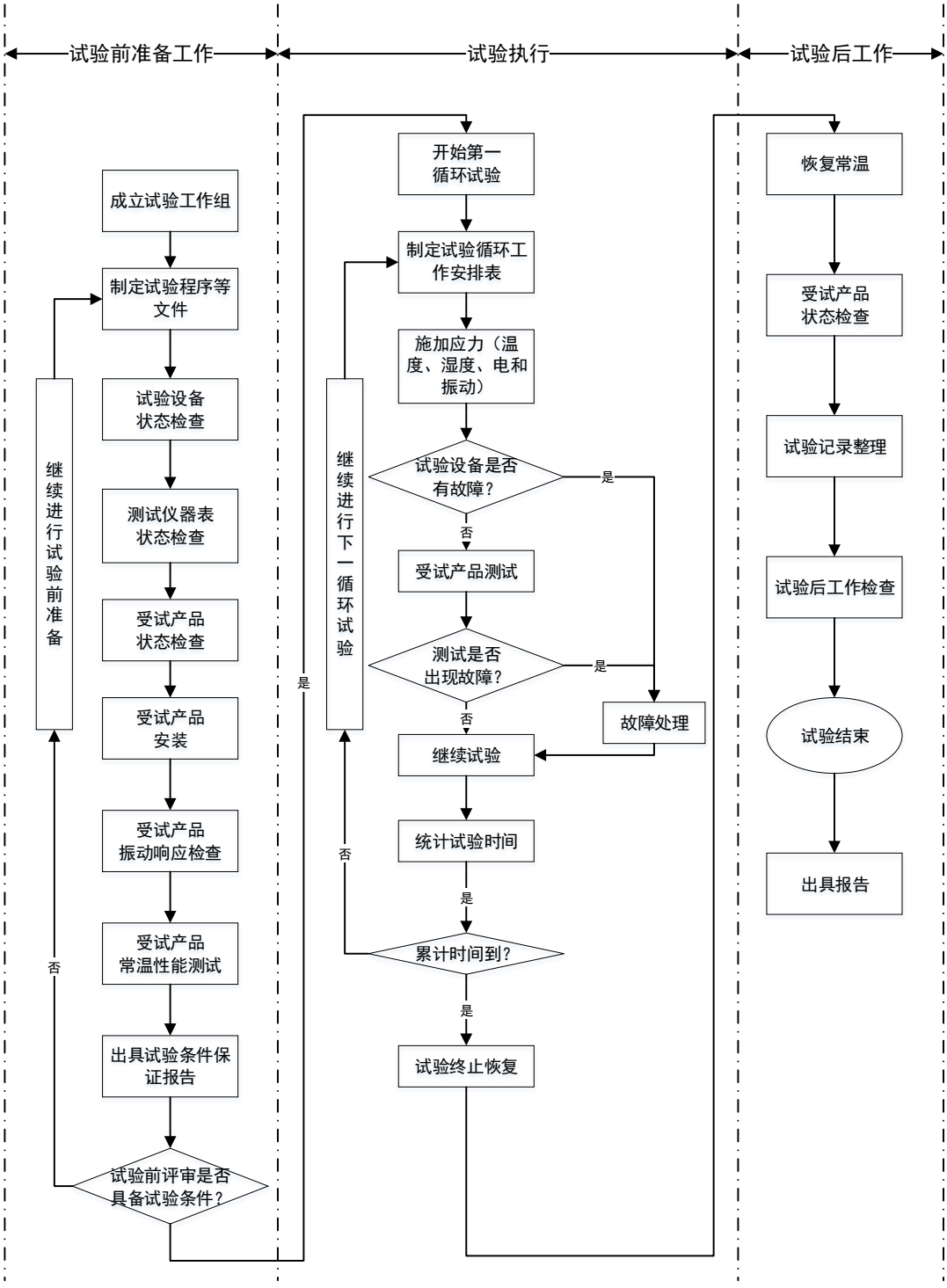


图 5.5 可靠性验证试验流程图

第 6 章　船舶计算机软件可靠性验证

6.1　一般说明

计算机软件的可靠性是软件质量的指标之一，软件失效可危及到整个系统。

软件可靠性验证的基础是软件测试，软件测试是保证软件质量、提高软件可靠性的主要手段。没有充分的测试工作，就不可能对软件可靠性进行有效的分析与预计。在进行软件可靠性验证之前，应保证度量指标达到预定的要求，即软件可靠性验证的前置条件是软件已运行过一段时间，并已通过功能性测试。软件测试的相关要求，参见 ISO/IEC/IEEE 29119。

软件需要硬件设备执行程序、存储和传输，因此软件可靠性测试还应综合考虑相关的软硬件环境和网络环境。

结合中国船级社《船用软件安全及可靠性评估指南》、《船舶网络系统要求及安全评估指南》和《智能设备检验指南》的相关要求，本章给出了适用于船舶计算机软件可靠性验证要求。

6.2　试验目的

计算机软件可靠性指标主要可分为成熟性、容错性和易恢复性。设定适合的计算机软件可靠性度量指标，可以为软件的需求方、评价方、供方提供统一的度量、测试和评价方法。本章的目的是验证软件是否满足可靠性度量指标。

6.3　试验环境

试验环境包括被测试的软件系统相应的软硬件及网络环境、选定的试验工具相应的软硬件及网络环境、设定的试验场景相应的软硬件及网络环境。试验场景的综合环境应力要求见本指南第 4 章第 4.5 节。

6.4　试验内容

针对可靠性度量的指标，利用失效数据和软件可靠性模型评估软件运行的可靠性，确认是否满足用户需求。

6.5 试验方法

6.5.1　软件可靠性指标

开展软件可靠性验证时，测试人员应根据用户提供的可靠性需求分析确定测试的可靠性指标。软件可靠性指标和测试值的关系，见表 6.5.1。

软件可靠性指标和测试值对照表　　表 6.5.1

可靠性指标			测试值	计算方法	说明
成熟度	失效度	失效密度	实际检测到的失效数 A 实际测试用例总数 B	X=A/B	X≥0 X 值越小越好，X 值应随测试进程越来越小
		失效解决率	同样条件下，未再次出现的失效数 A 实际检测到的失效数 B	X=A/B	0.0BX≤1.0 X 越接近 1.0 越好
	故	故障密	实际检测到的故障数 A	X=A/B	X≥0

可靠性指标			测试值	计算方法	说明
	障度	度	产品规模 B（如源代码行数或功能点数）		X 值越小越好，X 值应随测试进程越来越小
		潜在故障率	选定一种可靠性增长估计模型，预测潜在故障总数 A_1 实际测量的故障数 A_2 产品规模 B（如源代码行数或功能点数）	X=ABS（A_1-A_2）/B	X≥0 X 值越小越好，X 值应随测试进程越来越小
		故障排除率	确定已排除故障数 A_1 实际测量的故障数 A_2 选定一种可靠性增长估计模型，预测潜在故障总数 A_3	X=A_1/A_2 Y=A_1/A_3	0.0 靠 X≤1.0，0.0 靠 Y≤1.0， X 和 Y 越接近 1.0 越好
	测试度	测试覆盖率	测试期间实际执行的测试用例数 A 按覆盖要求计划执行的测试用例数 B	X=A/B	0.0BX≤1.0 X 越接近 1.0 越好
		测试通过率	测试或运行中通过的测试用例数 A 按覆盖要求计划执行的测试用例数 B	X=A/B	0.0BX≤1.0 X 越接近 1.0 越好
	有效度	平均失效间隔时间	运行时间 T_1 周期内，累计相继发生失效之间的时间间隔 T_2 实际检测到的失效总数 A	X=T_1/A Y=T_2/A	X>0，Y>0，X 和 Y 越大越好
		有效服务时间率	有效服务的时间 A 累计总的服务时间 B	X=A/B	0.0BX≤1.0 X 越接近 1.0 越好
		累计有效服务时间	累计所有已记录的无失效的服务时间 T	X=T	X≥0 X 值越大越好
容错性	正常运行度	避免宕机[1]率	经过分析，确定导致宕机发生的失效数 A 失效密度测试中实际检测到的失效数 B	X=1-A/B	0.0≤X≤1.0 X 越接近 1.0 越好
		避免宕机率	未发生关键的和严重的失效的测试用例数 A 执行的故障模式的测试用例数 B	X=A/B	0.0≤X≤1.0 X 越接近 1.0 越好
	抵御误操作率	-	未发生关键的和严重的失效的测试用例数 A 执行的误操作模式的测试用例数 B	X=A/B	0.0BX≤1.0 X 越接近 1.0 越好
易	重	平均宕	累计在特定试验周期内，每次	X=T/N	X > 0

可靠性指标			测试值	计算方法	说明
恢复性	启成功度	机时间	从宕机到软件可以正常使用所花费的时间 T 特定的试验周期内所观察（或记录）到的宕机次数 N		X 值越小越好
		平均恢复时间	每次失效起到完全恢复所花费的时间 T_1，T_2，……，T_n 特定的试验周期内软件进入恢复的总次数 N	X=（T_1+T_2+……T_n）/N	X > 0 X 值越小越好
	修复成功度	易修复性	经过分析，确定成功完成恢复的测试用例数 A 执行的恢复测试用例数 B	X=A/B	0.0BX≤1.0 X 越接近 1.0 越好
		修复有效性	经过分析，确定满足目标恢复时间成功完成恢复的测试用例数 A 执行的恢复测试用例总数 B	X=A/B	0.0BX≤1.0 X 越接近 1.0 越好

注 1：宕机意味着在系统重新启动之前，用户所有的任务均已停止或对系统失去控制，只能被迫停机。

6.5.2 软件可靠性测试方法

计算机软件可靠性测试方法包括专家评审法、技术测试法、数学计算法和用户调查法。四种测试方法的对比，见表 6.5.2。

常用软件可靠性测试方法　　表 6.5.2

方法名称	判断标准	对象	手段	结果
专家评审法	主观	评审项目表	打分	定性
技术测试法	客观	软件测试数据	自动测试工具/人工手工测试	定量
数学计算法	客观	软件测试数据	数学模型计算	定量
用户调查法	主观	特定调查表	填写问卷	定性

对于新技术含量高、可靠性要求高的新研软件，为得到客观、量化的测量结果，通常运用技术测试法或数学计算法。

6.5.3 测试流程

软件可靠性测试主要流程如图 6.5.3(1)所示。对于流程中关键步骤的说明如下，其他步骤的具体说明参见 GB/T 29832.3-2013 附录 A。

(1) 可靠性模型

进行软件可靠性测试时，应尽早确定可靠性模型，并考虑模型的假设条件，假设条件应符合软件的实际情况。每一条假设条件都应当进行分析，在满足其他条件的情况下，应选择相对成熟、应用范围广的模型作为分析模型。对于在确定时间内的失效总数，主要考虑指数失效时间模型、Weibull 或 Gamma 失效模型。上列模型的具体信息参见 GJB/Z161-2021。对于时间的失效分布，主要考虑泊松分布和二项分布。指数失效时间模型是失效强度函数为指数的有限失效模型。在设备可靠性建模中应用广泛的 Weibull 分布和 Gamma 分布，同样适用于软件领域，用来表示期望失效数目与失效强度函数的关系。

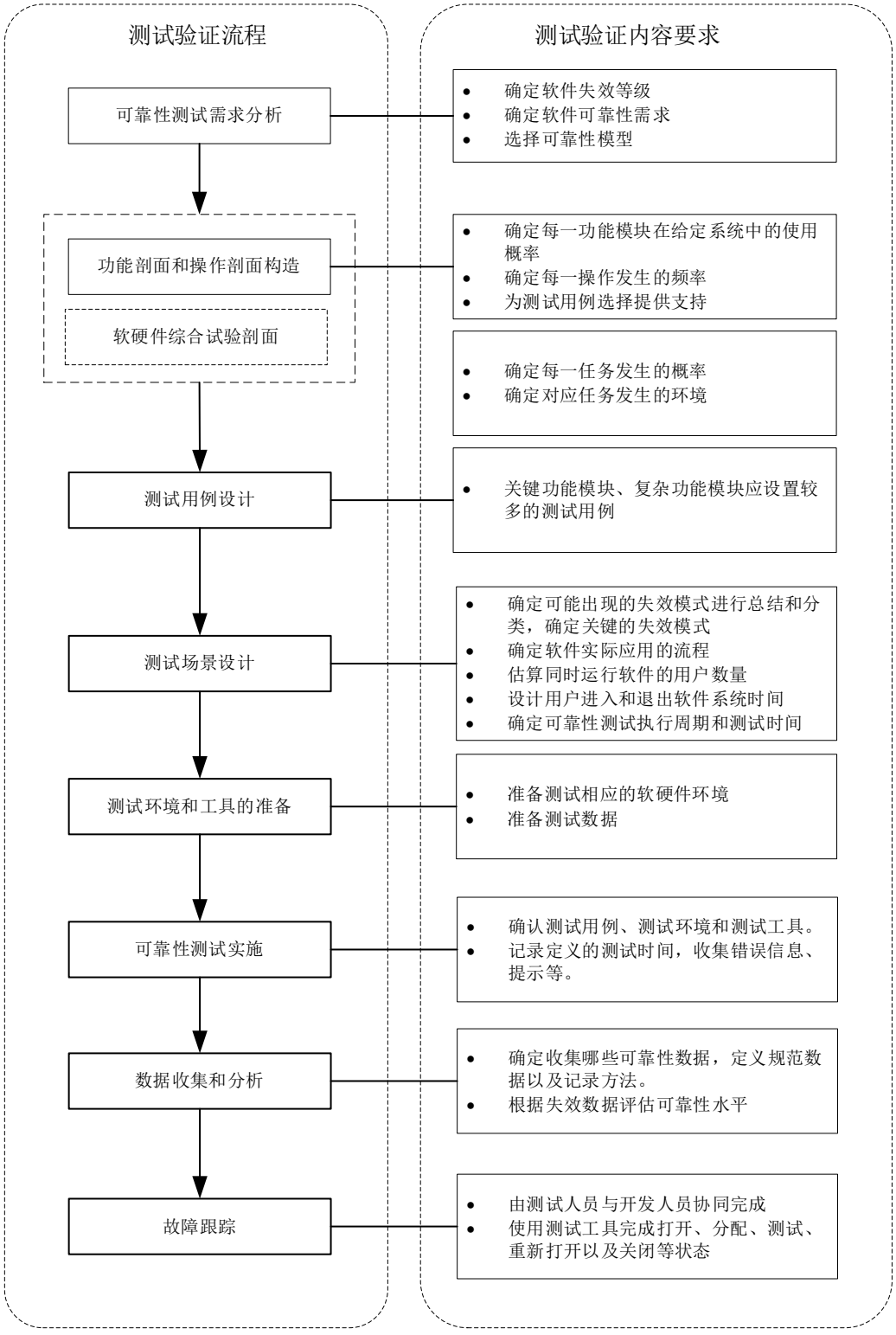


图 6.5.3(1) 软件可靠性测试流程

(2) 软件功能剖面软件操作剖面

软件功能剖面的构造对软件可靠性测试的用例选择有重要的影响。软件在使用中，各个功能的使用概率不同。同时，功能和操作存在一定的联系，一个功能可以对应一个或多个操作，一组功能可以重新合并成一组不同的操作，因此各个操作的使用概率也不同。软件功能剖面和操作剖面详细地刻画了软件的实际使用情况。在实际测试中，应根据实际情况对功能剖面和操作剖面进行合并剪裁，进而构建软件测试剖面。

应根据不同功能的使用频率来合理分配测试工作，以便在软件可靠性测试中更真实地反映软件在实际使用中的情况，使软件中的每个功能都得到充分的测试。

(3) 软硬件综合试验剖面

进行验证试验时，应尽可能模拟实际的使用条件，包括环境条件和工作条件，尽量覆盖所有可能的任务范围。对于设备的使用，可以分为任务、功能、操作三个相互关联的层面，任务是希望设备能够实现的目标，且各任务在时间上不能同时发生。通过一个或多个操作实现一个或多个功能，最终完成一项任务。任务发生的概率可以通过设备的维护数据和使用日志来确定。同时对于设备的使用，任务决定着主要环境条件。

综合以上，根据设备的实际情况，可设计软硬件综合试验剖面，设计流程见图 6.5.3(2)，其中设备综合环境应力参见本指南第 4 章第 4.5 节要求，软件测试剖面的构造见本节 6.5.2（2）。针对任意一种设备综合环境应力，都应分配到软件测试剖面。

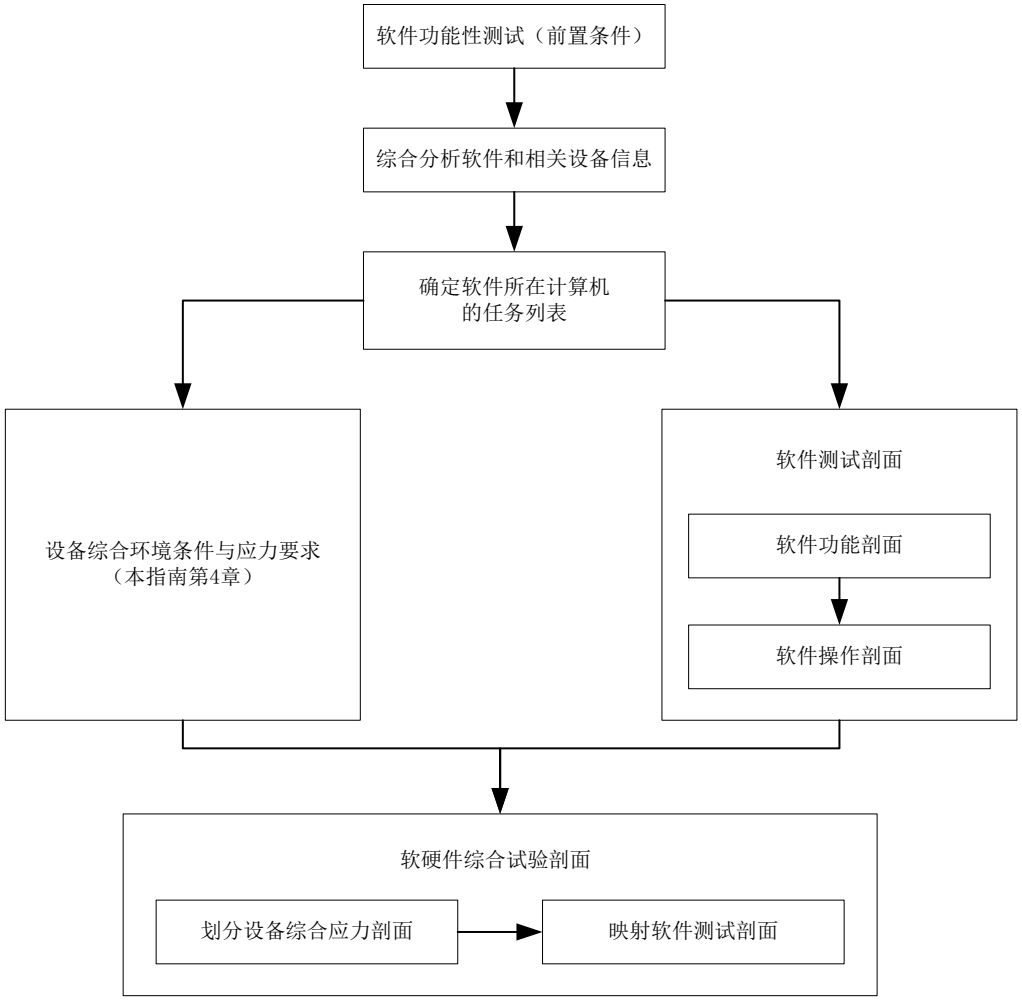


图 6.5.3(2) 软硬件综合试验剖面设计流程

第 7 章　船舶设备嵌入式软件可靠性验证

7.1　一般说明

船舶设备具有数据软硬件交互及嵌入式性质的软件系统，需要进行嵌入式软件可靠性测试验证。

7.2　试验目的

验证船舶设备嵌入式软件是否满足嵌入式系统开发合同或项目开发计划。

验证系统与子系统设计文档、软件需求规格说明和软件设计说明所规定的软件可靠性要求、可靠性的定量要求。

评估船舶设备当前嵌入式软件的可靠性水平。

7.3　试验环境

具备船舶设备运行目标环境，或高度一致的仿真实验室环境。

具备船舶设备应用验证相关的必要的测试仪表，例如，频率源、波形发生器、标准电压电流源、规约分析器等。

具备船舶设备运行的温度、湿度、振动等测试环境，具体参见本指南第 4 章。

具备船舶设备操作剖面所需要的全部外部输入输出的环境支持。

7.4　试验内容

船舶设备/嵌入式软件产品发布或交付前，为确定合同约定的可靠性指标得到满足而进行可靠性确认测试。

7.5　试验方法

7.5.1　总则

进行船舶设备嵌入式软件可靠性测试，首先应明确可靠性目标。当申请测试方没有提供规定的可靠性目标时，可按 7.5.2 中方法确定可靠性目标。

可靠性目标确定后，依次编制测试计划、开发操作剖面、进行测试准备、执行可靠性测试、分析评估，最后给出可靠性测试报告。

7.5.2　可靠性目标的确定

7.5.2.1　确定失效程度

对于船舶设备嵌入式软件，应根据产品的使用范围和对象，确定失效的严重程度。一般根据对人员生命、成本和系统能力的影响来划分失效的严重程度。通过划分失效严重程度级别，可以对失效数据进行分析，在测试过程中判定是否需要查找缺陷并加以解决。下表给出建议的失效程度级别。

嵌入式软件失效程度级别　　表 7.5.2.1

失效程度级别	对失效的描述
1	不能进行一项或多项关键操作
2	不能进行一项或多项重要操作
3	不能进行一项或多项操作，但有补救办法
4	一项或多项操作中的小缺陷

7.5.2.2 建立失效强度目标

根据船舶设备使用对象，为嵌入式软件建立失效强度目标。下表为推荐的失效强度目标、失效间隔时间与失效影响的对照表。

失效强度目标、失效间隔时间与失效影响　　表 7.5.2.2

失效造成的影响	典型失效强度目标	失效间隔时间
造成人员伤亡或千万元以上经济损失	10^{-6}	114a
没有人员伤亡，10 万元以上经济损失	10^{-4}	10000h
没有人员伤亡，万元以上经济损失	10^{-3}	1000h
没有人员伤亡，千元以上经济损失	10^{-2}	100h
没有人员伤亡，少量经济损失	10^{-1}	10h
没有人员伤亡，轻微或无经济损失	1	1h

注：表中，a 为天，h 为小时。

7.5.2.3 选择通用度量

由于船舶设备嵌入式软件一般是连续运行的，因此嵌入式软件在时间度量上，普通时间和执行任务时间是一致的。选择普通时间作为通用度量（通用度量为通常发生的事件），本测试方法采用小时（h）作为时间单位。表 7.5.2.3 为 1h 任务时间的可靠性与特定周期等效失效强度的对照表。

1h 任务时间的可靠性与特定周期等效失效强度的对照表　　表 7.5.2.3

1h 任务时间的可靠性	特定周期失效强度
0.368	1 次失效/1h
0.9	105 次失效/1000h
0.959	1 次失效/天
0.99	10 次失效/1000h
0.994	1 次失效/周
0.9986	1 次失效/月
0.999	1 次失效/1000h
0.99989	1 次失效/年

失效强度和可靠性转换按下列公式进行：

$$\lambda = -\frac{\ln R}{t}$$

$$R = \exp(-\lambda t)$$

式中：λ——失效强度；

R——可靠性；

t——时间单位数.

7.5.3 开发操作剖面

7.5.3.1 一般要求

船舶设备嵌入式软件的操作剖面可使用表格或图形方式构造。开发操作剖面时，首先确定输入及相关数据域，分析系统的可靠性需求，随后对所有可能的操作模式进行分类列表，分析影响软件操作模式的全部外界条件及其对软件圆形的影响程度，最后对各种功能需求之间的相关性进行分析和组合，对于密切相关的功能模块进行合并，对于部分相关的功能模块给出相应的输入变量的组合方式。

7.5.3.2 确定操作模式

对于不同的嵌入式软件，操作模式会显著不同，本指南建议按表 7.5.3.2 提供的方法确

定操作模式。

操作模式的确定方法　　表 7.5.3.2

确定操作模式	确定方法
主要时间和次要时间	某天或一天的某段时间，处理的事务或事务频度显著不同，处理事务的显著差别
不同的用户类型	管理员、一般使用者、新手等
输入的显著差别	大量和多边的输入
电源的极限	电源方面的要求
温度的极限	温度方面的要求
电磁的极限	电磁兼容方面的要求
其他环境的重大变化	湿度、振动、盐雾、噪声等方面的要求
行业规范要求的模式	电信、电力、银行等行业的要求

7.5.3.3　确定操作的发起者

操作发起者包括用户、外部条件、嵌入式系统自身等，按表 7.5.3.3 提供的确定方法进行识别。

操作发起者的确定方法　　表 7.5.3.3

操作发起者	确定方法
使用用户	使用者操作，远程登录等
外部条件	外部输入，例如输入一个量、收到输入信号
嵌入式系统自身	嵌入式系统软硬件判断出的条件，例如内存异常、中断信号、内部变量

7.5.3.4　选择表达方式

操作剖面的表达方式有表格法和图示法。本指南推荐采用表格法，用列表的方式，列出所有操作模式、操作发起者、操作、操作出现率等信息。

7.5.3.5　创建操作表

创建操作表需要参考用户需求、软件使用说明、行业规定、相关标准要求等，一般以操作的发起者来划分。在定义输入空间、操作覆盖输入空间时，应考虑覆盖的全面性。表 7.5.3.5 提供了创建操作表的示例。

创建操作表示例　　表 7.5.3.5

确定发起者	操作
A（外部输入一个信号）	输出一个信号到外部 1
	输出一个信号到外部 2
B（使用者输入一个指令）	显示一行信息
C（内部数据存储满）	提示数据满
	系统信号灯亮

7.5.3.6　确定出现率

根据用户需求、软件规格、使用说明、经验等信息，确定每种操作的出现率。表 7.5.3.6 举例说明如何确定出现率。

出现率示例　　表 7.5.3.6

操作	出现率（每小时出现次数）
输出一个信号到外部 1	10
输出一个信号到外部 2	10
显示一行信息	1000

操作	出现率（每小时出现次数）
提示数据满	0.001
系统信号灯亮	0.001
合计	1020.002

7.5.3.7 确定出现概率

每个操作出现率除以总出现率，即得到出现概率。表 7.5.3.7 举例说明如何确定出现概率。

出现概率示例　　表 7.5.3.7

操作	出现概率
输出一个信号到外部 1	0.0098
输出一个信号到外部 2	0.0098
显示一行信息	0.9804
提示数据满	0.00000098
系统信号灯亮	0.00000098
合计	1

7.5.4 测试准备

7.5.4.1 一般要求

测试准备工作主要包括根据概率分布信息和测试计划生成对应的测试用例输入文件，计算或给出每一测试用例预期的输出结果，构建测试环境，选择或开发测试工具，进行测试用例设计。准备测试用例时，必须保证测试的覆盖完整性。

7.5.4.2 测试用例准备

测试用例准备活动主要包括：

(1) 估计当前版本所需的新测试用例的数量；

(2) 在要测试的系统之间分配新测试用例的数量；

(3) 在每个系统的新操作之间分配新测试用例的数量；

(4) 指定新测试用例；

(5) 开发新测试用例，将新测试用例添加到以前版本的测试用例中；

(6) 基于前阶段的测试用例来设计新开发软件的第一版可靠性测试用例。

7.5.4.2.1 估计需要测试用例的数量

估计需要测试用例的数量，要考虑时间和成本因素，取这两个数量的最小值作为计划准备的测试用例的数量：

① 时间的计算，采用可用的时间乘以可用的人员数，再除以准备一个测试用例的平均时间；

② 成本的计算，采用建立测试用例的预算除以每个测试用例的平均准备成本。

对于再次测试，例如回归测试，只计算新增加的测试用例数量。

7.5.4.2.2 分配测试用例

为每个操作分配测试用例数量。对于回归测试，只分配新修改操作的测试用例。

根据操作出现率，进行下列工作：

① 确定很少出现的关键操作（概率小但应测到），为每个这样的操作分配测试用例的数量。关键操作是指失效会造成人身伤害、重大损失的操作，对这些操作要分配充足的测试用例；

② 确定偶然发生的操作（偶发性操作），分配一个测试用例。偶发性操作是指出现概率非常低的操作，这样做的目的是保证至少为这样的操作分配一个测试用例；

③ 根据操作概率，将剩下的测试用例分配给剩余的其他操作。

7.5.4.2.3 **指定测试用例**

为每个操作指定测试用例。指定测试用例的步骤包括：

① 从操作的直接输入变量的值域中，找出具有相似失效行为的值域，形成输入变量值域组合；

② 在选择了输入变量值域组合之后，从组成值域的集合成员中，随机选择输入变量，作为测试用例；

③ 选择了测试用例后，编制测试用例的脚本。

7.5.4.3 **测试过程准备**

为每个操作模式准备一个测试过程，制定或调整测试操作剖面和操作出现率，调整主要发生在回归测试或需求变更的测试过程。

7.5.5 **执行测试**

7.5.5.1 **一般要求**

被测软件测试环境（包括硬件配置和软件支持环境）应与预期的实际使用环境一致。

按测试计划和顺序对每一个测试用例进行测试，判断软件输出是否符合预期结果。测试时应记录测试结果、运行时间和判断结果。如果软件失效，那么还应记录失效现象和时间，以供失效分析。

7.5.5.2 **分配测试时间**

分配测试时间按照以下方法进行：

(1) 在要测试的系统之间分配测试时间；

(2) 先进行功能测试，以便充分执行测试用例，并对前一版本进行回归测试，然后把剩下的时间分配给负载测试；

(3) 在进行负载测试的操作模式之间分配测试时间；

(4) 测试时间分配以小时计。

估计测试需要的时间按下式计算：

$$t = \frac{T_N}{\lambda_F}$$

式中：t——用自然或时钟时间单元表示的测试时间；

λ_F——失效强度目标；

T_N——规范化度量（MTTF 数），见下式：

$$T_N = \frac{\ln\dfrac{\beta}{1-\alpha}}{1-\gamma}$$

式中：γ——分辨率；

α——生产方风险，即错误地认为失效强度目标没有达到但实际上已经达到的概率；

β——使用方风险，即错误地认为失效强度目标已经达到，但实际上没有达到的概率。

7.5.5.3 **调用测试**

功能测试根据分配的测试用例，按顺序调用测试用例，进行测试。

在每次对软件做了较大修改后，要进行回归测试。回归测试应全面检查需求变化处。随机测试和回归测试的要求不同，需要注意区分，按影响域调用相关测试用例。

7.5.5.4 **标识出现的失效**

在测试中应对测试的输出进行分析，标识出现的失效、失效时间和失效强度。

7.5.5.4.1 **分析测试输出的偏离**

采用自动化工具或以人工对测试结果审查，确定执行结果与相对预期行为的偏差。

在分析偏差的过程中，不计算级联。

7.5.5.4.2 **确定哪些偏离是失效**

对于出现的偏差，应确定是否为失效。

硬件错误引起的失效不作为嵌入式软件的失效纳入统计，但对于需要实现软件容错、避免严重错误的失效，应统计在内。

7.5.5.4.3 **估计失效发生的时间**

估计失效发生的时间采用统一的时间度量，即普通时间，以小时为单位，以出现顺序，累加度量单元。估计失效发生时间的范围包括所有操作模式的功能测试、回归测试、负载测试。

对于同时出现的多个失效记录，会导致多个零失效间隔，应在记录的时间间隔内，估计随机的时间，用于替代这些零间隔。

7.5.5.4.4 **指派失效的严重程度**

确定出失效的严重等级，失效严重等级参见表 7.5.2.1。

7.5.5.4.5 **形成测试记录**

按照执行的测试用例，记录测试过程、测试结果、运行时间、失效时间、失效现象，形成测试记录。表 7.5.5.4.5 提供了测试记录示例。

测试记录示例 **表** 7.5.5.4.5

事件	时间	失效的时间间隔/min
开始测试	2021 年 1 月 1 日 8 时 00 分	0
失效 1	2021 年 1 月 1 日 8 时 35 分	35
失效 2	2021 年 1 月 1 日 9 时 10 分	35
失效 3	2021 年 1 月 1 日 13 时 20 分	250
失效 4	2021 年 1 月 1 日 15 时 30 分	130
测试结束	2021 年 1 月 1 日 16 时 00 分	30/NA[1]

注 1：NA 表示测试结束时未失效，通过测试；30 则表示测试结束时失效，失效时间间隔为 30min，min 为分钟。

7.5.6 **可靠性确认测试**

7.5.6.1 **一般要求**

可靠性确认测试时为了确认在给定统计置信度下，对嵌入式软件当前的可靠性水平是否满足用户需要进行的测试，即确认嵌入式软件当前的可靠性水平是否满足所规定的可靠性目标。本指南采用失效执行时间和可靠性示图来进行确认测试。

7.5.6.2 **失效执行时间确认测试**

给定使用方风险 β 和 MTBF 的检验下限 θ，按下式计算出嵌入式软件的可靠性测试时间 T。

$$T = -\theta \ln \beta$$

式中：θ——MTBF 检验下限值。

β——使用方风险。

这种确认测试适用于 MTBF 在 1000h 以内的嵌入式软件可靠性确认测试，对于 MTBF 大于 1000h 的嵌入式软件，应采用可靠性示图确认测试。

7.5.6.3 **可靠性示图确认测试**

根据使用方风险和生产方风险级别构造可靠性示图，失效被绘制在图上，根据失效落入

的区域，判定被测嵌入式软件被接受、拒绝还是继续测试。

首先与提供商及客户协商确定生产方风险 α 和使用方风险 β，参照本指南附录 5 可靠性示图绘制的方法，绘制出可靠性示图。

生产方风险 α 和使用方风险 β 一般选取 20%以下，最大不宜超过 30%。对于可靠性要求很高的嵌入式软件，生产方风险 α 和使用方风险 β 应在 10%以内。

绘制可靠性示图时，需计算出继续和接受的边界、继续和拒绝的边界，并绘出边界线。边界线由下列两式求出：

$$T_{N,A}(n)=\frac{A-n\ln\gamma}{1-\gamma}$$

式中：$T_{N,A}$——已经出现的失效数对应的继续和接受边界的规范化度量；

n——失效数；

A——$\ln\frac{\beta}{1-\alpha}$

γ——分辨率，即最大可接受失效强度与失效强度目标的比值，取值范围 1.1~2.0。可靠性要求越高，取值应越小。

$$T_{N,\mathrm{B}}(n)=\frac{B-n\ln\gamma}{1-\gamma}$$

式中：$T_{N,B}$——已经出现的失效数对应的继续和拒绝边界的规范化度量

n——失效数；

B——$\ln\frac{1-\beta}{\alpha}$

γ——分辨率，即最大可接受失效强度与失效强度目标的比值，取值范围 1.1~2.0。可靠性要求越高，取值应越小。

下图的可靠性示图中，生产方风险 α=0.1，使用方风险 β=0.1，分辨率 γ=2。

根据失效数和失效发生的时间单元，计算出经过规范量化的度量（MTTF）。图 7.5.6.3 纵坐标为失效数，横坐标为计算出的规范化的度量，标注在可靠性示图上。按照如下方法进行判断：

如该点落在继续区域时，继续测试；

如该点落在拒绝区域时，结束测试，拒绝软件；

如该点落在接受区域时，结束测试，接受软件；

直到测试结束一直在继续区域时，计算 FI/FIO 比，FI/FIO 比大于 5 且出现失效时，拒绝软件；FI/FIO 比小于 5 时接受软件。

FI/FIO 比采用 λ_D 表征：

$$\lambda_D=\frac{T_{N,A}(n)}{t_t\lambda_F}$$

式中：t_t——测试结束时的时间单位数；

λ_F——失效强度目标。

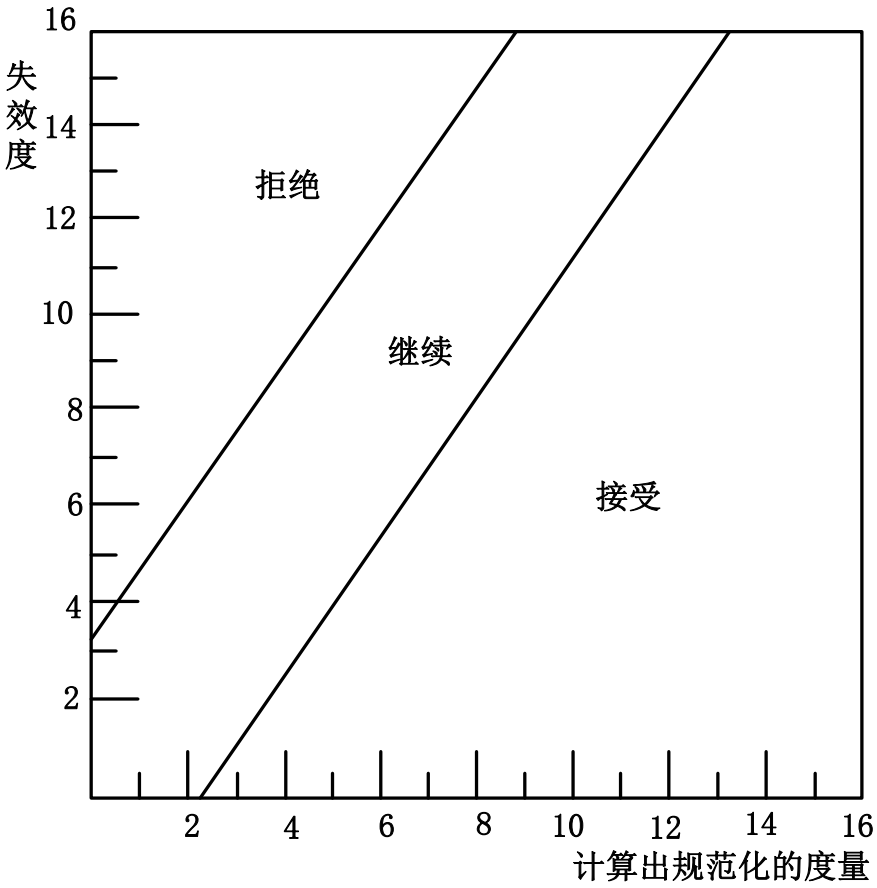


图 7.5.6.3 规范化的度量（MTTF）

第 8 章　船舶系统可靠性评估验证

8.1　一般说明

船舶系统其可靠性评估按系统寿命周期的各阶段分层次进行，应在低组装等级充分暴露缺陷并采取有效纠正措施，常见的可靠性特征量见表 8.1。

常见可靠性特征量　　表 8.1

系统级别	使用状况	
	连续或者间歇工作时间（可修复）	连续或者间歇工作时间（不可修复）
系统级	$R(t)$[a] 或 MTBF[b]	MTTF
分系统装置或者设备	$R(t)$[a] 或 MTBF[b]	MTTF
部件	λ[c]	λ[c]

[a] 可靠度

[b] 平均失效间隔时间

[c] 失效率

可靠性函数表示系统无失效运行到时间 t 的概率。对于不可修复的对象和系统。常用的可靠性函数 $R(t)=R(0,t)$，其中 $R(0)=1$。$R(t)$可由下式计算：

$$R(t)=\exp\left(-\int_0^t \lambda(u)du\right)$$

其中 $\lambda(u)$是对象的失效率。对于恒定失效 λ（即指数分布的失效时间），上列公式简化为：

$$R(t)=e^{-\lambda t}$$

对于不可修复的对象或者系统，MTTF 可由公式计算：

$$\mathrm{MTTF}=\int_0^\infty R(t)dt$$

其中，在失效时间服从指数分布的情况下，MTTF 简化为

$$\mathrm{MTTF}=\frac{1}{\lambda}$$

虽然 MTTF 的值可以针对几乎任何具有相应恒定或者非恒定失效率的失效时间分布进行计算，但由 MTTF 反向计算恒定失效率，必须确保失效率是恒定的。对于由不可修复部件组成的冗余系统，上列计算公式不适用。对于可修复对象，若组成单元发生故障后，经过修理可以使系统恢复至正常工作状态，常采用 MTBF 和 MTTR 衡量。

对于不考虑维修、不考虑失效发生顺序的系统，本指南建议采用可靠性框图法（RBD，Reliability block diagram）进行可靠性分析评估，并给出了几种常见系统类型（见 8.2）。对于需要考虑失效顺序或可维修系统, 可考虑采用其他的建模技术(如：MARKOV 模型，见附录 6)。其他复杂系统的可靠性分析评估方法，可参见 GB/T 37981-2019/IEC61078:2006。

8.2　常见系统类型

8.2.1　串联系统

如果系统的每一个元件都是实现系统整体功能所必须，只有系统全部单元都正常工作，系统才能正常工作，只要任一单元故障则系统故障，称此类系统为可靠性串联系统，其可靠性框图如下图所示：

图 8.2.1 串联系统可靠性框图

对于串联系统，系统的可靠性函数由以下公式计算：

$$R_S(t) = \prod_{i=1}^{n} R_i(t)$$

如果单个元件具有指数分布的失效时间，则

$$R_i(t) = e^{-\lambda_i t}$$

并且，

$$R_S(t) = e^{-\lambda_S t}$$

$$\lambda_S = \lambda_1 + \lambda_2 + \cdots + \lambda_n$$

式中：$R_S(t)$——系统的可靠性函数；

$R_i(t)$——不同元件的可靠性函数；

λ_S——系统的恒定失效率；

λ_i——不同元件的恒定失效率；

i——R1，R2，…，Rn。

由此可见，串联单元越多，系统的可靠性就越低。

8.2.2 并联系统

如果一个系统的多个元器件或子系统以冗余方式实现系统的整体功能，则这些单元被认为是并联的，如图 8.2.2 所示：

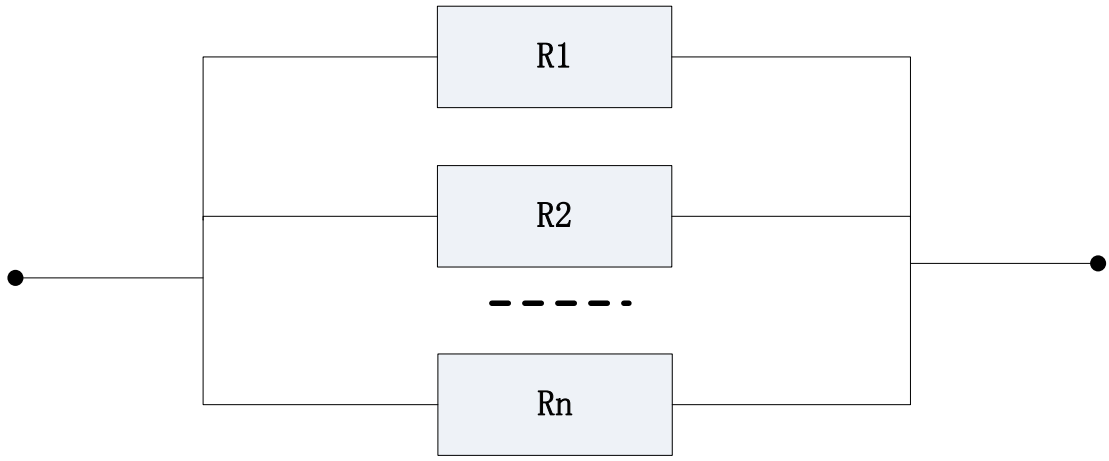


图 8.2.2 并联系统可靠性框图

对于含有不可修复元件的系统，使用以下公式：

$$R_S(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right]$$

如果单独的元件符合指数分布，则

$$R_i(t) = e^{-\lambda_i t}$$

$$\mathrm{MTTF}_{\mathrm{sys}} = \int_0^{\infty} \left[1 - \prod_{i=1}^{n} R_i(t)(1 - e^{-\lambda_i t})\right] dt$$

式中：$R_s(t)$——系统的可靠性函数；

$R_i(t)$——不同元件的可靠性函数；

$\mathrm{MTTF}_{\mathrm{sys}}$——系统的 MTTF；

λ_i ——不同部件的失效率；

I ——R1，R2，…，Rn。

8.2.3 混联结构

一般情况下，船舶系统不仅仅是用简单的串联或者并联系统来组成，通常可能是一个混联结构，混联系统可简化为若干个典型的串联或者并联的子系统，然后采用“等效模型法”来计算其可靠度。混联模型又有“串联-并联”结构和“并联-串联”混合结构，如图 8.2.3 所示为一个简化的串并联结构。

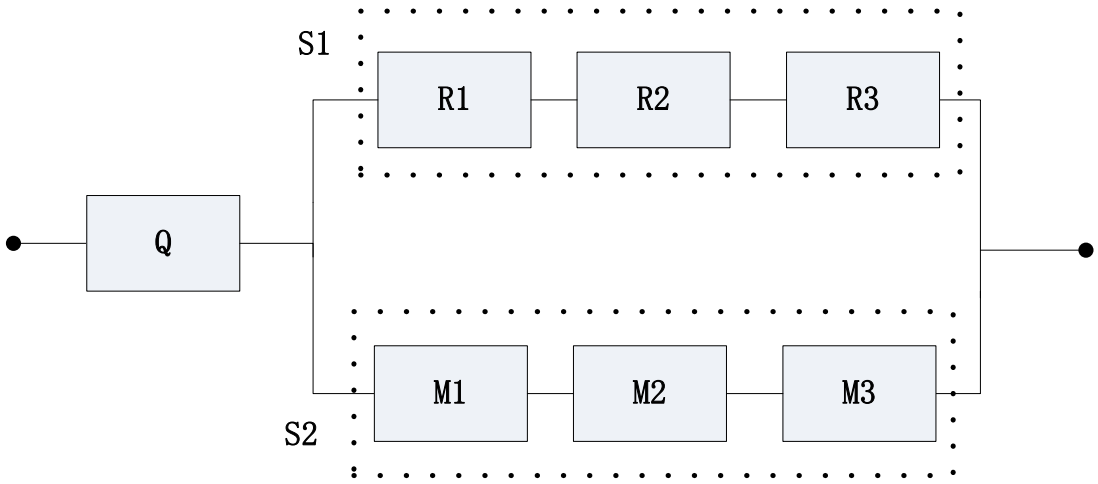


图 8.2.3 混联结构可靠性框图

则整个系统中子系统 S1 的失效率为，$\lambda_{S1}=\lambda_{R1}+\lambda_{R2}+\lambda_{R3}$

则整个系统中子系统 S2 的失效率为，$\lambda_{S2}=\lambda_{M1}+\lambda_{M2}+\lambda_{M3}$

若各单元符合指数分布，则整个系统的 MTTF 为；

$$\mathrm{MTTF}_{\mathrm{sys}}=\int_0^{\infty}R_S(t)dt=\int_0^{\infty}e^{-\lambda_Q t}\left[1-\left(1-e^{-\lambda_{S1}t}\right)\left(1-e^{-\lambda_{S2}t}\right)\right]dt$$

式中：λ_{S1}——系统 S1 失效率，S1 包含 R1、R2 和 R3；

λ_{S2}——系统 S2 失效率，S2 包含 M1、M2 和 M3；

λ_Q——设备 D 的失效率；

$R_S(t)$——系统的可靠性函数；

$\mathrm{MTTF}_{\mathrm{sys}}$——系统的 MTTF。

8.2.4 表决模型

除了 8.2.1，8.2.2，8.2.3 所列的三种模型外，如若为提升船舶系统的组装可靠性，采用了表决系统设计，则采用表决模型计算评估系统可靠性。此类系统特点是组成系统的 n 个单元中，不失效的单元个数不少于 k（k 介于 1 和 n 之间），系统就不会失效，又称为 k/n 系统。通常 n 个单元的可靠度相同，均为 R，则系统的可靠性计算为；

$$R_S=\sum_{i=k}^{n}C_n^i R^i\left(1-R\right)^{n-i}\qquad k\leqslant n$$

在 k/n 表决系统中，若 k=1，则系统即为 n 个单元的并联系统，若 k=n，则系统为 n 个单元的串联系统。

8.3 复杂系统评估验证要求

对于一些复杂度高、构成要素类型多的大型船舶系统，由于其成型数量较少，抽样理论子样数少，无法用评估单一单元产品可靠性的方法进行试验或测试。通常对此类复杂大型系统采用分解的方法：即任意大系统均是若干个子系统组成，各个子系统又分别由设备、软件

等单元构成，它们之间可以建立起类金字塔模型结构，应建立正确完整的模型结构，才能对系统可靠性做出相对精确的评估，其它相关要求见 IEC 62308: 2006 IDT。

通常此类系统评估要求如下；

(1) 在实验室和虚拟测试环境内进行系统各组成单元的试验和测试；

(2) 对系统进行典型工况的试验场测试和试航测试；

(3) 对系统开展少量的实船使用试验，开展使用试验前应进行 FMEA/FMECA 分析，并对相关报告进行审议；

(4) 综合以上三种方法的试验和测试结果，对系统可靠性进行评估。

通过上列方法，基于使用风险最小原则，实现用较少次数的全系统使用试验对复杂系统进行可靠性评估验证，主要流程如下：

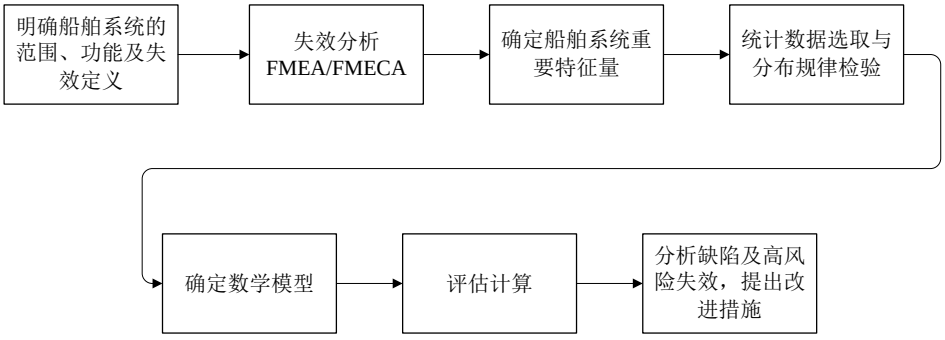


图 8.3.1 复杂系统可靠性评估

第 9 章　验证和审核

9.1　资料要求

申请对船舶设备与系统、计算机软件和嵌入式软件进行可靠性验证的船舶，船东、设备生产商及软件开发方应将以下资料提交中国船级社审核：

(1) 产品型号和版本信息；
(2) 产品规格说明书；
(3) 产品功能说明书；
(4) 产品环境条件及严酷度等级；
(5) 产品可靠性验证试验剖面要求；
(6) 产品环境试验报告；
(7) 产品可靠性验证试验报告；
(8) 产品可靠性试验总结报告；
(9) 产品可靠性试验完成情况评审；
(10) 产品可靠性框图（备查）；
(11) 型式认可试验报告（如有时）；
(12) 其他必要的支持材料。

其中，可靠性试验报告一般包括如下内容：

(1) 试验内容、目的和结论；
(2) 试验依据；
(3) 试验时间、地点及参试人员；
(4) 受试产品说明；
(5) 试验统计方案；
(6) 综合环境条件及应力施加方法说明；
(7) 试验设施和仪器情况；
(8) 试验前准备工作情况；
(9) 试验过程描述；
(10) 试验中发生的故障次数、故障分类及故障处理情况说明；
(11) 可靠性评估结论；
(12) 存在的问题及建议；
(13) 其他需要说明的有关事项。

9.2　可靠性验证与符合性证明

中国船级社依据本指南和申请方提供的资料，对船舶设备与系统开展可靠性验证。具体验证方法与过程详见本指南第 4 章至第 8 章。对于通过可靠性验证的船舶设备与系统、计算机软件及嵌入式软件，由中国船级社签发符合性证明（见附件 7）。

对于姊妹船或系列船，如其设备与系统完全相同且已通过可靠性验证，可提出申请，经船级社确认后签发可靠性验证符合性证明并免于重复验证。如姊妹船或系列船设备或系统与已通过可靠性验证的设备或系统发生了技术状态变更（如适用标准的变化、设备型号更换、设备性能指标变更、软件更新和升级等），需要将变更情况提交船级社进行审查并按本指南重新验证其可靠性。验证通过后，由船级社按照变更后的技术状态授予新的符合性证明。

9.3 营运数据反馈

投入营运后，依据本指南取得符合性证明的船舶设备、计算机软件及嵌入式软件的使用方应每年向中国船级社提供使用信息，包括故障、维修记录数据等，由中国船级社进行可靠性评价，以便使用方掌握设备、计算机软件及嵌入式软件在全生命周期内的可靠性表现，及时做出维护或更换决策，确保设备与系统可靠性水平与取得符合性证明时基本相当。具体如下：

(1) 设备与系统的运行监测数据及报警、故障、维修记录，一般包括发生故障的日期和时间，故障现象，故障原因（如有时），故障产品序列号或版本号，涉及的设备、软件或系统，故障时刻的工作条件和环境条件等基本描述，以及维修或恢复时间、后续每次故障的发生时间及其维修或恢复时间；

(2) 设备与系统的故障现象，包括局部或全部整体失效的原始症状、超出规定范围的参数值、软件报错描述等；

(3) 对于可维修产品，提供故障后的维修或恢复时间；对于不可维修产品有寿件及更换产品，提供的 MTBF、MTTF 及 MTTR 等参数信息产品更换时间信息。

附录 1　环境条件对照表

气候环境条件分级　　附表 1-1

环境参数	单位	等级						
		6K1	6K2	6K3	6K4	6K5	6K6[f]	6K7[f]
(1) 低温、空气	℃	+5	-25	-25[a]	-25	-40[b]	+5	-20
(2) 低温、水	℃	水的冰点[c]					+15	+15
(3) 高温、空气	℃	+40	+40	+55	+70	+70	+55	+70
(4) 高温、表面[d]	℃	—	—	—	+70	+70	+70	+70
(5) 高温、水	℃	+30	+35	+35	+35	+35	+35	+35
(6) 温度的梯度变化、空气/空气	℃ ℃/min	— —	-25/+20 1	-25/+40 3[a]	-25/+40 3	-25/+40 3	+5/+40 3	-20/+40 3
(7) 温度变化、空气/水	℃	—	—	—	+40/+5	+40/+5	+40/+15	+40/+15
(8) 湿度（不伴随有急剧温度变化）	% ℃	95 +30	95 +35	95 +35	95 +45	95 +45	95 +35	95 +45
(9) 湿度（在高相对湿度下伴随有急剧的温度变化）空气/空气	% ℃	— —	— —	95 -25/+35	95 -25/+35	95 -25/+35	95 +5/+30	95 -20/+30
(10) 湿度（在高含水量下伴随有急剧的温度变化[e]）空气/空气	g/m^3 ℃	— —	— —	— —	60 +70/+15	60 +70/+15	60 +55/+15	60 +70/+15
(11) 低相对湿度	% ℃	10 +30	10 +30	10 +30	10 +30	10 +30	10 +30	10 +30
(12) 周围介质的运动、空气	m/s	可忽略	可忽略	可忽略	30	50	50	50
(13) 降雨量	mm/min	—	—	—	6	15	15	15
(14) 太阳辐射	w/m^3	可忽略	700	700	1120	1120	1120	1120
(15) 热辐射	w/m^3	可忽略	600	1200	1200	1200	1200	1200
(16) 除雨以外的其他来源水	m/s	—	0.3	0.3	3	10	10	10
(17) 潮湿	—	—	潮湿表面					

[a] 有许多在机舱中的产品仅要求该处所经过一段时间的预热后就能工作。对这类产品来说，工作低温应为+5℃,而温度的梯度变化条件仅适用于非工作状态。

[b] 当空气温度低于-40℃时，船舶一般不航行。然而在一年最冷的时期中,船舶可能临时在港口停泊,此时装在船上的产品可能处于未加防护的状态。在这种情况下，处于非工作状态的产品就可能不得不承受最低至-55℃的低温环境。在内陆水道的特定情况下，船舶也可能会在低于-40℃的低温下航行。

[c] 由于盐或污染物等物质的存在，水的冰点可能低于 0℃。

[d] 产品可能会连接在一些发热部件上，这就涉及到表面温度，例如在一些机器上，极端表面温度可能会更高,必须对这种情况有所考虑。

[e] 假定产品仅承受急剧的降温(不是急剧的升温)，含水量的数值适用于降到露点的各种温度，在各种更低的温度下,可假定相对湿度约为 100%。

[f] 热带气候条件按 6K6(湿热)和 6K7(干热)分级。

生物环境条件分级 **附表 1-2**

环境参数	单位	等级	
		6B1	6B2
(1) 空气中的植物	—	可忽略	霉菌等存在
(2) 空气中的动物	—	可忽略	啮齿动物和其他对产品有害的动物存在

注：安装在船身外侧水下部分上的产品将承受水生动植物（海藻、浮渣、珊瑚）的侵蚀。

化学活性物质分级 **附表 1-3**

环境参数		单位	等级		
			6C1	6C2	6C3
空气中的物质 [a, b]	(1) 盐雾	mg/m^3 cm^3/m^3	—	存在 [c]	存在 [c]
	(2) 二氧化硫，SO_2	mg/m^3 cm^3/m^3	0.1 0.037	1.0 0.37	1.0 0.37
	(3) 硫化氢，H_2S	mg/m^3 cm^3/m^3	0.01 0.0071	0.5 0.36	0.5 0.36
	(4) 氧化氮，以 NO_2 的当量值表示	mg/m^3 cm^3/m^3	0.1 0.052	1.0 0.52	1.0 0.52
	(5) 臭氧，O_3	mg/m^3 cm^3/m^3	0.01 0.005	0.01 0.005	0.1 0.05
	(6) 盐酸，HCL	mg/m^3 cm^3/m^3	0.1 0.066	0.1 0.066	0.5 0.33
	(7) 氢氟酸，HF	mg/m^3 cm^3/m^3	0.003 0.0036	0.003 0.0036	0.03 0.036
	(8) 氨，NH_3	mg/m^3 cm^3/m^3	0.3 0.42	0.3 0.42	3.0 4.2
水中的物质 [d]	(9) 海盐	kg/m^3	可忽略	可忽略	30

[a] 由于装载特定货物，可能会存在其他物质和不同的严酷程度，油船应参照 IEC60092-505。

[b] 爆炸性气体不在本部分所考虑的范围，故未包括。

[c] 目前尚无具体数据指标。

[d]除了海盐以外，本部分未包括其他水中物质，对已采取防海盐措施的电气产品来说，其他水中物质对其影响可以忽略不计。

机械活性物质分级 **附表 1-4**

环境参数	单位	等级		
		6S1	6S2	6S3
(1) 空气中的沙	g/m^3	—	0.1	10
(2) 灰尘沉积	mg/（m^2.h）	可忽略	3.0	3.0
(3) 烟灰沉积	—	—	有烟灰存在	

注 1：由于装载特定货物，如粉状货物、沙（包括有腐蚀作用的物质）等，也可能会存在灰尘和沙的其他严酷程度，其中颗粒大小的分布和化学成分与颗粒的含量一样重要（目前尚无数据）。

注 2：在机舱空气中可能存在油雾微滴，其浓度可达到 $3mg/m^3$。靠近柴油机的部位或油水分离器舱室的浓度更高，可达 $20mg/m^3$。

机械环境条件分级 **附表 1-5**

环境参数	单位	等级			
		6M1	6M2	6M3	6M4
(1) 稳态振动（正弦）[a]					
位移	mm	—	1.5	1.5	1.5
加速度	m/s^2	—	10	20	50
频率范围	Hz	—	2~13 13~100	2~18 18~100	2~28 28~100
(2) 非稳态振动（含冲击）[b]					
I 类型					
冲击响应谱峰值加速度a	m/s^2	50	100	100	100
II 类型					
冲击响应谱峰值加速度a	m/s^2	100	300	300	300
III 类型					
冲击响应谱峰值加速度a	m/s^2	—	—	500	500
(3) 角运动倾斜 [c]					
绕 X 轴回转（横倾）					
角度	。	15	15	15	15
绕 Y 轴回转（纵倾）					
角度	。	10	10	10	10
(4) 角运动摇摆 [c]					
绕 X 轴回转（横摇）					
角度	。	22.5	22.5	22.5	22.5
频率	Hz	0.14	0.14	0.14	0.14
绕 Y 轴回转（纵摇）					
角度	。	10	10	10	10
频率	Hz	0.2	0.2	0.2	0.2
绕 Z 轴回转（首摇）					
角度	。	4	4	4	4
频率	Hz	0.05	0.05	0.05	0.05
(5) 恒定加速度 [c]					
X 轴向（纵落）					
加速度	m/s^2	5	5	5	5

环境参数	单位	等级			
		6M1	6M2	6M3	6M4
Y 轴向（横落） 加速度	m/s^2	6	6	6	6
Z 轴向（垂落） 加速度	m/s^2	10	10	10	10
[a] 常规船用发动机产生的一般是带有低频成分的正弦振动。在破冰船上会出现频率高达 2000Hz，强度高达 $50m/s^2$ 的振动。由于船身或者螺旋桨与水之间的碰撞可产生的力，船舶中也存在随机振动，但量级一般很低，故未将随机振动包括在内。 [b] 冲击是以峰值加速度α表示。 [c] 相对于船舶的三条互相垂直的坐标轴为： X=艏艉向 Y=横向 Z=垂向					

附录 2　可靠性测试验证剖面示例

可靠性任务剖面可分解成若干个不同类型的工作状态，例如：

不同环境下产品的开启/关闭工作状态；

不同环境下产品的持续工作状态；

不同环境下产品的贮存/休眠状态等。

根据适航航区不同，产品环境条件和要求也有所不同，实际合成剖面应综合考虑产品自身特点和使用场景要求，如下表为考虑温升变化的船舶电子元器件任务剖面示例：

考虑温升变化的船舶电子元器件任务剖面示例　　**附表 2**

任务剖面阶段	占空比（开启时间/关闭时间）		日常启动航行		锚地停泊		港内靠泊		进坞检修（法定 5 年 2 次，0.4 单位/年）	
航区	On	Off	热循环（次/年）	温变幅值（℃/次）	热循环（次/年）	温变幅值（℃/次）	热循环（次/年）	温变幅值（℃/次）	热循环（次/年）	温变幅值（℃/次）
远洋	0.73	0.27								
近海	0.68	0.32								
沿海	0.70	0.30								
遮蔽航区	0.63	0.47								
内河	0.58	0.42								
内湖	0.56	0.44								

注：表中剖面参数应根据实际情况进行取值，通常参数获取方法有以下几种；

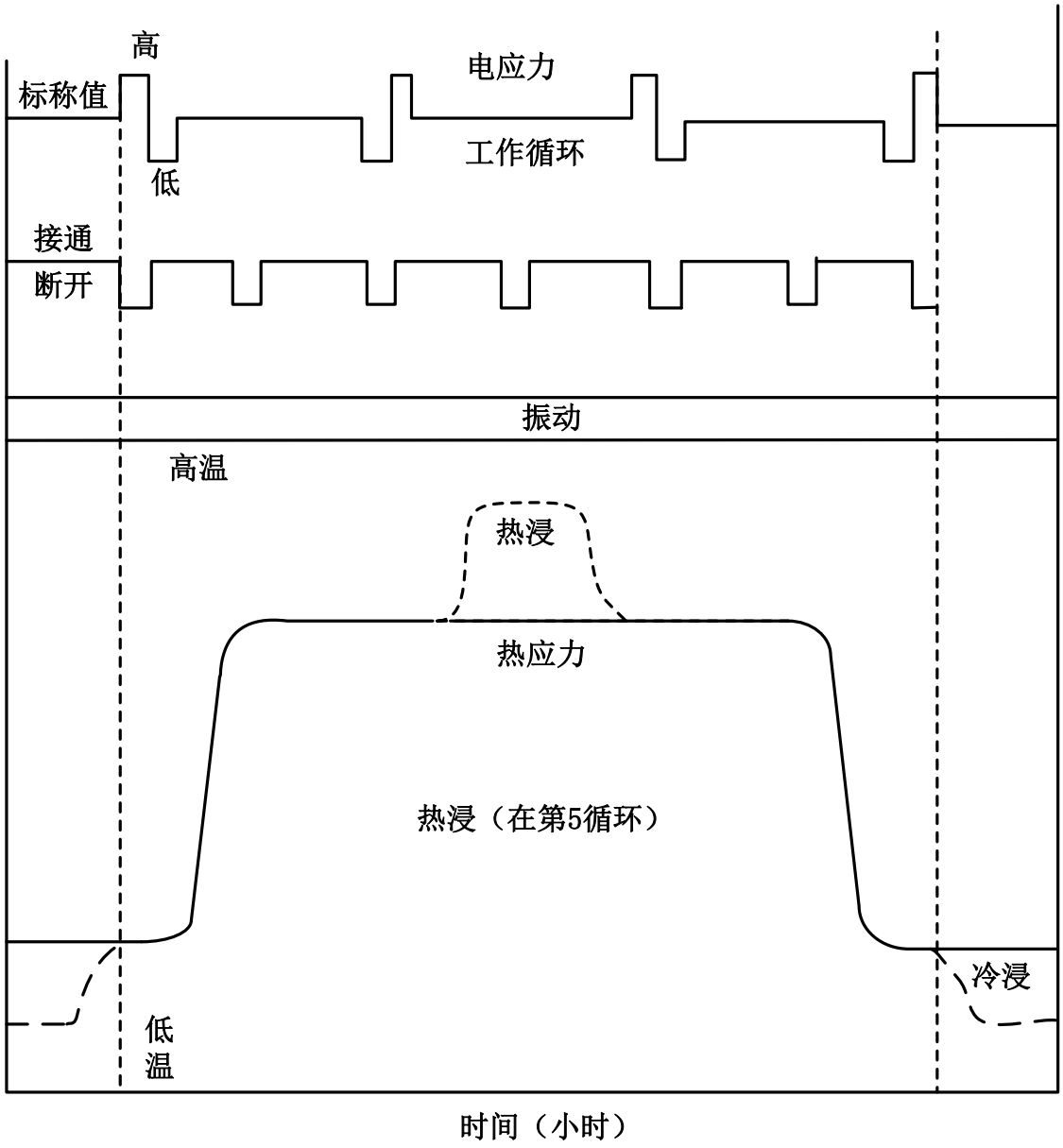
(1) 产品在实际使用中执行典型任务剖面时，在受试产品安装位置附近测得的数据；

(2) 在相同或者相似工作环境、物理环境和保障环境中使用的相同或者类似产品数据；

(3) 产品在预期使用环境条件下的物理和工程分析数据；

(4) 产品供应商的试验数据或者行业内通用的数据源，使用此类通用数据源应考虑参数的置信度，并通过产品使用过程中，不断迭代获取更好的替换数据。

对于船舶设备与系统的产品综合环境试验剖面，除非船东或者用户方另有规定，试验箱温度变化速率至少为 5℃/min。根据设备与系统安装部署和使用环境，热浸和冷浸可以选做，此时，振动、电应力和工作循环都不施加，冷浸时，湿度应达到足以引起明显的冷凝、结霜和结冰的水平。



附图 2 船舶设备与系统可靠性测试验证剖面示例

附录 3　可靠性验证试验实施要求

1　概述

1.1　试验目的与分类

可靠性验证试验的目的是验证产品的可靠性是否达到规定的要求。

可靠性验证试验根据产品的性质分为可靠性鉴定试验和可靠性验收试验。

可靠性鉴定试验是为了验证新开发产品的设计是否达到规定的最低可接收的可靠性定量要求。

可靠性验收试验是对正式转入批生产产品是否达到可靠性定量要求的试验。

1.2　统计概念

可靠性指标是产品性能的时间表征，是随机变量，无法用仪表检测，只有通过抽样试验或全寿命统计才能检验。

产品的可靠性使用指标，也是可靠性目标值，在合同中又称规定值，试验方案中可为样本值 θ_0。

产品必须达到的可靠性使用指标称可靠性门限值，在合同中叫最低可接受值，试验方案中为 θ_1。

可靠性验证试验方案建立在统计数学基础上，与“个体”、“总体”、“批”、“样本”、“样本量”、“随机抽取”、“分布”等统计概念有关。

1.3　一般要求

试验大纲必须经过产品生产方、试验场所和船级社的代表共同讨论批准。

统计试验方案由产品使用方在合同中规定，从有关标准中选定，推荐 GJB899a-2009，GB/T 5080.1-2012/IEC 60300-3-5:2001。

试验样品的技术状态应是经过批准的。

试验剖面应代表实际使用环境条件。

试验应在试验大纲确定的试验场所进行，必要时，由中国船级社进行现场见证。

2　可靠性验证试验大纲要求

2.1　试验大纲内容要求

可靠性验证应包括但不限于以下内容；

试验对象和数量；

试验目的、进度；

试验方案；

试验条件：试验设备提供的应力及其容差、检测设备及其精度要求；

试验场所：在中国船级社接受的公认独立第三方检测和试验机构或根据特别情况商定确定的场所；

设置评审点、开展失效报告、分析和纠正措施系统（Failure Report Analysis and Corrective Action System，简称 FRACAS）要求。

2.2　试验方案要求

2.2.1　根据大纲要求制定试验方案

试验方案内容包括：

试验项目；

选定统计试验方案：号码、鉴别比 D、风险 α 和 β、试验时间 T、样品数量、是否可替换；

试验剖面；

失效判据及分类；

有关试验方职责分工；

计划进度、经费、人员、维修器材等资源保证条件；

其它可靠性活动信息。

2.2.2 试验方案选定因素

定时截尾试验，累积试验时间是确定的，便于试验计划安排和管理，但不一定是最经济的。

定数截尾试验，累计相关故障数是确定的，在采取不可替换的试验时，样品数量是也确定的，也不一定是最经济的。

等概率比序贯试验，做出判据所需的故障数和累计试验时间比定时截尾和定数截尾试验的少，事前只能确定它们的最大值，但样品数量和试验时间难以确定，不便于试验计划安排和管理，最大累积试验时间和累计故障数有可能超过定时截尾或定数截尾的试验。

综上，试验方案选定应由两方（生产方或使用方）协商确定。

2.3 试验条件

可靠性验证试验剖面应代表产品的典型使用条件：

功能模式，当产品有超过 1 种使用模式时，应分析各自所占时间的百分比，确定模式转换的方式，提出试验用典型工作模式；

输入要求，试验中测试设备向样品输入一系列信号，使样品正常工作；

负载条件，样品输出端应模拟使用状态加载，测试样品输出性能；

样品操作，试验中由产品操作人员模拟使用状态进行操作；

保障条件，实验室提供的电源、水源、气源等的各项参数应符合要求；

试验剖面，尽量采用综合应力试验设备模拟产品使用条件，同时对样品施加温度、湿度、振动、气压等综合应力；

样品维护和修理，试验大纲可能规定样品有定期维护的程序，应按照产品使用说明正常维护，不得改变其技术状态；样品发生故障，应准予修理，产品生产方应保证条件并实施，不得改变样品技术状态。

2.4 试验程序

应根据试验方案制定试验程序，经使用方审批后作为落实试验计划的文件，内容包括：

试验过程；

样品及其技术状况；

需检测的特性参数、故障判据及其容限、检测时段及方法；

综合环境条件及其容差；

试验日志及记录的数据内容、记录时间间隔要求；

故障记录表格及其登记内容、分析报告要求；

中断试验的规定，包括定期维护时间、故障发生之后、试验条件超出容限无法纠正时、其他管理需要时的各种情况；

样品故障的处置程序，包括及时记录故障现象和发生的应力条件及操作动作、确认故障、报告试验负责人、在温度到达常温点中断试验、取出故障样品、修理样品或继续试验（在不可替换方案中，待样品修理检测正常后；在可替换方案中，装上备份样品后）、分析故障明确是否关联、开展 FRACAS、记录故障处理过程。

2.5 试验评审

试验评审包括：试验大纲评审、试验方案评审、试验程序评审、试验准备状态评审、试验中评审、试验完成综合评审。前 4 项评审可以结合在一起进行，必要时由使用方和中国船级社代表参加；试验中评审视情况进行，如对故障处理和试验进度、序贯试验终结与否进行评审，由试验现场负责人组织实施；试验完成综合评审，应在试验报告编制完成之后进行，评价试验结果、产品可靠性水平及其接收与否的结论、FRACAS 报告、问题处置和纠正措施的落实等。

2.6 联合试验小组

联合试验小组由试验方、产品供应商、使用方（船东）代表和中国船级社代表组成，包括试验、总体、设计、生产、质量可靠性等专业人员；一般由试验方任组长、产品生产方和使用方代表任副组长，负责协调实施试验大纲，具体工作包括：执行试验评审和试验程序，审核试验数据，审批样品故障的分类和 FRACAS 的纠正措施，审批试验中断程序。

2.7 试验报告要求

试验报告是产品可靠性水平的正式记录，包括试验中产生的各种原始记录和试验结果的处理报告和结论意见，应形成完整的存档，并提交中国船级社。

附录 4　可靠性测试用例

附录 4 列举了一些可靠性测试用例的实例，可作为测试用例设计参考。其他测试用例参见 GB/T 28171-2011 附录 C。

1. **故障注入测试**

故障注入测试步骤如下：

(1) 故障注入。将缺陷、故障和失效插入到代码中去，需要确定插入的位置，必要时还要添加适当的代码；

(2) 执行测试。通过输入必要的数据、产生内部或外部事件、发送特定消息等方法，激活注入的故障；

(3) 测试结果收集。收集测试前设置的观察点处测试到的数据、现象等，同时收集被测系统出现的各种异常现象，如死机、复位等；

(4) 测试结果评估。根据测试过程中收集的测试数据，结合实际使用和设计需求，判断当前出现现象是否属于正常。一般采用以下两条准则判断是否需要启动修改流程：

① 故障注入后引起使用方不可接受的严重故障；

② 故障停止注入后系统无法恢复，仍处于故障状态。

2. **任务延时测试**

任务延时测试的目的是了解任务延时后对系统造成的影响是否满足要求。具体测试步骤如下：

(1) 在任务中加入空循环作延时处理，重新编译程序；

(2) 构造测试数据，激活被测任务；

(3) 观察系统的性能是否出现明显下降，是否出现其他的故障，任务之间的交互时序是否出现变化及这个变化带来了什么影响。

3. **频繁中断**

频繁中断的测试步骤如下：

(1) 测试出被测中断的一次正常中断的执行时间（t_1）；

(2) 找到中断源对应的引脚，在引脚上插入中断信号发生器的输入信号，调节中断间隔时间（t_2）；

(3) 继续降低中断信号的时间间隔，使 $0.5t_1>t_2>0.25t_1$，即在处理中断服务程序时发生 2 个中断请求，观察系统运行情况；

(4) 在中断服务程序中增加中断计数变量，重新编译运行。正常运行后，利用中断信号发生器在很短的时间内快速发送 1000 个中断，观察系统运行情况。

4. **重复中断**

重复中断的测试步骤如下：

(1) 修改代码，在响应中断时，调用多次中断服务程序，重新编译程序；

(2) 按照实际条件触发该中断，观察程序的运行情况。

5. **中断丢失**

中断丢失的测试步骤如下：

(1) 修改中断服务程序，在入口处有选择性或随机地直接返回，重新编译程序；

(2) 按照实际条件触发该中断，观察系统的运行情况。

6. **中断挂起**

中断挂起的测试步骤如下：

(1) 运行程序，使被测程序正常运行，然后清除被测中断的使能位，关闭中断；

(2) 按照实际条件触发该中断，观察系统的运行情况。

7. **中断服务历程延时**

中断服务历程延时的测试步骤如下：

(1) 在中断服务历程中加入空循环，重新编译程序；

(2) 按照实际条件触发中断，使被测的中断服务历程能够被执行；

(3) 观察系统的运行情况。

8. **单板启动过程中触发所有中断测试**

单板启动过程中触发所有中断的测试步骤如下：

(1) 选择增加测试代码的位置；

(2) 在(1)中选择的位置增加一条死循环语句，死循环内部增加一个计数器或者增加一个闪灯的操作，重新编译程序；

(3) 在程序进入该死循环后，逐一触发所有中断源，检查是否异常，检查计数器值是否在增加或者灯是否在继续闪亮；

(4) 选择其他中断语句之后的位置，重复(2)和(3)，直到所有开中断语句均被测试过。

9. **触发未使用中断测试**

触发未使用中断的测试步骤如下：

(1) 屏蔽所有未使用的中断源；

(2) 运行程序，模拟实际条件触发所有未使用中断；

(3) 观察程序运行状态，检查是否发生异常；

(4) 检查中断标志位是否被置位。

10. **接口数据长度错误测试**

接口数据长度错误的测试步骤如下：

(1) 修改代码，可从后台直接发送十六进制格式的消息，重新编译程序并运行；

(2) 发送 0 长度消息，即长度域的值为 0，观察程序的处理情况；

(3) 发送超长消息，即长度值超过允许的最大值，观察程序的运行情况；

(4) 发送消息内容中的长度域，使其值在允许范围之外，观察程序的运行情况。

11. **接口数据类型错误测试**

接口数据类型错误的测试步骤如下：

(1) 修改代码，可从后台直接发送十六进制格式的消息，重新编译程序并运行；

(2) 发送消息类型为允许范围外的消息，观察程序的处理情况。

12. **数据错误测试**

数据错误的测试步骤如下：

(1) 修改代码，可从后台直接发送十六进制格式的消息，重新编译程序并运行；

(2) 发送消息类型为允许范围外的消息，观察程序的处理情况。

13. **消息数据的一致性错误测试**

消息数据的一致性错误测试步骤如下：

(1) 修改代码，可从后台直接发送十六进制格式的消息，重新编译程序并运行；

(2) 发送消息类型为允许范围外的消息，观察程序的处理情况。

14. **消息丢包测试**

消息丢包测试步骤如下：

(1) 在程序中加入适当的代码，从原消息流中截取通过的所有消息，然后按一定的比率强制释放这些消息，比率可以动态调整，重新编译程序；

(2) 运行程序，构造一些输入，使程序内部有消息流动，从小到大然后再从大到小调整丢包比率，观察系统的运行情况；
(3) 关闭丢包功能，消除丢包故障，观察系统的运行情况，检查系统的各模块状态是否一致，能否恢复正常运行状态。

15. **软误码测试**

由于软件错误造成传输数据被修改的过程称为软误码。软误码测试步骤如下：
(1) 增加测试代码，截取消息流中的消息包，按照一定的比率强制修改消息数据，重新编译程序；
(2) 构造适当的输入，使步骤(1)中的消息流中有消息经过；
(3) 观察系统的运行情况，检查系统是否出现告警、内存越界、死机，检查内部的各相关模块状态是否一致；
(4) 关闭误码程序，观察系统的运行情况，检查系统是否可以恢复正常运行。

16. **消息延时测试**

消息延时测试步骤如下：
(1) 修改代码，增加适当的程序，从消息通路上截取消息，将这些消息发送到延时队列中，经过一段时间后，再将这些延时队列中的消息按原来的时间间隔发送出去，相当于每一个消息都延长了一个相同的时间。延时的时间可以调节；
(2) 重新编译程序，构造测试输入数据，使被测的消息流中有消息经过；
(3) 调节消息的延时时间，观察系统的运行情况。

17. **消息重包测试**

消息重包测试步骤如下：
(1) 在消息流通路上选择适当的位置，增加测试代码，按照某一规则复制通过的消息，如按照某一比率或按照某一特征进行复制；
(2) 重新编译程序，构造测试输入数据，使被测的消息流中有消息经过；
(3) 观察程序的运行情况。

18. **消息乱序测试**

消息乱序测试步骤如下：
(1) 在消息流通路上选择适当的位置，增加测试代码，实现消息的顺序扰动；
(2) 重新编译程序，构造测试输入数据，使被测的消息流中有消息经过；
(3) 观察程序的运行情况；
(4) 停止消息的顺序扰动，观察系统的运行情况。

19. **突发大流量测试**

突发大流量测试步骤如下：
(1) 搭建好工具或增加适当的测试代码，实现向被测系统随意发送任意流量的消息或数据；
(2) 运行程序，配置被测链路，为了达到最大的处理量，尽可能将所有可以输入系统的端口打开并给予对应的输入；
(3) 调整流量达到最大，运行一段时间后，将流量调整到较低的水平运行一段时间，然后再次将流量调整到最大。如此反复多次，观察系统的运行情况。

20. **长时间大流量测试**

长时间大流量测试步骤如下：
(1) 搭建好工具或增加适当的测试代码，实现向被测系统随意发送任意流量的消息或数据；
(2) 运行程序，配置被测链路，为了达到最大的处理量，尽可能将所有可以输入系统的

端口打开并给予对应的输入；

(3) 调整流量达到最大并长时间运行，观察系统的运行情况。当运行时间达到规定的时间后，降低流量到 0，观察系统的运行情况。

附录 5　可靠性示图绘制

在采用可靠性示图确认测试时，为绘制可靠性示图，需要求出继续和接受边界、继续和拒绝边界，并绘出边界线，本指南推荐按下列方法绘制可靠性示图。

n=0 时的 T_N，与横轴的交点：

$$T_{N,A}(n)=\frac{A}{1-\gamma}$$

$$T_{N,B}(n)=\frac{B}{1-\gamma}$$

n=16 时的 T_N，与横轴的交点：

$$T_{N,A}(16)=\frac{A-16\ln\gamma}{1-\gamma}$$

$$T_{N,B}(16)=\frac{B-16\ln\gamma}{1-\gamma}$$

T_N=0 时，与纵轴的交点：

$$n_A(0)=\frac{A}{\ln\gamma}$$

$$n_B(0)=\frac{B}{\ln\gamma}$$

T_N=16 时，与纵轴的交点：

$$n_A(16)=\frac{A-16(1-\gamma)}{\ln\gamma}$$

$$n_B(16)=\frac{B-16(1-\gamma)}{\ln\gamma}$$

为使用方便，典型的参数见下表：

区域与边界的各个横轴和纵轴的交点值　　附表 5(1)

交点位置	分辨率 γ		
	2	1.5	1.1
n=0 点的横轴	-A,-B	-2A,-2B	-10A,-10B
n=16 点的横轴	-A+11.1,-B+11.1	-2A+13.0,-2B+13.0	-10A+15.2,-10B+15.2
T_N=0 点的纵轴	1.44A,1.44B	2.47A,2.47B	10.5A,10.5B
T_N=16 点的纵轴	（A+16）/0.693 （B+16）/0.693	（A+8）/0.405 （B+8）/0.405	（A+1.6）/0.0953 （B+1.6）/0.0953

各种生产方风险和使用方风险水平条件下的 A 值和 B 值　　附表 5(2)

生产方风险	参数	使用方风险			
		0.1	0.05	0.01	0.001
0.1	A	-2.20	-2.89	-4.50	-6.80
	B	2.20	2.25	2.29	2.30
0.05	A	-2.25	-2.94	-4.55	-6.86
	B	2.89	2.94	2.99	2.99

生产方风险	参数	使用方风险			
		0.1	0.05	0.01	0.001
0.01	A	-2.29	-2.99	-4.60	-6.90
	B	4.50	4.55	4.60	4.60
0.001	A	-2.30	-2.99	-4.60	-6.91
	B	6.80	6.86	6.90	6.91

由附表 5(2)所示，A 随使用方风险迅速变化，但随生产方风险变化很小，它决定接受边界与横轴线在 n=0 的交点，因此接受边界会随使用方风险急剧变化，随生产方风险有很小的变化。B 随生产方风险迅速变化，但随使用方风险变化很小，它决定拒绝边界与纵轴线在 T_N=0 的交点，因此拒绝边界会随生产方风险急剧变化，随使用方风险有很小的变化。

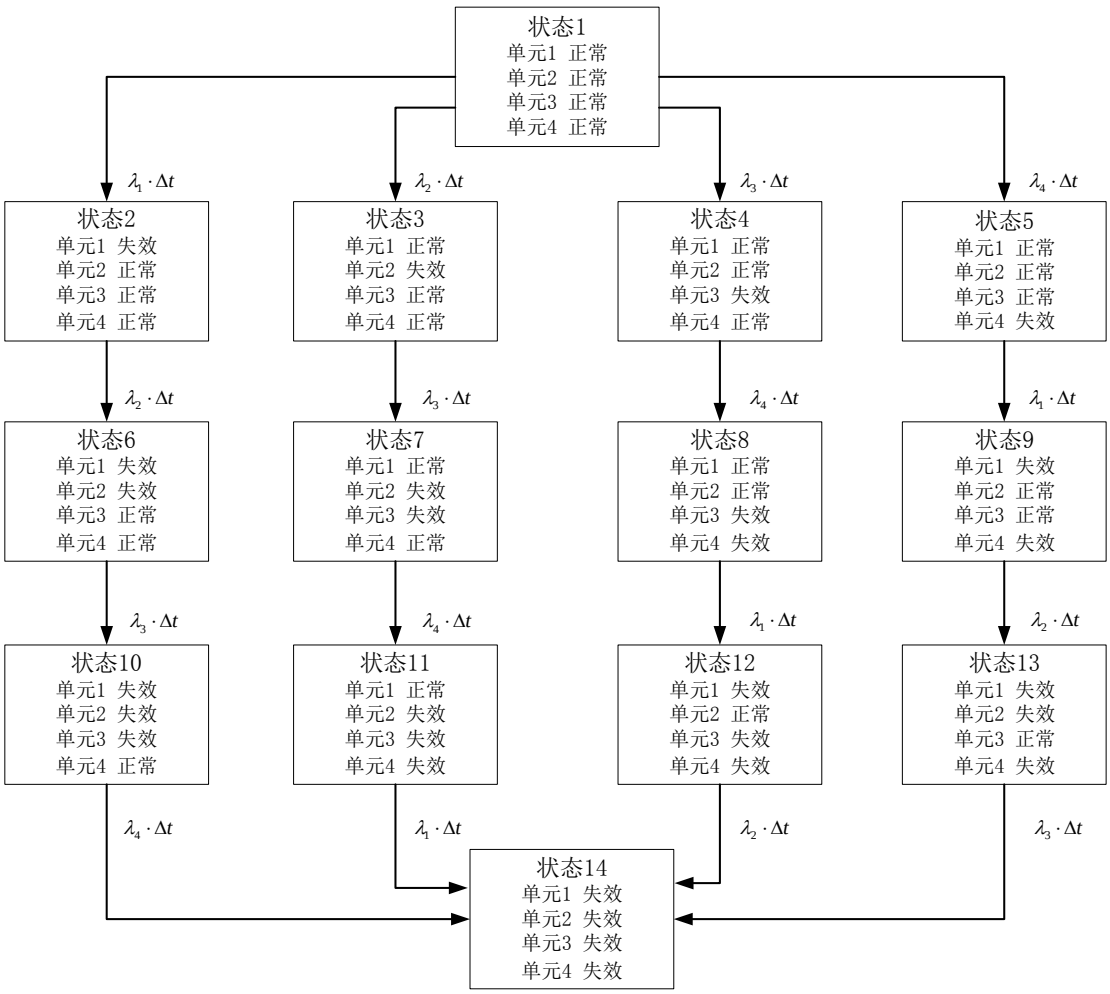
在确认测试时，可以根据需要，绘制出所需要的使用方风险和生产方风险所有组合的可靠性示图，也可以只绘制出使用方和生产方风险对称的可靠性示图。当二者风险不对称时，可采用足够近似的图。

随着分辨率、使用方风险水平或生产方风险水平的降低，继续区域会拓宽。因此如果要降低在估计失效强度中所能够容忍的错误，或降低错误决策的风险，达到拒绝或接受区域则需要开展更多的测试。

附录 6　MARKOV 模型及其可靠性评估计算

本附录给出了一种 4 单元 MARKOV 模型示例；在此模型中，假设每一个单元有两种状态：正常和失效，则该模型的状态根据每一单元的这两种状态组合而成，假定每一个单元均有恒定失效率 λ，其失效状态转移概率近似为 $\lambda\ \Delta t$, 在 t 时刻两种及以上的单元失效模式忽略。

则该 MARKOV 模型过程的状态转移图如图所示：



附图 6(1)　4 单元 MARKOV 模型状态转移图

MARKOV 微分方程是通过给出每个状态的概率 P 来展开，系统的行为表征为无记忆，即系统的将来状态除与最近以前的一个状态有关外，与过去所有状态无关，因此系统将来的随机特性只取决于现在，而不取决于过去，也不取决于如何到达现在的状态，即从一个给定的状态向另一个状态转移的概率，在过去和将来的所有时间里都必须相同的（平稳的）。基于以上 MARKOV 过程得到该四元 MARKOV 模型的方程如下；

$$
\begin{cases}
P_1(t+\Delta t)=P_1(t)\left[1-\left(\lambda_1+\lambda_2+\lambda_3+\lambda_4\right)\Delta t\right] \\
P_2(t+\Delta t)=P_1(t)\lambda_1\Delta t+\left[1-\left(\lambda_2+\lambda_3+\lambda_4\right)\Delta t\right]P_2(t) \\
P_3(t+\Delta t)=P_1(t)\lambda_2\Delta t+\left[1-\left(\lambda_1+\lambda_3+\lambda_4\right)\Delta t\right]P_3(t) \\
P_4(t+\Delta t)=P_1(t)\lambda_3\Delta t+\left[1-\left(\lambda_1+\lambda_2+\lambda_4\right)\Delta t\right]P_4(t) \\
P_5(t+\Delta t)=P_1(t)\lambda_4\Delta t+\left[1-\left(\lambda_1+\lambda_2+\lambda_3\right)\Delta t\right]P_5(t) \\
P_6(t+\Delta t)=P_2(t)\lambda_2\Delta t+\left[1-\left(\lambda_3+\lambda_4\right)\Delta t\right]P_6(t) \\
P_7(t+\Delta t)=P_3(t)\lambda_3\Delta t+\left[1-\left(\lambda_1+\lambda_4\right)\Delta t\right]P_7(t) \\
P_8(t+\Delta t)=P_4(t)\lambda_4\Delta t+\left[1-\left(\lambda_1+\lambda_2\right)\Delta t\right]P_8(t) \\
P_9(t+\Delta t)=P_5(t)\lambda_5\Delta t+\left[1-\left(\lambda_2+\lambda_3\right)\Delta t\right]P_9(t) \\
P_{10}(t+\Delta t)=P_6(t)\lambda_3\Delta t+\left[1-\lambda_4\Delta t\right]P_{10}(t) \\
P_{11}(t+\Delta t)=P_7(t)\lambda_4\Delta t+\left[1-\lambda_1\Delta t\right]P_{11}(t) \\
P_{12}(t+\Delta t)=P_8(t)\lambda_1\Delta t+\left[1-\lambda_2\Delta t\right]P_{12}(t) \\
P_{13}(t+\Delta t)=P_9(t)\lambda_2\Delta t+\left[1-\lambda_3\Delta t\right]P_{13}(t) \\
P_{14}(t+\Delta t)=P_{10}(t)\lambda_4\Delta t+P_{11}(t)\lambda_1\Delta t+P_{12}(t)\lambda_2\Delta t+P_{13}(t)\lambda_3\Delta t+1.P_{14}(t)
\end{cases}
$$

代入初始状态条件参数，则有：

$$P_1(0)=1,\ P_2(0)=0,\ \cdots,\ P_{14}(0)=0$$

得到如下等式：

$$
\begin{cases}
P_1(t)=e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} \\
P_2(t)=-e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+e^{-(\lambda_2+\lambda_3+\lambda_4)t} \\
P_3(t)=-e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+e^{-(\lambda_1+\lambda_3+\lambda_4)t} \\
P_4(t)=-e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+e^{-(\lambda_1+\lambda_2+\lambda_4)t} \\
P_5(t)=-e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+e^{-(\lambda_1+\lambda_2+\lambda_3)t} \\
P_6(t)=\dfrac{\lambda_2}{\lambda_1+\lambda_2}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}-e^{-(\lambda_2+\lambda_3+\lambda_4)t}+\dfrac{\lambda_2}{\lambda_1+\lambda_2}e^{-(\lambda_3+\lambda_4)t} \\
P_7(t)=\dfrac{\lambda_3}{\lambda_2+\lambda_3}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}-e^{-(\lambda_1+\lambda_3+\lambda_4)t}+\dfrac{\lambda_2}{\lambda_2+\lambda_3}e^{-(\lambda_1+\lambda_4)t} \\
P_8(t)=\dfrac{\lambda_4}{\lambda_3+\lambda_4}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}-e^{-(\lambda_1+\lambda_2+\lambda_4)t}+\dfrac{\lambda_1\lambda_4}{\lambda_4\lambda_3+\lambda_4}e^{-(\lambda_1+\lambda_2)t} \\
P_9(t)=\dfrac{\lambda_1}{\lambda_1+\lambda_4}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}-e^{-(\lambda_1+\lambda_2+\lambda_3)t}+\dfrac{\lambda_3}{\lambda_1+\lambda_4}e^{-(\lambda_2+\lambda_3)t} \\
P_{10}(t)=-\dfrac{\lambda_2\lambda_3}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+\dfrac{\lambda_3}{\lambda_2+\lambda_3}e^{-(\lambda_2+\lambda_3+\lambda_4)t}-\dfrac{\lambda_1\lambda_4}{\lambda_4(\lambda_2+\lambda_3)}e^{-(\lambda_1+\lambda_4)t} \\
\qquad +\left[\dfrac{\lambda_2\lambda_3}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)}-\dfrac{\lambda_3}{\lambda_2+\lambda_3}+\dfrac{\lambda_1\lambda_4}{\lambda_4(\lambda_2+\lambda_3)}\right]e^{-\lambda_4 t} \\
P_{11}(t)=-\dfrac{\lambda_3\lambda_4}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+\dfrac{\lambda_4}{\lambda_3+\lambda_4}e^{-(\lambda_1+\lambda_3+\lambda_4)t}-\dfrac{\lambda_2\lambda_3}{\lambda_3(\lambda_1+\lambda_2)}e^{-(\lambda_1+\lambda_3)t} \\
\qquad +\left[\dfrac{\lambda_3\lambda_4}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)}-\dfrac{\lambda_4}{\lambda_3+\lambda_4}+\dfrac{\lambda_2\lambda_4}{\lambda_4(\lambda_2+\lambda_3)}\right]e^{-\lambda_1 t} \\
P_{12}(t)=-\dfrac{\lambda_1\lambda_4}{(\lambda_3+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+\dfrac{\lambda_1}{\lambda_1+\lambda_4}e^{-(\lambda_1+\lambda_3+\lambda_4)t}-\dfrac{\lambda_1\lambda_3}{\lambda_1(\lambda_3+\lambda_4)}e^{-(\lambda_1+\lambda_2)t} \\
\qquad +\left[\dfrac{\lambda_1\lambda_4}{(\lambda_3+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}-\dfrac{\lambda_1}{\lambda_1+\lambda_4}+\dfrac{\lambda_1\lambda_3}{\lambda_1(\lambda_3+\lambda_4)}\right]e^{-\lambda_2 t} \\
P_{13}(t)=-\dfrac{\lambda_1\lambda_2}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_2+\lambda_4)}e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}+\dfrac{\lambda_2}{\lambda_1+\lambda_2}e^{-(\lambda_1+\lambda_2+\lambda_3)t}-\dfrac{\lambda_2\lambda_4}{\lambda_2(\lambda_1+\lambda_4)}e^{-(\lambda_2+\lambda_3)t} \\
\qquad +\left[\dfrac{\lambda_1\lambda_2}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_2+\lambda_4)}-\dfrac{\lambda_2}{\lambda_1+\lambda_2}+\dfrac{\lambda_2\lambda_4}{\lambda_2(\lambda_1+\lambda_4)}\right]e^{-\lambda_3 t} \\
P_{14}(t)=1-P_1(t)-P_2(t)-\cdots-P_{13}(t)
\end{cases}
$$

则系统在 t 时间的可靠度为，

$$R(t)=\sum_{i=1}^{n-1}P_i(t)\text{，}\ n=14$$

代入计算得，

$$R(t) = -3e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}\left[\frac{\lambda_2}{\lambda_1+\lambda_2+\lambda_3} + \frac{\lambda_3}{\lambda_2+\lambda_3+\lambda_4} + \frac{\lambda_4}{\lambda_1+\lambda_3+\lambda_4} + \frac{\lambda_1}{\lambda_1+\lambda_2+\lambda_4}\right]$$
$$+ e^{-(\lambda_2+\lambda_3+\lambda_4)t}\left(\frac{\lambda_3}{\lambda_2+\lambda_3}\right) + e^{-(\lambda_1+\lambda_2+\lambda_4)t}\left(\frac{\lambda_1}{\lambda_1+\lambda_4}\right) + e^{-(\lambda_1+\lambda_2+\lambda_3)t}\left(\frac{\lambda_2}{\lambda_1+\lambda_2}\right)$$
$$+ e^{-(\lambda_1+\lambda_3+\lambda_4)t}\left(\frac{\lambda_4}{\lambda_3+\lambda_4}\right) + \left[\frac{\lambda_1\lambda_2}{(\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3)}\right]e^{-\lambda_4 t} + \left[\frac{\lambda_2\lambda_3}{(\lambda_3+\lambda_4)(\lambda_2+\lambda_3+\lambda_4)}\right]e^{-\lambda_1 t}$$
$$+ \left[\frac{\lambda_3\lambda_4}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}\right]e^{-\lambda_2 t} + \left[\frac{\lambda_1\lambda_4}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_4)}\right]e^{-\lambda_3 t}$$

则系统的失效率为

$$F(t) = 1 - R(t)$$

系统的平均失效时间为

$$\mathrm{MTTF} = \int_0^\infty R(t)dt$$

$$\mathrm{MTTF} = -\frac{3}{\lambda_1+\lambda_2+\lambda_3+\lambda_4} + \frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_4}\left[\frac{\lambda_2}{\lambda_1+\lambda_2+\lambda_3} + \frac{\lambda_3}{\lambda_2+\lambda_3+\lambda_4} + \frac{\lambda_4}{\lambda_1+\lambda_3+\lambda_4} + \frac{\lambda_1}{\lambda_1+\lambda_2+\lambda_4}\right]$$
$$+ \frac{\lambda_3}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)} + \frac{\lambda_1}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_2+\lambda_4)} + \frac{\lambda_2}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)} + \frac{\lambda_4}{(\lambda_3+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}$$
$$+ \frac{\lambda_1\lambda_2}{\lambda_4(\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3)} + \frac{\lambda_2\lambda_3}{\lambda_1(\lambda_3+\lambda_4)(\lambda_2+\lambda_3+\lambda_4)} + \frac{\lambda_3\lambda_4}{\lambda_2(\lambda_1+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}$$
$$+ \frac{\lambda_1\lambda_4}{\lambda_3(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_4)}$$

附录 7　符合性证明样例

中　国　船　级　社
CHINA CLASSIFICATION SOCIETY　Job No. _____

可靠性验证符合性证明
COMPLIANCE CERTIFICATE FOR RELIABILITY VERIFICATION

申请方
Applicant _____

产品名称
Item _____

型号/版本 _____
Model/Version

兹证明上列船舶设备与系统业经本社按照有关规定进行了测试和评估，确认

1. 此产品:可靠性验证满足本社《船舶设备与系统可靠性验证指南》对_____的要求（设备/计算机软件/嵌入式软件/系统）;
2. 此产品:引用环境参数严酷度为_____（如 6K2/6B2/6C3/6S1/6M4）。

THIS IS TO CERTIFY that the above mentioned equipment & system has been evaluated and tested by this Society and hereunder confirmed that:

1. The system is in compliance with Guide for reliability verification of equipment & system on _____(equipment/computer software/embedded software/system) ; and
2. The system in compliance with the Severity of environmental parameter_____ (Such as 6K2/6B2/6C3/6S1/6M4) .

地　点
Issued at _____

_____
中 国 船 级 社
CHINA CLASSIFICATION SOCIETY

时　间
Issued on _____