指导性文件
GUIDANCE NOTES
GD008-2025

中 国 船 级 社

船用软件安全及可靠性评估指南

2025.05

目 录

1 范围及说明

1.1 本指南是对船用计算机系统（以下简称计算机系统，包括可编程电子系统）中软件的安全及可靠性评估指南，对计算机系统中软件的设计、开发、测试、认证、维护提出了安全及可靠性要求。本指南也对与软件相关的硬件制定了一些要求，这些要求需与产品的技术要求结合使用。

1.2 本指南适用于智能船舶的计算机系统、旨在提高船舶智能化的计算机系统、以及基于可编程控制器的计算机系统。对于以下计算机系统，应根据本指南第 10 章的要求进行测试、验证和批准：

(1) 安装在入级船舶上、提供符合入级要求的控制、报警、监测、安全或内部通信功能的计算机系统；

(2) 拟取得 SLC1、SLC2、SLC3 附加标志的计算机系统。

本指南不适用于具有法定要求的计算机系统，例如：装载仪、稳性计算机、以及 SOLAS 公约第 IV 章和第 V 章规定的无线电通信设备和航行设备。

1.3 本指南主要关注软件开发生命周期，对整体安全生命周期中的一些环节也有所采用。本指南软件开发以 V 模型为例，其他相关模型的演化并未包含在本指南中。

1.4 考虑到小型简单的计算机系统的直接应用和在复杂系统中对部分功能实现的应用，本指南定义了小型低复杂度计算机系统，并在附录 2 给出了简化的评估方法。

1.5 在应用本指南时，可根据利益相关方内部文件管理系统编制本指南中提到的文件，但内容应符合指南中提及的相关内容。

1.6 本指南包括四个附录，其中：

1.6.1 附录 1 是现场验船师进行计算机系统中软件的安全及可靠性评估时使用的测试和验证表。

1.6.2 附录 2 是小型低复杂度计算机系统的评估方法。

1.6.3 附录 3 是计算机系统设计和实现阶段的技术建议。

1.6.4 附录 4 是开发阶段的软件测试要求。

2 引用文件

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

表 2.1　引用文件

1.	R001-2024	中国船级社《钢质海船入级规范》
2.	GD019-2024	中国船级社《电气电子产品型式认可试验指南》
3.	GB/T33783-2017	可编程逻辑器件软件测试指南
4.	IACS UR E22	计算机系统
5.	IEC 61508	电气/电子/可编程电子安全相关系统的功能安全
6.	IEC 61511	功能安全 安全仪表系统在过程工业中的应用
7.	IEC 60092-504	船舶电气设施 第504部分：专辑 自动化控制装置和仪器仪表
8.	IEC 60812	系统可靠性分析技术 故障模式影响分析
9.	IEC 61025	故障树分析
10.	IEEE 730	软件质量保证计划
11.	ISO 9001	质量管理体系要求
12.	ISO/IEC 90003	软件工程 计算机软件 ISO9001:2015 应用导则
13.	ISO/IEC 12207	系统和软件工程 软件生命周期过程
14.	ISO/IEC 15288	系统和软件工程 系统生命周期过程
15.	ISO 17894	船舶和海上技术 计算机应用 海上用可编程电子系统的开发和使用总则
16.	ISO/IEC 25000	系统和软件工程 系统和软件质量要求和评估（SQuaRE）SQuaRE 导则
17.	ISO/IEC 25041	系统和软件工程 系统和软件质量要求和评估（SQuaRE）开发者、受让人和独立评价者用评价指南
18.	ISO 10007	质量管理 配置管理指南
19.	ISO 24060	船舶和海洋技术 船舶操作技术软件记录系统

3　术语及缩略语

3.1 术语

3.1.1　软件（Software）

与计算机系统操作有关的计算机程序、规程、规则，以及可能有的文件、文档及数据。

3.1.2　软件安全性（Software safety）

软件安全性是指船用软件在面对潜在威胁和攻击时的保护能力，主要关注保护软件的机密性、完整性和可用性，以防止未经授权的访问、数据泄露、恶意篡改或服务中断。

3.1.3　软件可靠性（Software reliability）

软件可靠性是指船用软件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　计算机系统（Computer-based system）

一种可编程电子设备，或者一组可互操作的可编程电子设备，为达到一个或多个特定目的而组织起来，如信息的收集、加工、维护、使用、共享、传播或处置。船用计算机系统通常包括 IT 系统和 OT 系统。船用计算机系统可以是通过网络连接的子系统的组合体，直接或通过公共通信方式（如互联网）连接到岸上计算机系统、其他船舶的计算机系统和/或其他设施。

3.1.5 系统（System）

组件、设备和逻辑的组合体，具有明确的用途、功能和性能。计算机系统就是一种系统。在本指南中，系统特指计算机系统，由系统供应商交付。

3.1.6 子系统（Subsystem）

系统的可识别部分，可执行特定功能或一组功能。

3.1.7 集成系统（System of systems）

由多个计算机系统组成的系统。在本指南中，集成系统作为船舶的一部分，包括船厂交付的所有监测、控制和安全系统。

3.1.8 模块（Module）

可以分解、组合及更换的单元，是组成系统、并易于处理的基本单位。

3.1.9 软件模块（Software module）

软件中独立、具有特定功能且可以独立编译和执行的程序组件。它由程序代码和相关数据结构组成，可以使用特定的接口与其他模块进行交互。

3.1.10 软件组件（Software component）

一段独立的代码，提供特定且紧密耦合的功能。

3.1.11 软件主文件（Software master files）

构成软件初始源的计算机文件。对于定制软件来说，可能是可读的源代码文件，而对于现有商用软件来说，可能是不同形式的二进制文件。

3.1.12 软件结构（Software structure）

不同软件组件如何交互的概述，通常称为软件体系结构或软件层次结构。

3.1.13 软件注册表（Software registry）

用来登记船用软件的软件名称、版本号、开发完成日期、发布状态、变更记录等信息。

3.1.14 安全功能（Safety function）

针对特定的危险事件，为达到或保持安全状态，由计算机系统、其它技术安全相关系统或外部风险降低设施实现的功能。

3.1.15 受控设备（Equipment under control（EUC））

用于制造、加工、运输或其它活动的设备、机器、器械和/或成套装置。计算机系统可作为一种受控设备或受控设备的一部分。

3.1.16 小型低复杂度计算机系统（Small low complexity computer system）

一种计算机系统，其中：已很好确定了每个部件的失效模式，能完全确定在故障情况下的系统行为。

注：在故障状态下系统行为可用试验和/或分析的方法确定。

3.1.17 动态测试（Dynamic testing）

用系统的、受控的方式执行软件和/或操作硬件以证明所要求行为的存在，以及非要求行为的不存在。

3.1.18 质量计划（Quality plan）

对特定的项目、产品或合同，规定由谁及何时应使用哪些质量体系程序和相关资源的文件。

3.1.19 规程（Regulation）

在保证设备安全、人身安全的前提下，将工作程序贯穿一定的标准、要求和规定。

3.1.20 程序文件（简称：程序，Procedure）

程序是质量管理体系中质量手册的下一级文件层次，规定某项工作的一般过程。此处的程序，不同于计算机程序。

3.1.21 系统生命周期（System lifecycle）

指计算机系统从立项、开发、运维到消亡的整个过程。

3.1.22 软件生命周期（Software lifecycle）

从软件开始构思到软件永久停用的生存过程。

注：一个典型的软件生命周期包括需求、开发、测试、集成、安装、变更等阶段。

3.1.23 软件配置管理（Software Configuration Management，SCM）

是一种标识、组织和控制变更的技术，应用于整个软件生命周期。

3.1.24 可编程设备（Programmable device）

安装有软件的物理单元。

3.1.25 船舶（Vessel）

安装计算机系统的船只或近海设施。

3.1.26 利益相关方（Stakeholders）

能够影响、受到影响或认为自己受到决策或者活动影响的人或组织。

3.1.27　业主（Owner）

在船舶建造阶段，订购船舶的组织或个人；在船舶营运阶段，拥有或管理在役船舶的组织。在指南中，业主是一个具有明确职责的角色。

3.1.28　系统集成商（System integrator）

在计算机系统的整个生命周期，负责协调系统和子系统供应商之间互动的单个组织或个人，其目的是将系统和子系统集成到经过验证的全船范围内的集成系统中，并为计算机系统提供适当的操作和维护服务。在本指南中，系统集成商是一个具有明确职责的角色。在设计和交付阶段，船厂是默认的系统集成商；在营运阶段，业主是默认的系统集成商。

3.1.29　供应商（Supplier）

通用术语，指服务、系统组件或软件的签约提供商或者分包提供商，可以是组织，也可以是个人。

3.1.30　系统供应商（System supplier）

在系统集成商的协调下，提供系统组件或软件的承包商或分包商。系统供应商可以是组织，也可以是个人。在本指南中，系统供应商是一个具有明确职责的角色。

3.1.31　服务供应商（Service supplier）

非 IACS 成员雇佣的个人或公司，应设备制造商、船厂、业主或其他客户的要求，从事相关检查工作，为船舶（含海上移动平台）提供诸如安全系统和设备的测量、试验或检修之类的服务。船级社验船师在开展入级或法定认证服务时，会参考其提供的结果，再做出决定。

3.1.32　黑盒描述（Black-box description）

从系统外部观察到的关于系统功能、行为和性能的描述。

3.1.33　黑盒测试方法（Black-box test methods）

仅通过操纵输入和观察输出来验证系统、子系统或组件的功能、性能和鲁棒性。这不需要任何系统内部工作的知识，只需关注被测系统/组件的可观察行为，以达到所需的验证水平。

3.1.34　故障模式描述（Failure mode description）

描述系统故障（非系统支持设备的故障）造成的影响的文件，应涵盖以下方面：需要评估的故障列表，对每一个故障的系统响应，以及对每一个故障后果的评价。

3.1.35　参数化（Parameterization）

通过更改参数来配置调整系统和软件的功能，通常不需要计算机编程，由系统供应商或服务提供商完成，而不是由操作人员或终端用户完成。

3.1.36　鲁棒性（Robustness）

可以用于反映一个系统在面临内部结构或外部环境改变时也能够维持其功能稳定运行的能力。

3.1.37 模拟测试（Simulation test）

在进行监测、控制或安全系统测试时，受控设备部分或全部用模拟工具替代，或者通信网络和线路部分用模拟工具替代。

3.2 缩略语

3.2.1 ISO：International Organization for Standardization，国际标准化组织。

3.2.2 IEC：International Electrotechnical Commission，国际电工委员会。

3.2.3 IEEE：Institute of Electrical and Electronics Engineers，电气电子工程师学会。

3.2.4 FMEA：Failure Mode and Effects Analysis，故障模式及影响分析。

3.2.5 FMECA：Failure Mode, Effects and Criticality Analysis，故障模式及影响分析和危害性分析。

3.2.6 FAT：Factory Acceptance Test，工厂验收测试。

3.2.7 SAT：System Acceptance Test，系统验收测试。

3.2.8 SOST：System Of Systems Test 集成系统测试。

3.2.9 PE：Programmable Electronic，可编程电子。

3.2.10 COTS：Commercial Off-The-Shelf，商业成品。

3.2.11 IT：Information Technology，信息技术。

3.2.12 OT：Operational Technology，操作技术。

3.2.13 PMS：Planned Maintenance System，计划维护系统。

3.2.14 SSLS：Ship Software Logging System，船舶软件记录系统。

4 计算机系统分类

4.1 基于系统功能故障的影响，将计算机系统分成表 4.1 所示类别。

表 4.1 计算机系统分类

类别	影响	典型系统功能
I	这些系统的故障不会对人员的安全、船舶的安全以及环境产生危害。	- 监测、信息和管理功能。

II	这些系统的故障最终会对人员的安全、船舶的安全以及环境产生危害。	- 对保持船舶处于正常运营和起居状况所必要的报警、监测和控制功能。
III	这些系统的故障即刻会对人员的安全、船舶的安全以及环境产生危害或灾难。	- 保持船舶推进和操舵的控制功能； - 船舶安全功能。

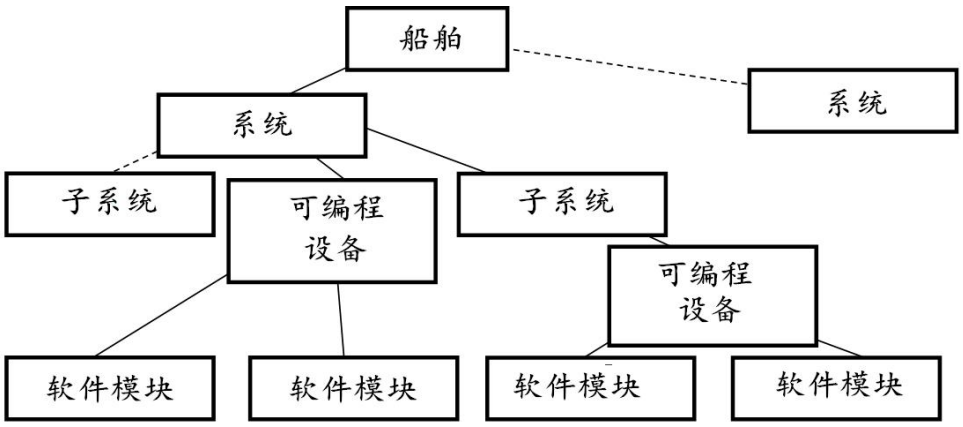
4.2 I 类系统通常不需要中国船级社（简称：CCS）的验证，因为这些系统的故障不会导致危险情况出现。但是，应提供与 I 类系统有关的信息，以确定系统分类的正确性，或确保 I 类系统不会影响 II 类和 III 类系统的运行。系统类别应始终结合具体船舶进行评估，因此计算机系统的分类会因船而异，表 4.2 的系统分类仅用作参考，且示例并未详尽。

表 4.2 系统分类举例

系统类别	举例
I	（1）燃油监测系统； （2）维修保障系统； （3）诊断和故障排除系统； （4）闭路电视； （5）客舱安全、娱乐系统； （6）鱼群探测系统。
II	（1）货物围护系统的控制、监测和安全系统； （2）舱底水探测和舱底泵相关控制； （3）燃油处理系统； （4）惰性气体系统； （5）压载水阀门遥控系统； （6）稳定和浮态控制系统，例如：减摇鳍控制系统； （7）推进机械和辅助机械的报警、监测和安全系统。
III	（1）推进控制系统，即产生和控制机械推力以移动船舶（不包含仅在操纵工况下使用的设备，例如：艏侧推）； （2）舵机控制系统； （3）电力系统（包括电力管理系统）； （4）船舶安全系统，包括探火和灭火、进水探测和排水、涉及撤离的内部通信系统、涉及救生设备操作的船舶系统； （5）附加标志 DP2 和 DP3 的动力定位系统； （6）钻井系统。

4.3 对象

4.3.1 计算机系统的典型层级结构和关系如下图所示。



注：图中虚线表示尚未开发的分支。

图 4.3.1　计算机系统层次结构图示

5　质量体系要求

5.1　质量保证体系

5.1.1　在计算机系统软硬件的设计开发阶段，以及在子系统、系统、集成系统的集成阶段，应采用全局自顶向下、跨越整个生命周期的管理方法。该方法应根据 CCS 接受的标准制定，并由 CCS 进行验证。

5.1.2　应通过质量保证体系证明系统供应商和系统集成商具有一定的产品质量保证能力和质量管理水平。系统供应商和系统集成商应制定能确保计算机系统符合 CCS 规范及相关公约的管理制度。

5.1.3　系统供应商和系统集成商应建立并实施 ISO9001 或等效标准的质量管理体系，并持有国家认可机构颁发的有效证书，或者由 CCS 通过特定评估来确认。系统供应商和系统集成商在开发计算机系统时，应遵循公认的质量标准，如 ISO9001 和 IEC/ISO90003 的规定。质量管理体系应至少包括以下内容：

表 5.1.3　质量管理体系

领域		角色	
序号	要求	系统供应商	系统集成商
1	员工的职责和能力。	x	x
2	软件和相关硬件的完整生命周期管理。	x	x
3	对计算机系统、组件、及其版本，进行唯一标识的具体程序。	x	
4	船舶计算机系统结构的创建和更新。		x
5	从供应商处采购软件和相关硬件的机构设置。	x	x
6	软件代码编写和验证的机构设置。	x	

7	船上集成之前负责系统验证的机构设置。	x	
8	在工厂验收测试和系统验收测试时，实施和批准系统的具体程序。	x	x
9	系统文档的创建和更新。	x	
10	船上软件修改和安装的具体程序，包括与船厂和业主的沟通流程。	x	x
11	软件代码的具体验证程序。	x	
12	计算机系统集成和集成系统测试的具体程序。	x	x
13	在工厂验收测试之前，软件和配置的变更管理程序。	x	
14	在工厂验收测试之后，软件和配置的变更管理及记录程序。	x	x
15	组织对自身遵守质量管理体系的跟踪检查点。检查点可以是一份要求提交的文件、一次测试、一次技术审查会或者专家评审会。	x	x

5.2　质量计划

5.2.1　系统供应商和系统集成商应制定针对系统生命周期的质量计划，其中包括软件质量计划。

5.2.2　软件质量计划应规范该软件在整个生命周期的活动，明确相关程序、职责和文件，包括配置管理。所制定的质量计划可参照 IEEE 730 的要求。

5.2.3　对于 II 类、III 类系统的软件，质量计划应包含安全功能要求部分，应设计具体保证方法，以验证和确认安全功能要求是否得到满足。

5.2.4　应制定计算机系统的配置管理，详见 5.7。

5.3　生产中质量控制

5.3.1　通过切实可行的质量保证措施、计划和组织，确保计算机系统的产品质量。

5.3.2　系统供应商和系统集成商应具有针对计算机系统的产品质量控制文件，该质量控制文件应准确描述计算机系统的开发流程或生产工艺流程，并用文字以及图表清晰描述各流程的质量控制要求；还应包含明确的控制对象、控制标准、控制方法、检验方法、以及生产质量保证措施落实的证明文件。对于安全相关功能的产品，还要求提供通过试验或测试的证明文件。

5.4　最终的试验报告

系统集成商应对计算机系统进行最终测试，并提供报告（如系统验收测试报告和集成系统测试报告）。

5.5　软件可追溯性

5.5.1　必须根据质量管理体系要求，对软件代码内容和数据的修改以及版本的变化进行标识并文档化。确保在需要时对软件产品质量的形成过程实行可追溯。通过软件配置管理及软件版本说明等质量保证文件，明确代码内容、数据的修改以及版本的变化所必须遵循的流程（特别是告知业主软件变更和船上安装的流程），并记录这些变更或变化。

5.5.2　这些文件应至少保存到软件退役后一年。系统集成商应有明确证据证明该软件确实退役。

5.6　安保策略

5.6.1　除非经授权，否则应不能修改软件。无论是物理系统或远程控制系统，都应采取物理和逻辑安保措施以防止未经授权的或无意的修改。

5.6.2　所有上船安装的固件、软件代码、可执行程序和物理媒介应在安装前进行漏洞、病毒、恶意软件等方面的安全扫描。安全扫描结果应记录在测试报告、软件注册表或同类文件中。

5.7　配置管理

5.7.1　配置管理的目的是保证当某些可交付项有改变时，几种开发的可交付项的一致性。一般来讲，配置管理包括硬件配置管理和软件配置管理。

5.7.2　要求：

(1) 在软件开发生命周期阶段，应使用行政和技术手段管理软件变更，并保证有关软件安全的规定要求（如安保策略）始终能得到满足。

(2) 应确保所有必需的操作已被执行，以满足相关软件需求。

(3) 应保持精确的和维护计算机系统完整性所必需的所有配置项的唯一识别性。配置项至少包括：安全分析和要求；软件需求文档和设计文档；软件源代码模块；应用于计算机系统软件组件和软件包的测试计划和测试结果；所有用于创建、测试或执行计算机系统软件的工具和开发环境。

(4) 应依据变更管理程序，采取物理和逻辑安保措施以防止未经授权的或无意的变更；变更请求应文档化；分析变更的影响以批准或拒绝请求；对所有准许变更的细节和授权应文档化；确保所有软件基线的构成（包括早期基线的重建）。

(5) 应对配置状态、发布状态、所有变更的判断和通过、变更的细节等信息文档化，以便接受审核。

(6) 软件的发布应文档化。软件的主要备份和所有相关文档在已发布软件的整个生命周期内应被保存，用于软件的维护和变更。

6 技术要求

6.1 系统标识

提供识别计算机系统名称、版本、标识和制造商的方法和应用。建议计算机系统按照国际标准 ISO24060 的规定，自动向船舶软件记录系统（SSLS）报告其软件状态。

6.2 数据链路

6.2.1 风险评估分析/FMEA 中应明确 II 类和 III 类计算机系统的数据链路失效状况，包括：

(1) III 类系统数据链路的单一故障不应导致船舶功能的丧失。此类故障的任何影响都应符合故障安全原则（fail-to-safe）。

(2) 对于 II 类和 III 类系统，远程控制系统的任何功能损失应能通过本地/手动方式进行补偿。

(3) 数据链路应具有防止或应对过高通信速率的手段。

(4) 数据链路应具有自检功能，能够检测到链路本身的故障或性能问题，以及连接到链路上的节点的数据通信故障。

(5) 检测到故障时应启动报警。

6.2.2 III 类系统不得使用无线数据链路，除非 CCS 依据可接受的国际或国家标准进行工程分析后特别考虑。其他类别的系统可使用无线数据链路，但应满足以下要求：

(1) 应使用认可的国际无线通信系统协议，并应满足以下要求：

a. 信息完整性：通过故障预防、检测、诊断和纠正，使接收的消息与发送的消息相比，不会被破坏或更改。

b. 配置和设备认证：应仅允许与系统设计中包含的设备连接。

c. 信息加密：保护机密和/或关键数据内容。

d. 安全管理：保护网络资产，防止非法访问网络资产。

(2) 船舶内部无线系统应满足国际电信联盟和船旗国主管机关对无线电频率和功率水平的要求。

(3) 系统操作应考虑到港口和当地法规在射频传输方面的规定，因频率和功率的限制而禁止使用无线数据通信链路。

(4) 无线数据通信设备应在系泊试验和航行试验期间进行测试，证明在预期的操作条件下，射频传输不会因电磁干扰引起自身和任何其他设备的故障。

6.3 CCS 验证

系统设计文档应说明计算机系统针对技术要求的符合程度。CCS 将会把技术要求的实施情况作为系统说明、工厂验收测试、系统验收测试的一部分进行验证。

7 文件要求

按要求应至少向 CCS 提交以下计算机系统的相关文件。

7.1 系统供应商应提交的基础文件：

序号	文件名称	系统类别		
		I 类系统	II 类系统	III 类系统
1	质量计划	Ⓘ（必要时）	Ⓘ	Ⓘ
2	系统说明	Ⓘ（必要时）	Ⓐ	Ⓐ
3	环境符合性测试报告	Ⓘ（必要时）	Ⓘ	Ⓘ
4	软件测试报告	Ⓘ（必要时）	Ⓘ（必要时）	Ⓘ（必要时）
5	系统测试报告	Ⓘ（必要时）	Ⓘ（必要时）	Ⓘ（必要时）
6	工厂验收测试程序	-	Ⓐ	Ⓐ
7	工厂验收测试报告	-	Ⓘ	Ⓘ
8	其他工厂验收测试文件（如用户手册等）	-	Ⓘ（必要时）	Ⓘ（必要时）
9	变更管理程序	Ⓘ（必要时）	Ⓘ	Ⓘ

注：表中采用的符号及其含义如下：Ⓐ 提交 CCS 批准；Ⓘ 提交 CCS 备查。

7.2 系统集成商应提交的基础文件：

序号	文件名称	系统类别		
		I 类系统	II 类系统	III 类系统
1	质量计划	Ⓘ（必要时）	Ⓘ	Ⓘ
2	系统类别清单	Ⓐ	Ⓐ	Ⓐ
3	风险评估报告	Ⓐ（必要时）	Ⓐ（必要时）	Ⓐ（必要时）
4	系统结构说明	Ⓘ	Ⓘ	Ⓘ
5	系统验收测试程序	-	Ⓐ	Ⓐ
6	系统验收测试报告	-	Ⓘ	Ⓘ

7	集成系统测试程序	-	Ⓐ	Ⓐ
8	集成系统测试报告	-	Ⓘ	Ⓘ
9	软件变更管理程序	Ⓘ（必要时）	Ⓘ	Ⓘ

注：表中采用的符号及其含义如下：Ⓐ 提交 CCS 批准；Ⓘ 提交 CCS 备查。

8 系统生命周期

8.1 系统生命周期的划分

8.1.1 系统生命周期划分为五个阶段，分别为概念、需求、实现、验证、运行。每个阶段根据目的和范围的不同又做了划分，其关系和要求见下表和图。

注：在系统生命周期内，IEC61508 通常认为计算机系统是一种受控设备。

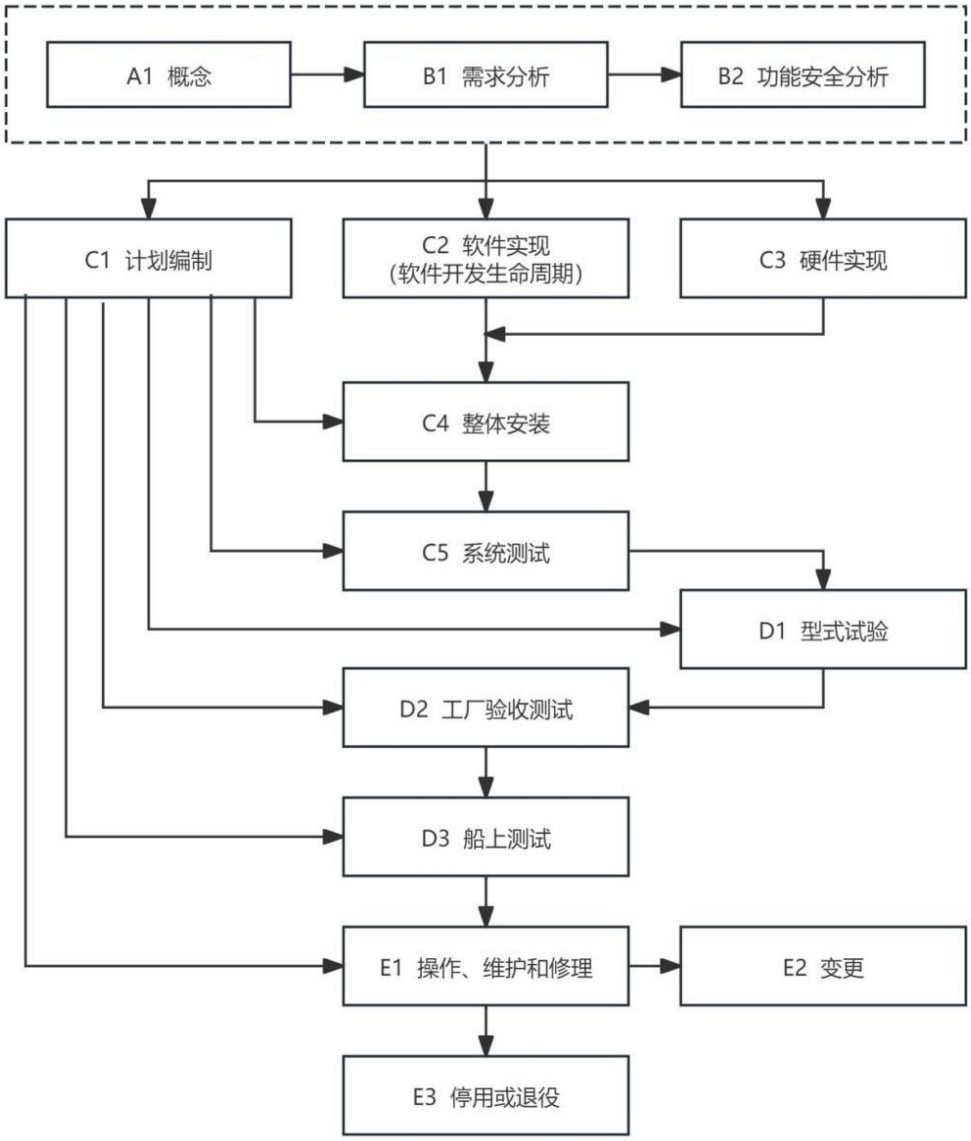


图8.1.1 系统生命周期

表8.1.1　系统生命周期概述

系统生命周期阶段		目的	要求	输入	输出
图8.1.1方框号	标题				
A 概念					
A1	概念	提高对计算机系统及其环境（实际的、法律的等）的理解水平，以更好地执行其生命周期活动。	对计算机系统及其要求的控制功能和实际环境进行全面的了解；确定可能的危险源；获取确定危险的有关信息；获取当前的安全法规；考虑相邻近的受控设备之间相互作用所产生的危险；以上所要求的信息和结果应文档化。	满足该条要求所必需的全部相关信息。	从概念至整体范围获取的信息。
B 需求					
B1	需求分析	在新建或修改计算机系统时，描写系统的目的、范围、定义和功能时所要做的全部工作，包括： (1) 确定计算机系统的边界； (2) 规定安全分析的范围。		从概念至整体范围获取的信息。	系统需求规格说明。
B2	功能安全分析	为了保证计算机系统的安全可靠性，证明对于单一故障，系统应进入故障安全状态，并且运行中的系统功能不会丢失或降低到不能满足 CCS 规定的可接受性能标准。		系统需求规格说明。	安全相关功能要求文档（包含安全要求分配的信息和记录）。
C 实现					

C1	计划编制	明确在规定规程和技术方面的工作步骤，证明计算机系统满足安装、操作和维护要求。	拟定计算机系统的安装、操作和维护计划，以确保在操作和维护过程中保持所要求的功能安全。 拟定工厂验收测试程序和船上测试程序（包括系统验收测试程序和集成系统测试程序），测试程序中需包括安全相关功能试验。	系统需求规格说明； 安全相关功能要求文档。	质量计划； 系统安装、操作和维护计划； 型式试验程序； 工厂验收测试程序； 系统验收测试程序； 集成系统测试程序。
C2	软件实现	开发符合计算机系统需求规格说明和安全相关功能要求文档的计算机系统软件。	详见第 9 章软件开发生命周期。	系统需求规格说明。	每个计算机系统软件满足计算机系统需求规格说明的证据，其中包括软件测试报告。 详见第 9 章软件开发生命周期。
C3	硬件实现	开发符合计算机系统需求规格说明和安全相关功能要求文档的计算机系统硬件。	参见 8.2.1.3、8.2.1.4、6.2。	系统需求规格说明。	每个计算机系统硬件满足计算机系统需求规格说明的证据。
C4	整体安装	安装计算机系统的软件和硬件，形成一个完整的计算机系统。		系统需求规格说明； 系统安装、操作和维护计划。	已安装就绪的计算机系统。
C5	系统测试	系统测试的主要目的是让系统供应商在内部验证整个计算机系统符合规范、批准的文件以及适用的法规。	参见 8.2.1.6。	系统需求规格说明； 系统安装的软件列表和版本号； 软件功能描述； 软件维护和使用手册；	系统测试报告

				系统和船舶其他系统之间接口的列表； 数据传输标准的列表。	
D 验证					
D1	型式试验	确认计算机系统满足系统需求规格说明（包含安全相关功能）； 确认系统满足 GD019-2024 的要求。	II 类和 III 类系统按 GD019-2024 进行环境试验； I 类系统必要时可参照 GD019-2024 进行环境试验。	系统需求规格说明； 安全相关功能要求文档； 型式试验程序。	确认计算机系统满足安全相关功能要求的证据； 提供型式试验报告，如环境符合性测试报告。
D2	工厂验收测试(FAT)	在工厂对计算机系统进行验收测试。	工厂验收测试报告应记录：①使用的工具和设备；②工厂验收测试活动；③实际结果和预期结果的差异以及处理。 当预期结果和实际结果出现差异时，应分析和评估确定是继续测试，还是提出变更请求。	系统需求规格说明； 工厂验收测试程序。	工厂验收测试报告； 其他工厂验收测试文件(如用户手册等)。
D3	船上测试	通过船上测试，验证所有系统互连后，系统执行预定功能的能力。船上测试包括系统验收测试(SAT)和集成系统测试(SOST)。	系统验收测试应验证在实际硬件环境及最终应用软件的条件下，功能可以正常实现。 集成系统测试应验证所有系统集成状态下的功能可以正常实现。	系统需求规格说明； 系统类别清单； 系统结构说明； 系统验收测试程序； 集成系统测试程序。	系统验收测试报告； 集成系统测试报告。
E 运行					

E1	操作、维护和修理	为保持要求的功能安全，操作、维护和修理计算机系统。	参见 8.3。	系统安装、操作和维护计划。	可持续保持计算机系统所拥有的功能； 按时间排序的计算机系统的操作、维护和修理文档。
E2	变更	在变更阶段中及阶段后，保证计算机系统受控。	提前告知利益相关方对已批准系统的变更和变更方案，并进行影响分析。 变更时应返回生命周期合适阶段。 变更后的软件应进行变更验证，以证明满足相关计算机系统要求。 利益相关方应对变更进行记录。 对 II 类、III 类系统的软件和硬件进行的后续重大变更应提交给 CCS 进行批准。 注：重大变更指影响船舶安全行驶和/或安全的修改。	系统需求规格说明； 质量计划； 变更说明； 变更影响分析； 变更管理程序； 相应阶段的测试程序。	在变更阶段中及阶段后，均可达到计算机系统要求的功能安全； 按时间排序的计算机系统的操作、维护和修理文档； 测试报告或总结。
E3	停用或退役	在计算机系统的停用或退役活动中及活动后，保证计算机系统的功能安全适应这种情况。	在进行停用或退役活动之前，应进行影响分析，并制定一个计划，包括系统的关闭、系统的拆除。 在计算机系统使用说明书中应提示对敏感信息的销毁和处置。	功能安全管理规程对计算机系统停用或退役的要求。	计算机系统安全停用或退役。

8.1.2　下面将对系统生命周期表中需要补充的内容，依据角色单独列出。

8.1.3　软件开发生命周期将在第 9 章详述。

8.2　计算机系统的开发要求

计算机系统的开发要求，跨越了系统生命周期的概念、需求、实现和验证阶段。下面针对不同的角色，详细说明计算机系统的开发要求。

8.2.1　对系统供应商的要求

8.2.1.1　针对将要交付的具体计算机系统的设计、制造、交付和维护，系统供应商应制定质量计划，并执行质量管理体系。应证明系统供应商执行了 5.1.3 表中与其相关的所有要求。对于 II 类和 III 类系统，质量计划应在工厂验收测试期间提交给 CCS 备查。

8.2.1.2　应采用能够唯一标识计算机系统、不同软件组件、同一软件组件不同版本的方法。该方法应用于系统和软件的整个生命周期，是质量管理体系的一部分。

8.2.1.3　应在系统说明中明确系统的设计规格。除了作为设计和实现的要求之外，系统说明的目的是确保整个系统交付符合适用的规范和条款。系统说明应包含以下信息：

(1) 目的和主要功能，包括安全方面；

(2) 定义的系统类别；

(3) 关键性能特征；

(4) 符合的技术要求和 CCS 规范；

(5) 用户界面/模拟；

(6) 通信和接口方面：识别和描述与其他船舶系统的接口；

(7) 硬件布置方面：

a. 网络架构/拓扑，包括所有网络组件，如交换机、路由器、网关、防火墙等；

b. 系统所有接口和硬件节点的内部结构（例如操作站、显示器、计算机、可编程设备、传感器、执行器、I/O 模块等）；

c. I/O 分配（将现场设备映射到信道、通信链路、硬件单元、逻辑功能）；

d. 硬件和外部相关设备的技术规格明细表；

e. 电源布置；

f. 故障模式描述。

上述信息统称为系统说明，系统说明可以分成不同的文件和/或模型。

对于 II 类和 III 类系统，系统说明应提交给 CCS 批准；对于 I 类系统，系统说明在必要时提交给 CCS 备查。

8.2.1.4 应按照 CCS《电气电子产品型式认可试验指南》对系统和子系统的硬件进行环境测试。对于 II 类和 III 类系统，环境符合性测试报告或型式认可证书，应提交给 CCS 备查；对于 I 类系统，环境符合性测试报告或型式认可证书在必要时提交给 CCS 备查。

8.2.1.5 为交付项目而创建、变更或配置的软件，应根据质量计划中所选定的标准进行开发，并对其质量保证活动进行评估。质量保证活动可以在软件结构的多个层级上进行，并应酌情包括定制的软件和配置的组件（如软件库）。

如果采用黑盒测试方法，则对软件的验证应至少包含以下几个方面：

(1) 所有软件组件的参数和配置的正确性、完整性和一致性；

(2) 预期功能；

(3) 预期鲁棒性。

在软件质量保证活动中，通常会使用诸如“软件单元测试”或“开发人员测试”等测试方法，并且还会使用诸如“代码审查”、“静态代码分析”等验证方法。

对于 I 类、II 类和 III 类系统中的软件，所有已进行的审查、分析、测试和其他验证活动的范围、目的和结果，都应记录在测试报告中。测试报告在必要时提交给 CCS 备查。

8.2.1.6 在工厂验收测试之前，应尽可能地进行内部的系统测试。系统测试的主要目的是让系统供应商验证整个系统交付符合规范、批准的文件和适用的法规。进一步地讲，就是系统已经完成，并且准备好进行工厂验收测试了。

应在系统、子系统、软件模块之间完成系统的集成测试，目的是检查软件功能的正确执行，以及软件与其控制的硬件之间的正常交互和功能执行。应尽可能真实地模拟故障，以验证系统拥有恰当的故障检测和故障响应能力。

有一些测试可以利用模拟工具和同型硬件来执行。测试环境应被记录下来，包括对任何模拟器、仿真器、测试存根、测试管理工具、或其他影响测试环境的工具及其限制条件的描述。测试用例和测试结果应分别记录在测试程序和测试报告中。

系统测试应至少准备以下文件资料：

(1) 系统说明，包括系统需求规格说明；

(2) 系统安装的软件列表和版本号；

(3) 软件功能描述；

(4) 软件维护和使用手册；

(5) 系统和船舶其他系统之间接口的列表；

(6) 数据传输标准的列表。

系统测试应至少验证系统以下方面：

(1) 功能；

(2) 故障和故障影响（包括诊断功能、检测、报警响应）；

(3) 性能；

(4) 软件和硬件之间的集成；

(5) 人机界面；

(6) 与其他系统的接口。

对于 I 类、II 类、III 类系统，系统测试报告在必要时提交给 CCS 备查。

8.2.1.7 在系统安装到船上之前，应安排系统的工厂验收测试（FAT）。工厂验收测试的主要目的是向 CCS 证明该系统已经完成，并且符合适用的入级规则，从而能够为系统颁发 CCS 证书。

工厂验收测试程序应从系统测试中选出具有代表性的测试项目（参见8.2.1.6），包括正常的系统功能测试和故障响应测试。所有计划上船安装的软件及其物理媒介在安装之前应进行漏洞、病毒、恶意软件等方面的安全扫描。对于 II 类和 III 类系统，还应进行网络测试，以验证其符合网络韧性要求。如果各方同意，网络测试可以作为船上测试的一部分进行。

通常，工厂验收测试应使用专用软件在船上实际安装的硬件上执行，并具备必要的用于功能模拟和故障响应的工具或手段。对于其他测试方案，如采用同型硬件或模拟工具（仿真器），需征得 CCS 同意。

应向 CCS 提交功能测试和故障响应测试流程，CCS 可能要求进行 FMEA 分析，以支持故障响应测试流程。对于 II 类和 III 类系统，CCS 还会把标识应用作为工厂验收测试的一部分进行验证。

对于每个测试用例，应注明测试通过或不通过，并将测试结果记录在测试报告中。测试报告还应包含在执行测试时已安装在系统中的软件（包括软件版本）的列表。

对于复杂系统，工厂验收测试之前的内部系统测试和工厂验收测试之间的测试范围可能存在很大差异；而对于某些系统，测试范围可能是相同的。

对于 II 类和 III 类系统，工厂验收测试程序应事先获得 CCS 批准；工厂验收测试应由 CCS 现场见证，包括功能测试和故障响应测试；工厂验收测试报告

应提交给 CCS 备查，其他工厂验收测试文件（如用户手册、系统测试报告等）在必要时提交给 CCS 备查。

8.2.1.8 计算机系统软件在船上的初始安装和后续更新，应按照系统供应商和系统集成商约定的变更管理程序进行。变更管理程序应符合 8.4 中的相关要求；网络安全措施应符合 CCS《船舶网络安全指南》的相关要求。

对于 II 类和 III 类系统，变更管理程序和相关记录应提交给 CCS 备查，参见 8.4.12。

8.2.2 对系统集成商的要求

8.2.2.1 船厂被视为船舶开发和交付阶段的系统集成商，除非明确指定了其他组织或个人。

8.2.2.2 针对船上计算机系统的安装、集成、完工和维护，系统集成商应制定质量计划，并执行质量管理体系。应证明系统集成商执行了 5.1.3 表中与其相关的所有要求。对于 II 类和 III 类系统，质量计划应在系统验收测试/集成系统测试期间提交给 CCS 备查。

8.2.2.3 对于交付给具体船舶的计算机系统，应根据系统的故障影响确定该系统属于哪个类别。系统类别确定后，应告知相关系统供应商。对于 I 类、II 类和 III 类系统的分类，应形成系统类别清单，提交给 CCS 批准。

8.2.2.4 如果 CCS 提出要求，系统集成商应对船舶的特定系统进行风险分析，形成风险评估报告，以确定系统的适用类别。可根据 IEC/ISO31010《风险管理-风险评估技术》确定风险评估的方法。

I 类、II 类和 III 类系统的风险评估报告在必要时提交给 CCS 批准。若基于风险评估修正系统类别，可能需要获得 CCS 和系统供应商的同意。当计算机系统的风险显而易见时，允许免除提交风险评估报告，但系统集成商应提交证明文件以说明免除的理由。

8.2.2.5 应规定船舶的计算机集成系统（System of systems），并形成系统结构说明。该系统结构说明，通过将功能分配给不同的系统，以及定义系统之间的主要接口，为系统类别的确定和不同集成系统的开发奠定了基础。同时，它还作为对集成系统进行船上测试的依据（参见 8.2.2.7）。

系统结构说明应至少包含以下内容：

(1) 整个系统结构的概述（集成系统）；

(2) 每个系统的用途和主要功能；

(3) 不同系统之间的通信和接口。

对于 I 类、II 类和 III 类系统，系统结构说明应提交给 CCS 备查。

8.2.2.6　应在船上进行系统验收测试（SAT）。系统验收测试的主要目的是：在计算机系统安装之后，并与船上相关机械/电气/过程系统，包括与其他控制和监测系统之间可能存在的接口集成之后，验证计算机系统的功能运行情况。对于 II 类和 III 类系统，CCS 还会把标识应用作为系统验收测试的一部分进行验证。

每个测试用例应注明测试通过或不通过，并将测试结果记录在测试报告中。测试报告还应包含在执行测试时已安装在系统中的软件（包括软件版本）的列表。

对于 II 类和 III 类系统，系统验收测试程序应事先获得 CCS 批准；系统验收测试应由 CCS 现场见证；系统验收测试报告应提交给 CCS 备查。

8.2.2.7　不同系统在船上最终环境中安装和集成之后，应进行整船的集成测试（即集成系统测试，SOST）。集成系统测试的目的是：验证不同系统在完整安装之后的功能，包括所有接口和相互依赖关系是否符合要求和规定。测试应至少验证集成系统的以下几个方面：

(1) 集成系统的整体功能；

(2) 系统之间的故障响应，应符合故障安全原则；

(3) 性能；

(4) 人机界面；

(5) 不同系统之间的接口和互连。

对于复杂系统，船上的系统验收测试和集成系统测试的测试范围可能存在很大差异，而对于某些系统，测试范围可能重叠或相同。当测试范围相似时，可以将这两项测试合并为一项。

对于 II 类和 III 类系统，集成系统测试程序应事先获得 CCS 批准；集成系统测试应由 CCS 现场见证；集成系统测试报告应提交给 CCS 备查。

8.2.2.8　系统集成商应遵循 8.4 所述的变更管理程序对系统进行变更。对于 II 类和 III 类系统，变更管理程序和记录应提交给 CCS 备查，参见 8.4.12。

8.3　计算机系统的维护要求

8.3.1　对利益相关方的要求

8.3.1.1　业主被视为船舶营运阶段的系统集成商，除非明确指定了其他组织或个人。业主应及时告知 CCS 由其指定的系统集成商。系统的任何变更应由系统集成商和系统供应商共同负责。

8.3.1.2　系统集成商应确保船上存放必要的软件和硬件的变更管理程序，并确保任何软件修改/升级均按该程序执行。变更管理的具体要求，参见 8.4。系统集成商应记录计算机系统在运行阶段的变化。记录内容应包含相关软件版本信息，以及 8.4.10 所述的其他相关信息。

8.3.1.3　系统供应商应遵循计算机系统的维护程序，包括 8.4 所述的变更管理程序。对船上计算机系统进行变更之前，系统供应商应确保计划中的系统变更已经通过了相关内部测试。

8.3.2　维护阶段的系统安全

8.3.2.1　保证维护部门能胜任其活动，尤其应满足以下要求：

(1) 对维护人员进行必要的故障诊断、故障修复、以及系统测试方面的培训；

(2) 对操作人员进行培训；

(3) 对维护人员进行定期再培训。

8.3.2.2　与维护活动有关的人员的培训、经验和资格都应文档化。

8.3.2.3　针对操作人员，应建立接收、记录、解决、问题跟踪和变更申请的程序。应建立和保持计算机系统操作计划，包括识别配置项、操作规程和预期的维护活动。计划还应包括软件迁移和退役问题。

8.3.2.4　制定对操作和维护性能进行分析的规程，尤其是：

(1) 识别危及功能安全的系统故障的规程，包括用于检测重复性故障的日常维护所使用的规程；

(2) 评估需求率、以及在操作和维护期间的失效率是否与系统设计期间的假设一致。

8.3.2.5　进行系统的危险事故（或产生危险的潜在事故）分析，制定使其重复发生的概率降到最低的规程。

8.3.2.6　制定保持潜在危险和安全相关系统信息准确的规程。

8.3.2.7　确定在适当场合的应急服务信息和培训条款。

8.3.2.8　制定对安全相关系统进行修改的规程。

8.3.2.9　确定进行修改所需要的批准规程和主管部门。

8.3.2.10　系统和/或组件每一个新的修改、升级或发布，操作者应进行测试。发布操作使用的组件应满足指定的标准。如果发布组件的接口已被修改，测试应包括集成测试。

8.3.2.11　软件和数据的重大修改，以及版本的改变，要被记录并提交给 CCS 批准。

8.3.2.12　在维护阶段，计算机系统配置管理包括以下内容：

(1) 制定配置控制规程；

(2) 对一个配置管理项（软件和硬件）的全部要素进行唯一标识；

(3) 防止未授权项进入服务。

8.3.2.13　应定期进行配置审核，来验证操作配置的完整性。

8.4　计算机系统的变更管理要求

8.4.1　在计算机系统生命周期的不同阶段，变更管理应由各利益相关方共同协商进行。一般情况下，变更管理至少包括以下三个不同阶段：

(1) 工厂验收测试之前的开发和内部验证阶段，涉及系统供应商和分包供应商；

(2) 工厂验收测试到交付给业主阶段，涉及系统供应商、系统集成商、CCS和业主；

(3) 运行阶段，涉及系统供应商、服务供应商、业主和 CCS。

8.4.2　如果计算机系统在获得利益相关方（在工厂验收测试期间，通常指系统集成商和 CCS）批准之后需要对其进行变更，则应遵循已制定的变更管理程序。

8.4.3　利益相关方应制定文档化的、涵盖计算机系统软件和硬件的变更管理程序。在工厂验收测试之后，系统供应商应按照程序对系统的所有变更进行管理，这些变更包括购买的新版本软件、新的硬件、修改的控制逻辑、更改的配置参数等。变更管理程序应至少包含 8.4.4 至 8.4.11 的内容。

8.4.4　系统供应商应确保每个系统和软件版本都能被唯一识别，详细内容参见 8.2.1.2。

8.4.5　应建立机制，用于对构成软件主文件的文件进行处理。应明确人员权限，以及保证主文件完整性的工具和机制。

8.4.6　应明确规定如何对船上计算机系统的软件进行备份和恢复。

8.4.7　在对计算机系统进行变更之前，应进行影响分析。影响分析结果将决定变更活动的执行程度。变更之前影响分析的目的是：

(1) 确定变更的后果；

(2) 确定对现有文件的影响；

(3) 确定所需的验证和测试活动；

(4) 确定是否需要将变更告知其他利益相关方；

(5) 确定变更前是否需要获得其他利益相关方（如 CCS 和/或业主）的批准。

8.4.8　当维护过程包括在系统中安装新版本软件时，应能将软件回滚到以前安装的版本，以使系统恢复到已知的稳定状态。应对回滚操作进行记录和分析，以便发现和消除导致变更失败的根源。

8.4.9　系统变更在安装到船上之前应尽可能进行测试验证。安装之后，应根据文档化的验证程序在船上再次进行测试验证，包括：

(1) 验证新功能和/或改进是否达到预期效果；

(2) 通过回归测试，验证变更没有对不该受到影响的功能或能力产生任何负面影响。

注：回归测试是指修改了旧代码后， 重新进行测试以确认修改没有引入新的错误或导致其他代码产生错误。

8.4.10　系统和软件的变更应形成记录，以保证变更的可见性和可追溯性。变更记录应至少包含以下内容:

(1) 变更目的；

(2) 变更和修改说明；

(3) 变更影响分析的主要结论（参见 8.4.7）；

(4) 所有新系统或软件的标识和版本（参见 8.4.4）；

(5) 测试报告或测试总结（参见 8.4.9）。

8.4.11　软件变更可以记录在计划维护系统（PMS）、软件注册表或同类文件中。必要时，软件变更应进行安全扫描。

8.4.12　CCS 对变更管理的验证

8.4.12.1　船舶营运阶段，CCS 通常在船舶年度检验时对变更管理进行验证。检验时，应向 CCS 提供变更管理程序和相关变更记录。如果变更需要事先获得 CCS 的批准，那么变更的相关程序和文件可以在申请批准期间进行验证。

8.4.12.2　船舶建造阶段，CCS 对变更管理的验证分为两个部分：

(1) 变更管理程序作为质量管理体系（参见 5.1.3）的一部分进行验证；

(2) 在工厂验收测试期间和之后，结合变更管理程序在具体项目中的实际应用情况进行验证。

9　软件开发生命周期

9.1　系统供应商和系统集成商应制定针对软件开发生命周期的质量计划。应在软件的生命周期中使用行政和技术手段加以控制，以便管理软件变化和保证有关

软件安全方面的要求得到满足，并证明系统供应商和系统集成商存在有效的、能够满足软件开发生命周期各阶段的质量控制程序。

9.2　软件质量计划应包含以下内容：

9.2.1　软件开发生命周期应满足 5.2 的要求。

9.2.2　在软件开发生命周期，计算机系统应有配置管理，特别是：

(1) 对于特定阶段，执行必要的配置控制节点；

(2) 唯一标识计算机系统软件和硬件的所有构成部分；

(3) 阻止非授权项进入服务。

9.2.3　软件开发生命周期的划分及关系请参见下图和表。

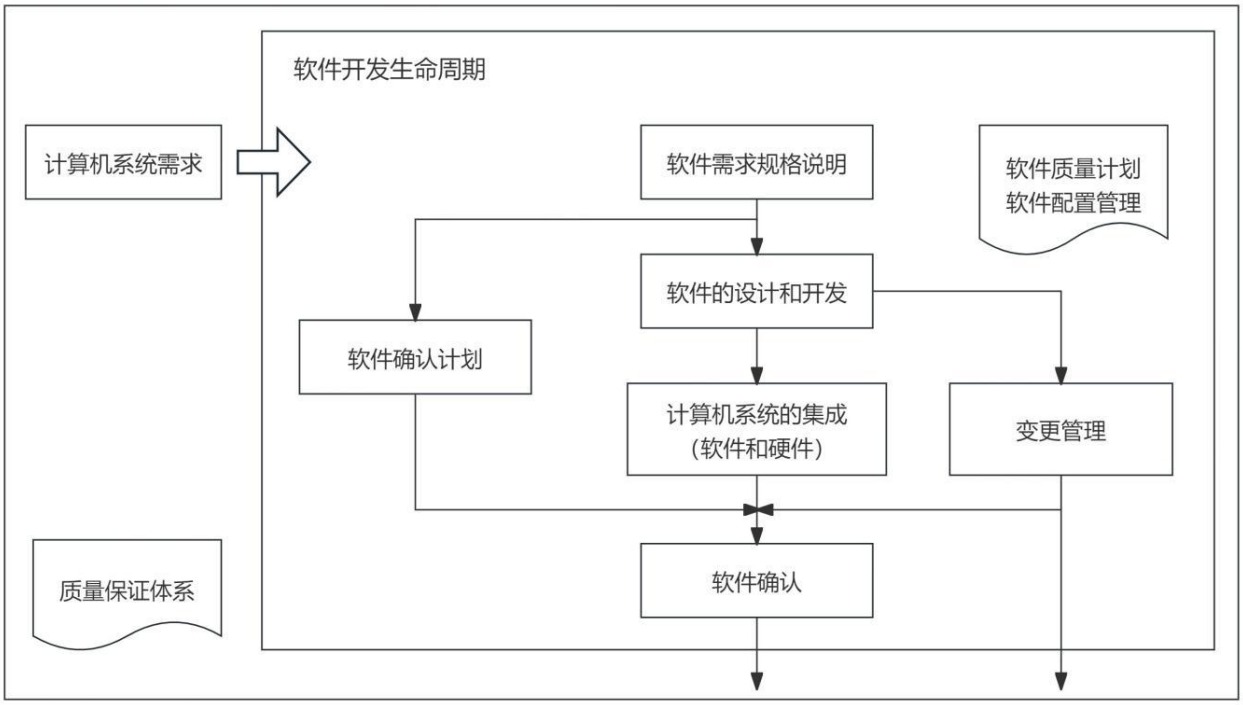


图 9.2.3-1　软件开发生命周期

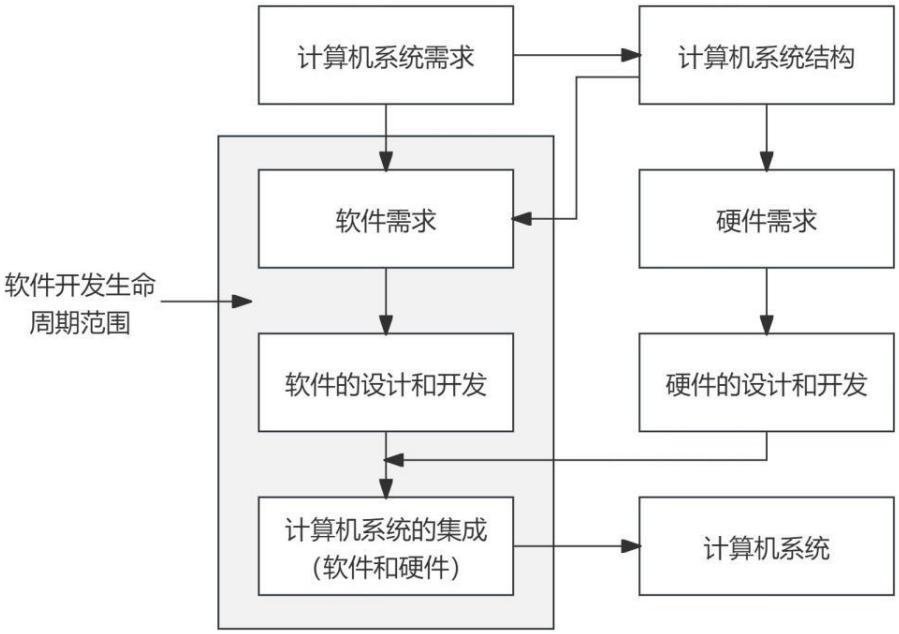


图 9.2.3-2　软件开发生命周期的范围及外部关系

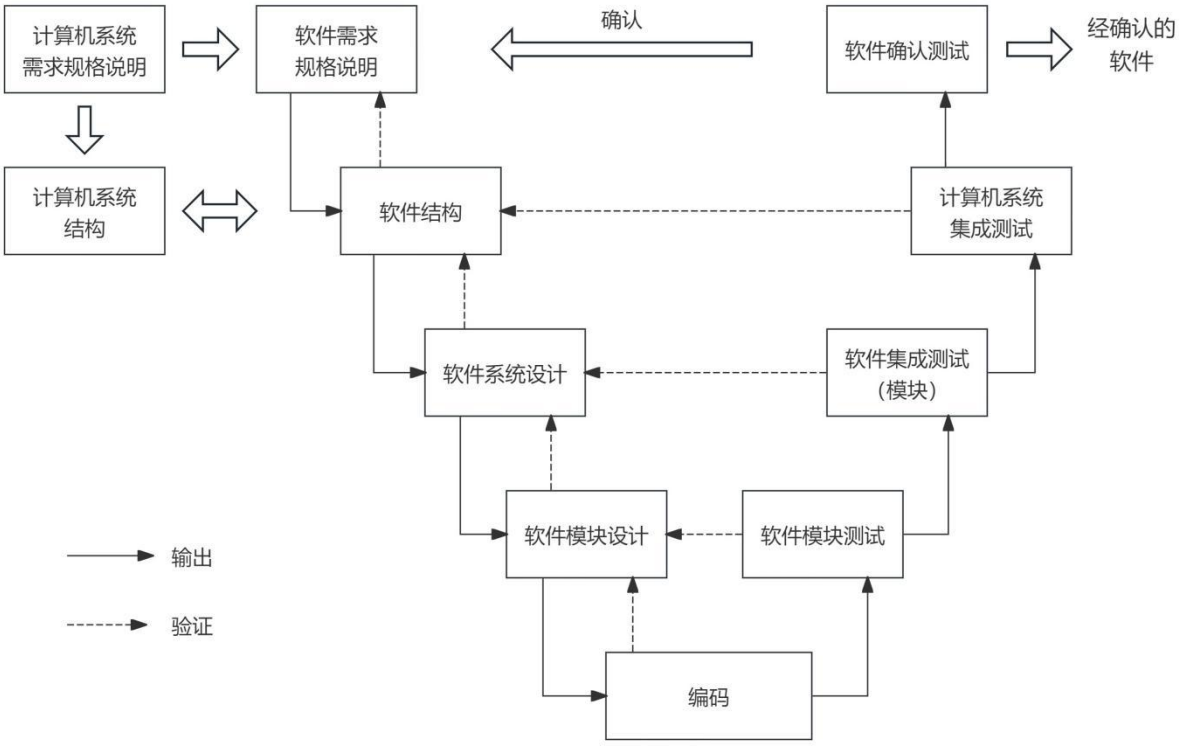


图 9.2.3-3　软件开发生命周期模型（V 模型）

注：　除 V 模型外，本指南亦接受其他经 CCS 同意的软件开发生命周期模型。

9.3 软件需求规格说明

9.3.1 目的

(1) 根据系统功能要求规定软件需求规格说明；

(2) 针对每个需要实现一定安全功能的计算机系统，规定其软件安全功能要求；

(3) 规定计算机系统对软件测试的要求。

9.3.2 要求

(1) 软件开发人员应复审 9.3.1 中的信息以确保全面规定软件需求，应特别考虑以下环节：

① 安全功能；

② 系统配置或构成；

③ 硬件需求；

④ 软件需求；

⑤ 容量和响应时间；

⑥ 设备和操作人员界面。

(2) 在要求的系统类别等级范围内，软件安全的规定要求应得到表达和组织，以使其：

① 清楚、准确、不含糊、可验证、可测量、可维护、可行；

② 可回溯到计算机系统安全要求的规定；

③ 不使用不明确的、或在软件开发生命周期任一阶段使用这些文档的人所不能理解的术语和描述。

(3) 如果没有详细定义计算机系统的特殊安全要求，那么应在软件安全的特殊要求中详细说明计算机系统及其运行模式。

(4) 软件需求规格说明应对软件和硬件之间的任何与安全有关的约束进行规范并文档化。

(5) 在计算机系统硬件结构设计要求的范围内，软件需求规格说明应考虑如下内容：

① 软件自监视；

② 可编程电子硬件、传感器和执行器的监视；

③ 在系统运行时，安全功能的周期测试；

④ 当系统运行时，使安全功能可测试。

(6) 软件需求规格说明应将计算机系统的非安全功能和安全功能清晰区分。

(7) 软件需求规格说明应表达计算机系统要求的安全属性，但不是工程项目的安全属性。

9.3.3 输入

系统需求规格说明

9.3.4 输出

软件需求规格说明

9.4 软件确认计划

9.4.1 目的

根据软件需求规格说明编制软件确认计划。

9.4.2 编制要求

(1) 软件确认计划应考虑：

① 确认时的细节情况；

② 执行确认的人员的细节情况；

③ 确定系统的相关运行模式，应包括：

— 使用前的准备工作，包括设置和调整；

— 启动、教学、自动化、手动、半自动化、稳定状态运行；

— 重置、关机、维护；

— 合理可预见的异常状况和误操作。

④ 在开始调试前，应针对每个系统运行模式确认其软件要求；

⑤ 确认活动的技术策略（如分析方法、统计测试等）；

⑥ 用于确保每个软件功能符合规定要求的措施和规程；

⑦ 根据软件需求规格说明确定的特殊要求；

⑧ 确认活动所需要的环境（如测试所需的调校工具和设备）；

⑨ 通过/失败的准则；

⑩ 评价确认结果的方针和规程，特别是失败时。

(2) 软件确认的技术策略应包括下列信息：

① 手动或自动技术选一或选二；

② 动态或静态技术选一或选二；

③ 分析或统计技术选一或选二。

(3) 完成软件确认的通过/失败准则应包括：

① 要求的输入信号及其次序和值；

② 预期的输出信号及其次序和值；

③ 其他可接受的准则，如存储使用、时序、值的允许偏差。

9.4.3 输入

软件需求规格说明

9.4.4 输出

软件确认计划。

9.5 软件的设计和开发

这部分描述软件开发生命周期中的软件设计和开发活动。

9.5.1 软件结构和工具集要求

(1) 目的

① 软件结构：

创建软件结构，满足不同安全等级对软件安全的规定要求。

复审和评价计算机系统硬件对软件的要求，包括软件和硬件相互作用对计算机系统安全的影响。

② 工具集：

在整个软件生命周期中，根据要求的安全等级，选择合适的工具集（包括编程语言、编译器等），用于辅助验证、确认、评价和修改软件。

(2) 软件结构的要求

软件结构是定义软件主要组件和子系统，包括它们如何实现内部连接，如何获得所要求的属性，特别是安全完整性。主要软件组件包括操作系统、数据库、大型设备输入/输出子系统、通信子系统、应用程序、编程和诊断工具等。

软件结构设计由软件供方和/或开发人员来建立，软件结构设计的描述应详细，描述内容包括：

① 在软件开发生命周期中，为满足系统的不同安全等级要求，应选择和论证一组必要的技术和措施。这些技术和措施包括故障允许偏差（与硬件一致）和故障避免的软件设计策略，包括（适用时）冗余和多样性。

② 根据组件/子系统的划分，每一部分应提供以下信息：

— 它们是否是新的、已存在的、或者拥有专利的；

— 它们是否已被验证，如果是，它们的验证条件；

— 每一个组件/子系统是否与安全有关。

③ 确定所有软件/硬件相互作用关系，评价和细化它们的重要性。

④ 使用符号表示法表示软件结构。

⑤ 选择用于保持所有数据安全完整性的设计特征。这种数据可包含大型设备输入/输出数据、通信数据、操作界面数据、维护数据和内部数据库数据。

⑥ 根据软件结构，规定适当的集成测试来保证软件结构满足规定的软件安全要求。

(3) 工具集的要求

① 对于使用有限可变语言的应用程序编程，在一个低安全完整性等级下，要求的工具和编程语言可被限定为一套标准的编程语言、编辑器、加载器。其符合性的责任主要由供方承担。

② 在较高等级的系统上，需限制编程语言的子集，验证和确认诸如代码分析器和仿真器等工具。该环境下的责任由供方和用户共同承担。

③ 即便是在低等级的系统上，也可广泛使用完全可变语言来开发嵌入式应用程序。符合性的责任主要由软件开发人员来承担。

④ 根据软件开发的固有特性， 确保以下(a)-(e)符合性要求的责任由供方或用户单独承担，或由两者共同承担，责任的划分应编制在安全技术文档中。

(a) 一套合适的工具集，包括编程语言、编译器、配置管理工具、自动测试工具等，应根据安全要求进行选择。应考虑在计算机系统整个生命周期中提供相应服务的合适开发工具（不一定是系统开发初期使用的工具）的可用性。

(b) 在安全完整性等级要求的范围内，所选的工具或设计表述（包括编程语言）应：

- 具有符合国家标准或国际标准的翻译器/编译器，或对其目的适用性进行评估；
- 仅使用已定义的语言特性；
- 与应用特性匹配；
- 包含便于检测程序错误的特性；
- 与设计方法相匹配的特性。

(c) 当不能完全满足 (b) 时，软件结构设计规格说明中应给出另一种可选择编程语言的理由，理由应足够详细说明编程语言的适用性，以及针对已识别编程语言缺点的附加措施。

(d) 编码标准应：

- 由评估方复审其使用目的是否合适；
- 用于开发所有功能安全相关软件。

(e) 编码标准应规定良好的编程习惯，禁止不安全的语言特性（如未定义的语言特性、非结构化设计等），并制定建立源代码文档的规程。源代码文档中应包括下列信息：

- 法律实体（如公司、作者等）；
- 描述；
- 输入和输出；
- 配置管理历史。

(4) 输入

① 软件需求规格说明

② 计算机系统硬件结构设计

(5) 输出

① 软件结构设计规格说明

② 支持工具和编码标准

③ 开发工具的选择

④ 软件集成测试规格说明

⑤ 计算机系统集成测试规格说明

9.5.2 详细设计

(1) 目的

设计软件，以满足不同安全等级对软件的要求。软件应可分析，可验证，并能被安全地修改。

详细设计包括软件系统设计和软件模块设计。

(2) 要求

① 详细设计首先指软件系统设计，包括把软件结构中的主要组件划分到软件模块、单独的软件模块设计、编码如何实现等。

② 软件的详细设计需要对每一个软件组件提供逻辑设计，并产生详细设计文件，以定义内部结构和组成部分的接口，其中包括相关测试内容。

③ 设计的软件应具有模块化、可测试性、可安全修改的能力。

④ 对于软件结构设计中的每一个主要组件/子系统，设计的进一步细化应基于软件模块的划分。应规定每个软件模块的设计以及对每个软件模块的验证。

⑤ 需提供软件系统设计规格说明和软件模块设计规格说明。

⑥ 设计规格说明应包括如下内容：

(a) 安装在每个硬件单元中的基本软件的描述；

(b) 安装在网络节点中的通信软件的描述；

(c) 应用软件的描述（不是程序清单）；

(d) 用于系统设置和设备配置的工具；

(e) 说明功能、性能、模块和其他部件之间的相互约束和依赖关系。

对软件的描述，应满足以下要求：

(a) 依赖的系统模块（必须工作以维持功能），以及对其他系统的依赖关系；

(b) 每个模块的描述细节应达到足以了解其功能的水平；

(c) 软件模块（必须运行以保持相关功能）之间的关系；

(d) 软件模块之间的数据流和控制流；

(e) 软件的配置，其中包括优先级策略；

(f) 冗余系统的切换机制（若有）；

(g) 软件自我监控（如应用驱动看门狗、数据范围验证等）；

(h) 验证测试和外部设备诊断测试（如传感器和终端元件）；

(i) 对非预期的过程变量（如传感器值超出范围、开路、短路）应采取的措施。

(3) 输入

① 软件结构设计规格说明

② 支持工具和编码标准

(4) 输出

① 软件系统设计规格说明

② 软件模块设计规格说明

③ 软件系统集成测试规格说明

④ 软件模块测试规格说明

9.5.3 代码实现

(1) 目的

利用合适的工具集（包括编程语言、编译器等）来实现软件。

(2) 要求

源代码应：

① 可读、可理解和可测试；

② 满足软件模块设计的规定要求；

③ 满足编码标准的规定要求；

④ 满足安全计划中规定的相关要求。

应复审每一个软件代码模块，以检查代码编写和它的记录是否符合详细设计文档的描述。

(3) 输入

① 软件系统设计规格说明

② 软件模块设计规格说明

③ 支持工具和编码标准

(4) 输出

① 源代码清单

② 代码复审报告

9.5.4 软件模块测试

(1) 目的

软件模块测试是一种验证活动，是代码复审和测试工作的结合，用以证明软件模块满足它的相关要求。

(2) 要求

① 每一个软件模块都应根据在软件设计阶段确定的测试规格说明进行测试。这些测试应表明每一个软件模块执行预定功能，且不执行非预定功能。

② 软件模块测试应实现文档化。II 类、III 类系统的软件模块测试文档应包括但不限于软件模块设计规格说明、软件模块测试计划、软件模块测试用例、软件模块测试记录、测试记录分析报告、软件模块测试问题报告和测试总结报告。

③ 应制定未通过测试的纠正措施规程。

④ 采用合适的测试方法对软件模块的逻辑及需求进行全面的测试。

⑤ 可采用白盒测试的方法执行模块测试，根据边界值分析、错误推测、等价类或输入划分等方法设计测试用例。可根据软件的安全等级要求及船用可编程设备的特性要求选择上述方法。

(3) 输入

① 软件模块测试规格说明

② 源代码清单

③ 代码复审报告

(4) 输出

① 软件模块测试记录

② 经验证和测试的软件模块

9.5.5 软件集成测试

(1) 目的

软件集成测试是验证软件能否被正确集成的一种活动，通过测试应证明所有软件模块、组件和子系统能相互正确作用来实现其预定的功能，不实现非预定的功能。

(2) 一般要求

① 软件集成测试应在设计和开发阶段予以规定。

② 软件集成测试一般包括：软件子系统测试和软件系统测试。

③ 软件集成测试应规定以下内容：

(a) 将软件划分为可管理的集成集；

(b) 测试用例和测试数据；

(c) 执行测试的类型；

(d) 测试环境、工具、配置和程序；

(e) 判定测试完成的准则；

(f) 测试失败的校正措施规程。

④ 软件集成测试应根据规定的软件集成测试要求进行测试。这些测试应表明所有软件模块、组件和子系统能相互正确作用以执行其预定的功能，而不执行非预定的功能。

⑤ 软件集成测试应文档化，并说明测试结果是否满足测试目的和测试准则。如果出现失败，记录失败原因。

⑥ 在软件集成过程中，应对软件的任何修改或变更进行影响分析，以确定所有受影响的软件模块和所需要的再验证、再设计活动。

(3) 软件子系统测试附加要求：

① 建议采用黑盒测试方法来执行子系统测试。可使用动态测试、等价类划分、边界值分析等方法设计测试用例。可根据软件的等级要求及船用可编程设备的特性选择上述方法。

② 对于 II 类、 III 类系统，应执行子系统测试，并分析测试结果，以验证软件模块是否被正确地集成。测试结果的确认依据可追溯到测试计划文档中由测试可追溯性建立的测试准则。

(4) 软件系统测试附加要求：

① 对于 II 类、III 类系统，应保证其满足子系统测试要求。

② 船用可编程设备的软件应根据系统测试计划的规定进行测试活动。

③ 软件系统测试应验证防修改保护功能：

(a) 防止用户修改软件；

(b) 防止用户修改软件的运行参数。

④ II 类 、III 类系统的软件系统测试，应验证单一故障条件下软件系统符合故障安全原则。

⑤ 应采用黑盒测试方法执行软件系统测试，采用等价类或过程仿真方法设计测试用例。可根据安全等级要求和船用可编程设备要求选择上述方法。

⑥ 当预期结果和实际结果出现差异时，应进行分析和评估，确定是继续测试，还是提出变更请求。若提出变更请求，则应返回软件开发生命周期较早阶段。这些决定应作为软件系统测试的确认结果，并文档化。

(5) 输入

软件集成测试规格说明（软件子系统/系统测试）

(6) 输出

① 软件集成测试记录

② 经验证和测试的软件系统

9.6 计算机系统（软件和硬件）的集成

9.6.1 目的

(1) 在目标计算机系统硬件上集成软件。

(2) 计算机系统集成测试可保证软件和硬件的兼容性，并满足预定的要求。

9.6.2 一般要求

(1) 应在设计和开发阶段规定集成测试，以保证计算机系统中软件和硬件的兼容性。

(2) 计算机系统（软件和硬件）集成测试，可以简写为计算机系统集成测试，是本指南中主要的系统测试方式，应规定：

① 将系统拆分为各个集成集；

② 测试用例和测试数据；

③ 执行测试的类型；

④ 测试环境包括工具、支持软件和配置描述；

⑤ 判定测试完成的准则。

(3) 在进行计算机系统（软件和硬件）规定的集成测试时，应区别开发人员按自己意图所执行的活动和从用户立场出发所进行的活动。

(4) 计算机系统（软件和硬件）集成测试，应区分以下活动：

① 将软件纳入目标计算机系统硬件；

② 计算机系统集成，即通过增加接口，连接传感器、执行器等设备；

③ 计算机系统和 EUC（其他系统）的全部集成。

(5) 应根据计算机系统（软件和硬件）集成测试规格说明，对软件和硬件进行集成测试。

(6) 应对计算机系统（软件和硬件）的任何修改或变更进行影响分析，用来确定所有受影响的软件组件/模块，以及所需要的再验证、再设计活动。

(7) 应记录测试用例和测试结果，用于随后的分析。

(8) 计算机系统（软件和硬件）的集成测试应文档化，说明测试结果是否满足测试目的和测试准则。如果出现失败，记录失败原因。

(9) 对于 II 类、III 类系统，应保留并按要求提交集成测试的证明文件，文件包括测试计划和测试报告。

9.6.3 故障模拟测试要求

(1) 故障模拟测试，也可以称为故障响应测试。根据计算机系统设计规格说明，制订系统的故障模拟测试规格说明。应尽可能真实地进行故障模拟，以证明系统具有适当的故障响应能力。

(2) 故障模拟测试规格说明包括以下内容：

① 故障组件或元器件名称；

② 故障类型；

③ 故障注入方式；

④ 要求的故障响应（输出记录）。

(3) 故障模拟测试的测试用例及其预期结果应文档化。应说明故障模拟测试的测试结果以及是否满足测试目的和测试准则。如果出现失败，应分析和记录失败原因。

9.6.4 输入

(1) 计算机系统集成测试规格说明（含故障模拟测试）

(2) 软件和硬件已集成的计算机系统

9.6.5 输出

(1) 计算机系统集成测试记录

(2) 经验证和测试的计算机系统

9.7 软件确认

9.7.1 目的

保证集成后的计算机系统（软件和硬件）符合软件需求规格说明。

9.7.2 要求

(1) 软件确认通常不能脱离与它相关的硬件和系统环境。

(2) 在软件确认时，应考虑下列属性：

① 针对软件需求规格说明，所做确认的完整性；

② 针对软件需求规格说明，所做确认的正确性；

③ 可重复性；

④ 精确定义的确认配置。

(3) 应根据软件确认计划进行软件的确认活动。

(4) 以下软件确认结果应文档化：

① 按时间顺序的确认活动记录，以便追溯活动的顺序；

② 所用的软件确认计划版本；

③ 根据软件确认计划，被确认（通过测试或分析）的软件需求；

④ 使用的工具、设备及其校准数据；

⑤ 确认活动的结果；

⑥ 实际结果和预期结果的差异。

(5) 当实际结果和预期结果出现差异时，应进行必要的分析，以便决定是继续确认，还是提出变更请求，并返回软件开发生命周期的较早阶段。

(6) 软件确认应符合以下要求：

① 软件确认测试应是软件确认的主要方法，分析、动画和建模可作为确认活动的补充；

② 必要时，可以采用仿真/模拟测试方法进行软件确认；

③ 应使系统开发人员得到软件确认结果及其附属文档。

(7) 软件确认结果应满足以下要求：

① 软件确认测试应证明所有软件规定的要求都得到了满足,并且软件不执行非预定的功能；

② 测试用例及测试结果应文档化，用于后续的分析和独立评估；

③ 文档化的软件确认测试结果应表明：(a)软件已通过确认，或(b)未通过确认的原因。

9.7.3 输入

软件确认计划

9.7.4 输出

(1) 软件确认结果；

(2) 已确认的软件。

9.8 变更管理

9.8.1 目的

依据软件变更管理程序，指导修正、增强、调整已确认或已批准的软件，保证软件变更后的计算机系统安全可控。

9.8.2 要求

(1) 基于计算机系统的变更管理要求（参见8.4），细化和完善软件的变更管理程序。

(2) 应提前告知利益相关方对已批准系统的软件变更方案，并进行影响分析，同时应向 CCS 报备。对 II 类和 III 类系统进行的软件重大变更，应提交给 CCS 进行批准。

(3) 应对软件变更进行验证和记录。对于 II 类和 III 类系统，CCS 应见证软件重大变更的验证过程。

(4) 对软件变更进行的验证活动包括回归测试。当软件代码更改率超过 30% 时，应对更改后的软件和系统进行一次完整、全面的测试。

9.8.3 输入

(1) 软件变更管理程序

(2) 软件变更请求

9.8.4 输出

(1) 软件变更影响分析结果

(2) 软件变更记录

(3) 相应测试报告

9.9 软件验证

9.9.1 目的

测试和评估软件开发生命周期在给定阶段的输出，以保证该阶段输出对于相应输人的正确性和一致性。

9.9.2 要求

(1) 对软件开发生命周期的每一个阶段，软件验证应与开发过程做好同步计划，并且软件验证应文档化。

(2) 软件验证计划编制应涉及验证活动中使用的准则、技术和工具，并应包括以下内容：

① 安全完整性要求的评价；

② 验证策略、活动和技术的选择及其文档化；

③ 验证工具（测试工具、专用测试软件、输入/输出仿真器等）的选择和使用；

④ 验证结果的评价；

⑤ 采用的纠正措施。

(3) 软件验证应根据计划执行。

(4) 应对软件验证的证据文档化，以表明对相关阶段的验证已在各个方面圆满完成。

(5) 每次验证后，验证文档应包括：

① 被验证项的识别；

② 完成验证所依据信息的识别；

③ 不符合项（如软件模块、数据结构和不适用的算法）。

(6) 软件开发生命周期 N 阶段中所有 N+1 阶段正确执行所需的信息都应可获得并被验证，N 阶段的输出包括：

① N 阶段的文档、设计或代码应充分满足：

— 功能性；

— 安全完整性、性能和其他安全计划编制的要求；

— 对于开发团队而言的可读性；

— 进一步验证的可测试性；

— 允许进一步改进的安全修改。

② 针对 N 阶段的设计要求和设计表述，N 阶段规定的确认计划和/或测试应该是充分的。

③ 检查下列内容之间的不一致性：

— N 阶段规定的测试和 N-1 阶段规定的测试；

— N 阶段中的各个输出。

(7) 软件开发生命周期的各阶段应执行下列验证活动：

① 软件需求的验证；

② 软件结构的验证；

③ 软件系统设计的验证；

④ 软件模块设计的验证；

⑤ 代码验证；

⑥ 数据验证；

⑦ 时间性能的验证；

⑧ 软件模块测试；

⑨ 软件集成测试；

⑩ 计算机系统集成测试；

⑪ 软件确认；

⑫ II 类和 III 类系统数据链路的额外要求。

(8) 软件需求的验证：在规定软件需求之后，并且在接下来的软件设计和开发阶段之前，验证应：

① 考虑规定的软件需求是否已充分满足计算机系统规定的功能、安全完整性、性能、以及其他方面的要求。

② 考虑软件确认计划是否已充分满足规定的软件安全要求。

③ 检查下列内容之间的不一致性：

— 软件需求和计算机系统需求；

— 软件需求和软件确认计划。

(9) 软件结构的验证：在完成软件结构设计后，验证应：

① 考虑软件结构设计是否充分满足软件需求规格说明；

② 考虑软件结构设计规定的集成测试是否充分；

③ 考虑每一个主要组件/子系统的属性是否充分满足：

— 所需安全性能的可行性；

— 进一步验证的可测试性；

— 对于开发团队而言的可读性；

— 允许进一步改进的安全修改。

④ 检查以下内容之间的不一致性：

— 软件结构设计和软件需求规格说明；

— 软件结构设计和软件结构集成测试；

— 软件结构集成测试和软件确认计划。

(10) 软件系统设计的验证：在完成软件系统设计后，验证应：

① 考虑软件系统设计是否充分满足软件结构设计；

② 考虑软件系统集成规定的测试是否充分满足软件系统设计；

③ 考虑软件系统设计的每一个主要组件的属性是否充分满足：

— 所需安全性能的可行性；

— 进一步验证的可测试性；

— 对于开发团队而言的可读性；

— 允许进一步改进的安全修改。

④ 检查以下内容之间的不一致性：

— 软件系统设计和软件结构设计；

— 软件系统设计和软件系统集成测试；

— 软件系统集成测试和软件结构集成测试。

(11) 软件模块设计的验证：在完成每一个软件模块设计后，验证应：

① 考虑软件模块设计是否充分满足软件系统设计要求；

② 考虑每一个软件模块的规定测试是否充分满足软件模块设计要求；

③ 考虑每一个软件模块的属性是否充分满足：

— 所需安全性能的可行性；

— 进一步验证的可测试性；

— 对于开发团队而言的可读性；

— 允许进一步改进的安全修改。

④ 检查以下内容之间的不一致性：

— 软件模块设计和软件系统设计；

—（对于每一个软件模块）软件模块设计和软件模块测试；

— 软件模块测试和软件系统集成测试。

(12) 代码验证：源代码需通过静态方法验证，以确保符合软件模块设计、要求的编码标准和软件确认计划的要求。

注：在软件开发生命周期的早期阶段，验证是静态的（如审查、复审、形式化证明等)。代码验证包括审查和走查等技术。代码验证与软件模块测试结合，保证每一个软件模块满足相关文件要求。此后，测试成为验证的主要方法。

(13) 数据验证

① 数据结构验证包括：

— 完整性；

— 自身一致性；

— 对改变或破坏的防范；

— 与数据驱动系统功能要求的一致性。

② 应用数据验证包括：

— 与数据结构的一致性；

— 针对应用要求的完整性；

— 与相关系统软件的兼容性（如执行的序列、运行时等）；

— 数据值的正确性。

③ 针对应用要求，验证所有运行参数，以防止：

— 无效或未定义初始值；

— 错误、不连续或不合理值；

— 非批准改变；

— 数据损坏。

④ 所有设备接口和相关软件（即传感器、执行器和离线接口）应进行以下验证：

— 预期接口失效的检测；

— 预期接口失效的容错。

⑤ 所有通信接口和相关软件，应适度验证以下内容：

— 失效检测；

— 错误防范；

— 数据确认。

(14) 时间性能的验证：验证在时间域的行为可预测性。

注：时间行为可能包括性能、资源、响应时间、最坏情况下的执行时间、超负荷、无死锁、运行时系统等。

(15) 其余验证：此处不对软件模块测试、软件集成测试和计算机系统集成测试提出额外要求，因为这些测试本身就是验证活动。同样，不对软件确认提出额外要求，因为软件确认就是证明其符合软件需求的验证活动。

9.9.3 输入

适当的验证计划（根据阶段）

9.9.4 输出

适当的验证报告（根据阶段）

10 测试、验证和批准

10.1 计算机系统应根据下表的要求进行测试和验证，本节仅针对软件提出了具体的要求。小型低复杂度计算机系统的评估应按照本指南附录 2 的要求进行测试和验证。

表 10.1 测试和验证

序号	要 求	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件
1	质量管理							①质量计划 ②安保策略相关的程序和文件
1.1	实施 ISO9001 或等效标准的质量管理体系	X	X		Ⓘ (必要时)	Ⓘ	Ⓘ	
1.2	质量计划	X	X		Ⓘ (必要时)	Ⓘ	Ⓘ	
1.3	软件可追溯性	X	X	X	Ⓘ (必要时)	Ⓘ	Ⓘ	
1.4	安保策略	X	X	X	Ⓘ (必要时)	Ⓘ	Ⓘ	
2	计算机系统技术要求							①对计算机系统、组件、及其版本进行唯一标识的具体程序
2.1	系统标识要求	X	X			Ⓘ	Ⓘ	
2.2	II 类和 III 类系统数据链路要求	X	X			Ⓘ	Ⓘ	
2.3	采用无线数据链路时的补充要求	X	X			Ⓘ	Ⓘ	

3	**系统说明（软件描述和相关硬件描述）**	X			Ⓘ (必要时)	Ⓐ	Ⓐ	①系统说明（可分解成相关文档）②计算机系统需求规格说明 ③计算机系统硬件说明 ④软件需求规格说明 ⑤软件结构设计规格说明 ⑥软件结构集成测试规格说明 ⑦软件模块设计规格说明 ⑧软件模块测试规格说明 ⑨软件系统设计规格说明 ⑩软件系统测试规格说明 ⑪软件集成测试规格说明 ⑫计算机系统集成测试规格说明 ⑬支持工具和编码标准 ⑭开发工具的选择
3.1	**软件说明**							
3.2	**硬件说明**							
3.3	**技术要求**							
4	**软件代码验证**	X				Ⓘ (必要时)	Ⓘ (必要时)	①代码复审报告
5	**软件模块测试**	X				Ⓘ (必要时)	Ⓘ (必要时)	①软件模块测试规格说明 ②软件模块测试记录
6	**软件集成测试**	X			Ⓘ (必要时)	Ⓘ (必要时)	Ⓘ (必要时)	①软件集成测试规格说明 ②软件集成测试记录 ③软件系统测试规格说明 ④软件系统测试记录 ⑤软件结构集成测试规格说明 ⑥软件结构集成测试记录 ⑦软件测试报告
6.1	**软件集成测试一般要求**							
6.2	**软件子系统测试附加要求**							
6.3	**软件系统测试附加要求**							
7	**计算机系统(软件和硬件)集成测试，属于系统测试**	X			Ⓘ (必要时)	Ⓘ (必要时)	Ⓘ (必要时)	①计算机系统集成测试规格说明 ②计算机系统集成测试记录 ③计算机系统故障模拟测试规格说明 ④计算机系统故障模拟测试记录 ⑤系统测试报告
7.1	**计算机系统集成测试的一般要求**							
7.2	**计算机系统的故障模拟测试要求**							
8	**工厂验收测试(FAT)，包括软件确认测试**							①系统说明 ②FAT程序 ③FAT报告 ④用户手册 ⑤系统测试报告等
8.1	**编制 FAT 程序(试验大纲)**	X				Ⓐ	Ⓐ	
8.2	**执行 FAT**	X				Ⓦ	Ⓦ	
8.3	**编制 FAT 报告**	X				Ⓘ	Ⓘ	
8.4	**其他 FAT 文件**	X				Ⓘ (必要时)	Ⓘ (必要时)	
9	**硬件的环境合规性要求**	X			Ⓘ (必要时)	Ⓘ	Ⓘ	①环境符合性测试报告或型式认可证书。
10	**船上测试前的准备工作**							①系统说明 ②系统类别清单 ③风险评估报告 ④系统结构说明 ⑤FAT报告 ⑥用户手册
10.1	**系统类别清单**		X		Ⓐ	Ⓐ	Ⓐ	

10.2	**风险评估报告**		X		Ⓐ (必要时)	Ⓐ (必要时)	Ⓐ (必要时)	
10.3	**系统结构说明**		X		Ⓘ	Ⓘ	Ⓘ	
11	**船上测试**							①SAT程序 ②SAT报告 ③SOST程序 ④SOST报告
11.1	**编制船上测试程序（试验大纲）**		X			Ⓐ	Ⓐ	
11.2	**执行船上测试**		X			Ⓦ	Ⓦ	
11.3	**编制船上测试报告**		X			Ⓘ	Ⓘ	
12	**计算机系统的变更验证**							①变更管理程序 ②变更请求或变更说明 ③变更影响分析结果 ④变更记录 ⑤相应测试报告
12.1	**一般验证要求**	X	X	X	Ⓘ (必要时)	Ⓘ	Ⓘ	
12.2	**重大变更附加验证要求**	X	X			Ⓐ Ⓦ	Ⓐ Ⓦ	

注 1：表中采用的符号及其含义如下:

Ⓐ 提交 CCS 批准　　Ⓘ 提交 CCS 备查　　Ⓦ 需 CCS 见证

注 2：如果表中具体要求项的“角色”和“系统类别”没有提出要求（空白），那么则采用其标题项的要求。

注 3：表中“需提供的文件”，可以合并或分解，也可以使用其他名称，只要拥有本指南要求的内容即可。

注 4：见证的等级按照上述的要求评估后决定，若采取与预定要求不一致的设计或布置，应向 CCS 提交按照相关国际（参见 SOLAS 公约第 II-1 章第 55 条。）或国内标准进行的工程分析，并获得认可。

10.2　CCS 应见证和检验的项目如下，相关责任方应为活动提供便利。

序号	项目	责任方	系统类别		
			I 类系统	**II 类系统**	**III 类系统**
1	工厂验收测试（FAT）	系统供应商	-	Ⓦ	Ⓦ
2	系统验收测试(SAT)	系统集成商	-	Ⓦ	Ⓦ
3	集成系统测试(SOST)	系统集成商	-	Ⓦ	Ⓦ
4	重大变更验证	系统集成商	-	Ⓦ	Ⓦ

注：表中采用的符号及其含义如下：Ⓐ 提交 CCS 批准；Ⓘ 提交 CCS 备查；Ⓦ 需 CCS 见证。

10.3　系统供应商或系统集成商可按照 CCS《船舶网络安全指南》中的要求，向 CCS 申请进行网络安全方面的检验或评估。如果需要专业的可靠性验证，可按照 CCS《船舶设备与系统可靠性验证指南》中的要求，向 CCS 申请可靠性验证符合性证明。

10.4　系统供应商或系统集成商可按照 CCS《电气电子产品型式认可试验指南》完成 II 类和 III 类系统内集成的可编程设备的认可。CCS 验证所要求的测试后，可编程设备的认可可以采取单件检验方式或作为型式认可的组成部分完成。认可文件应描述可编程设备在船舶应用中的兼容性，以及船上测试的必要性。

10.5　计算机系统型式认可

常规制造并包含通用软件功能的计算机系统，可根据 CCS 相关要求进行型式认可。型式认可包括两个主要验证活动：

(1) 对型式认可文件进行评估，包括 7.1 所列文件以及申请 CCS 型式认可所需的其他文件；

(2) 对通用功能进行检验和测试，其中软件测试可由专业机构实施（参见附录 4）。

对于建立了系统生命周期的计算机系统，依照 CCS《钢质海船入级规范》等要求通过了系统和硬件的认证，并满足本指南对软件的要求，可根据其不同的系统类别（分类见 4.1），授予下列附加标志：

(1) 对于 I 类系统，SLC1；

(2) 对于 II 类系统，SLC2；

(3) 对于 III 类系统，SLC3。

当因为具体船舶的功能、参数配置和安装元件需要进行实船验证时，即使计算机系统完成型式认可，也仍需持有产品证书。

10.6　计算机系统产品证书

实现船舶功能所必需的 II 类或 III 类计算机系统应持有产品证书。产品证书的目的是确认该系统的设计和制造已经完成，并符合适用的入级要求。获得产品证书，需要进行两个主要验证活动：

(1) 对计算机系统的文件进行评估，包括 7.1 所列文件；

(2) 对上船的计算机系统进行检验和测试，其中软件测试可由专业机构实施（参见附录 4）。

在满足要求的情况下，CCS 可以接受替代验证方案，并颁发产品证书。

附录 1　测试和验证表

申请方名称：_____　　工作控制号：_____

产品名称：_____　　产品型号：_____

软件名称：_____　　软件版本号：_____

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
1	**质量管理**								① 质量计划 ② 安保策略相关的程序和文件	
1.1	**实施 ISO9001 或等效标准的质量管理体系。**	5.1.3								
a	规定员工的职责和能力。		X	X			Ⓘ	Ⓘ		
b	实施软件和相关硬件的完整生命周期管理。		X	X			Ⓘ	Ⓘ		
c	制定对计算机系统、组件、及其版本，进行唯一标识的具体程序。		X			Ⓘ (必要时)	Ⓘ	Ⓘ		
d	创建和更新船舶计算机系统结构。			X			Ⓘ	Ⓘ		
e	设置从供应商处采购软件和相关硬件的机构。		X	X			Ⓘ	Ⓘ		
f	设置软件代码编写和验证的机构。		X				Ⓘ	Ⓘ		
g	设置船上集成之前的系统验证机构。		X				Ⓘ	Ⓘ		
h	制定在FAT和SAT时实施和批准系统的具体程序。		X	X			Ⓘ	Ⓘ		
i	创建和更新系统文档。		X			Ⓘ (必要时)	Ⓘ	Ⓘ		
j	制定船上软件修改和安装的具体程序，包括与船厂和业主的沟通流程。		X	X		Ⓘ (必要时)	Ⓘ	Ⓘ		

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
k	制定软件代码的具体验证程序。		X				Ⓘ	Ⓘ		
l	制定船舶计算机系统集成和集成系统测试的具体程序。		X	X			Ⓘ	Ⓘ		
m	制定在FAT之前软件和配置的变更管理程序。		X			Ⓘ (必要时)	Ⓘ	Ⓘ		
n	制定在FAT之后软件和配置的变更管理及记录程序。		X	X		Ⓘ (必要时)	Ⓘ	Ⓘ		
o	确定组织对自身遵守质量管理体系的跟踪检查点。检查点可以是一份要求提交的文件、一次测试、一次技术审查会或者专家评审会。		X	X			Ⓘ	Ⓘ		
1.2	**质量计划**	5.2	X	X		Ⓘ (必要时)	Ⓘ	Ⓘ		
a	具有明确的标准和指导性文件来定义计算机系统。									
b	所有的相关方（如开发人员、项目负责人等）对计算机系统进行了审查。									
c	已经建立了计算机系统的验收标准。									
d	计算机系统已经明确定义了目标和应用范围。									
e	明确了哪些软件内容已经被软件质量保证计划覆盖。									
f	规定了软件的预定用途。									
g	描述了软件开发生命周期哪部分已经被质量计划覆盖。									
h	包含了可用的参考资料。									
i	包括了项目管理结构的概要。									
j	细化了用于管理系统和软件的开发、验证、确认、使用和维护的文件。									
k	对文件进行了列表和描述。									
l	已经列出需要被质量计划评估的文件。									
m	使用的标准、实践和质量要求已被识别（如 IEC、ISO、IEEE 等标准）。									
n	描述了如何监测和保证计算机系统及过程的符合性（如追溯、报告和趋势）。									
o	明确和描述了软件管理计划在软件验证及确认中的角色。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
p	描述了对问题进行报告、跟踪和解决的方法和程序。									
q	描述了哪些工具和技术被用于支持软件质量保证活动（如检查清单、计划和报告模板、用于追溯的数据库）。									
r	讨论了通过内外部监督确保供应商的控制能满足客户的要求（如检查、评估/审核、月度状态报告）。									
s	软件的设计和开发能确保其满足特殊的设计和开发要求，即对潜在的失效条件进行预防和响应。									
t	告知业主软件变更和船上安装的流程已经明确。									
1.3	**软件可追溯性**	5.5	X	X	X	Ⓘ (必要时)	Ⓘ	Ⓘ		
a	按质量管理程序，对编程内容和数据的修改以及版本的变化进行标识并文档化。									
b	实施了计算机系统的软件/硬件的配置管理。									
c	明确了编程内容、数据的修改以及版本的变化所必须遵循的流程，并确定在文件中记录这些修改或变化。									
d	告知业主软件变更和船上安装的流程已经明确。									
e	业主如果指定系统集成商作为软件变更的负责方，应告知 CCS。									
f	软件变更影响分析结果和测试报告应提交给 CCS 备查。									
g	系统集成商可通过更新软件注册表或等效文件完成变更的记录。									
1.4	**安保策略**	5.6	X	X	X	Ⓘ (必要时)	Ⓘ	Ⓘ		
a	业主、系统集成商和系统供应商应在质量体系和程序中采取安保策略。									
b	除非经授权，否则应不能修改软件。无论是物理系统或远程控制系统，都应采取物理和逻辑安保措施以防止未经授权的或无意的修改。									
c	所有计划上船安装的固件、软件代码、可执行程序和物理媒介应在安装前进行漏洞、病毒、恶意软件等方面的安全扫描。扫描结果保存在软件注册表或等效文件中。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
2	**计算机系统技术要求**								① 对计算机系统、组件、及其版本进行唯一标识的具体程序	
2.1	**系统标识要求**	6.1	X	X			①	①		
a	提供识别系统（包括软件和硬件）名称、版本、标识和制造商的方法和应用。									
2.2	**II 类和 III 类系统数据链路要求**	6.2.1	X	X			①	①		
a	单一故障应能被自动处理以恢复系统正常运行。									
b	远程控制系统的任何功能损失应能通过本地/手动方式进行补偿。									
c	能够防止在任何工况下数据链路的通信速率过载。									
d	具有自检功能，检测自身链路故障和与链路连接的节点的通信故障。									
e	故障发生时应发出报警。									
2.3	**采用无线数据链路时的补充要求**	6.2.2	X	X			①	①		
a	III 类系统不应采用无线数据链路，除非经 CCS 特别考虑。									
b	使用认可的国际无线通信系统协议。									
c	信息完整性：通过故障预防、检测、诊断和纠正，使接收的消息与发送的消息相比，不会被破坏或更改。									
d	配置和设备认证：应仅允许与系统设计中包含的设备连接。									
e	信息加密：保护机密和/或关键数据内容。									
f	安保管理：保护网络资产，防止非法访问网络资产。									
g	船舶内部无线系统应满足国际电信联盟和船旗国主管机关对无线电频率和功率水平的要求。									
h	系统操作应考虑到港口和当地法规在射频传输方面的规定，因频率和功率的限制而禁止使用无线数据通信链路。									
i	无线数据通信设备应在系泊试验和航行试验期间进行测试，证明在预期的操作条件下，射频传输不会因电磁干扰引起自身和任何其他设备的故障。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
3	**系统说明（软件描述和相关硬件描述）**	8.2.1.3	X			① (必要时)	Ⓐ	Ⓐ	① 系统说明（可分解成相关文档） ② 计算机系统需求规格说明 ③ 计算机系统硬件说明 ④ 软件需求规格说明 ⑤ 软件结构设计规格说明 ⑥ 软件结构集成测试规格说明 ⑦ 软件模块设计规格说明 ⑧ 软件模块测试规格说明 ⑨ 软件系统设计规格说明 ⑩ 软件系统测试规格说明 ⑪ 软件集成测试规格说明 ⑫ 计算机系统集成测试规格说明 ⑬ 支持工具和编码标准 ⑭ 开发工具的选择	
3.1	**软件说明**									
a	根据系统功能要求规定了软件需求规格说明。									
b	对每个需实现一定安全功能的计算机系统规定软件安全功能的要求。									
c	定义计算机系统的系统类别。									
d	规定了每一个计算机系统对于软件集成的要求，包括通信和接口方面。									
e	软件结构设计的描述包括：在所需的软件开发生命周期中，按不同等级的系统，选择和判断满足软件需求规格说明的集成技术。									
f	软件需求文档的技术和措施包括：故障允许偏差（与硬件一致），故障避免的软件设计策略，（适用时）冗余和多样性。									
g	软件结构设计的描述包括：确定所有软件/硬件相互作用和评价，以及细化它们的重要性。									
h	软件结构设计的描述包括：规定适当的软件结构集成测试来保证软件结构满足规定系统等级上的软件安全要求。									
i	标准和命名规则已经明确。									
j	提供了软件系统设计和模块设计规格说明方面的文档。									
k	软件系统设计和模块设计文档说明了功能、性能、模块和其他部件之间的相互约束和依赖关系。									
l	软件系统设计和模块设计文档说明了软件自我监控（例如：应用驱动的看门狗和数据范围验证）。									
m	软件系统设计和模块设计文档要求进行验证测试和外部设备诊断测试（例如：传感器和终端元件）。									
n	软件系统设计和模块设计文档对坏的过程变量，如传感器值超出范围、开路、短路，采取了措施。									
3.2	**硬件说明**									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
a	包括网络架构/拓扑，包含所有网络组件，如交换机、路由器、网关、 防火墙等。									
b	包括系统所有接口和硬件节点的内部结构（例如操作站、显示器、计算机、可编程设备、传感器、执行器、I/O 模块等）。									
c	包括 I/O 分配（将现场设备映射到信道、通信链路、硬件单元、逻辑功能）。									
d	包括硬件和外部相关设备的技术规格明细表。									
e	包括电源布置。									
f	包括故障模式描述。									
3.3	**技术要求**									
a	对于 II 类和 III 类系统，系统技术要求的实施情况作为系统说明的一部分进行验证。									
4	**软件代码验证**	9.5.3	X				Ⓘ (必要时)	Ⓘ (必要时)	① 代码复审报告	
a	检查软件代码编写和它的结果是否符合详细设计文档的描述。									
b	检查软件代码是否符合软件模块设计、要求的编码标准和软件确认计划的要求。									
5	**软件模块测试**	9.5.4	X				Ⓘ (必要时)	Ⓘ (必要时)	① 软件模块测试规格说明 ② 软件模块测试记录	
a	软件模块测试活动已实现文档化。									
b	II 类、III 类系统的软件模块测试文档包括软件模块测试规格说明、软件模块测试计划、软件模块测试用例、软件模块测试记录、测试记录分析报告、软件模块测试问题报告和测试总结报告。									
c	在规定每一个软件模块设计后，验证：考虑规定的软件模块设计是否已充分满足规定的软件系统设计。									
d	在规定每一个软件模块设计后，验证：考虑每一个软件模块的规定测试是否已充分满足规定的软件模块设计。									
e	在规定每一个软件模块设计后，考虑每一个软件模块的属性是否充分满足：①所									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
	需安全性能的可行性；②进一步验证的可测试性；③对于开发团队而言的可读性；④允许进一步改进的安全修改。									
f	在规定每一个软件模块设计后，检查以下内容之间的不一致性：①软件模块设计和软件系统设计；②（对于每一个软件模块）软件模块设计和软件模块测试；③软件模块测试和软件系统集成测试。									
6	**软件集成测试**	9.5.5	X			Ⓘ (必要时)	Ⓘ (必要时)	Ⓘ (必要时)	① 软件集成测试规格说明 ② 软件集成测试记录 ③ 软件系统测试规格说明 ④ 软件系统测试记录 ⑤ 软件结构集成测试规格说明 ⑥ 软件结构集成测试记录 ⑦ 软件测试报告	
6.1	**软件集成测试一般要求**									
a	在完成软件结构设计后，验证：软件结构设计是否充分满足软件需求规格说明。									
b	在完成软件结构设计后，验证：软件结构设计规定的集成测试是否充分。									
c	在完成软件结构设计后，考虑每一个主要组件/子系统的属性是否充分满足：①所需安全性能的可行性；②进一步验证的可测试性；③对于开发团队而言的可读性；④允许进一步改进的安全修改。									
d	在完成软件结构设计后，检查下列内容的不一致性：①软件结构设计和软件需求；②软件结构设计和软件结构集成测试；③软件结构集成测试和软件确认计划。									
e	软件集成测试应规定以下内容：①将软件划分为可管理的集成集；②测试用例和测试数据；③执行测试的类型；④测试环境、工具、配置和程序；⑤判定测试完成的准则；⑥测试失败的校正措施。									
f	软件集成测试是否表明所有软件模块、组件和子系统能相互正确作用以执行其预定功能，而不执行非预定功能。									
g	软件集成测试应文档化，并说明测试结果是否满足测试目的和测试准则。如果出现失败，记录失败原因。									
h	在软件集成过程中，应对软件的任何修改或变更进行影响分析，以确定所有受影响的软件模块和所需要的再验证、再设计活动。									
6.2	**软件子系统测试附加要求**									
a	对于 II类、III 类系统，执行软件子系统测试，并分析测试结果，以验证软件模块被正确地集成。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
6.3	**软件系统测试附加要求**									
a	通过软件系统测试，验证软件系统的防修改保护功能。									
b	对于 II 类、III 类系统，执行软件系统测试，验证单一故障条件下软件系统符合故障安全原则。									
7	**计算机系统（软件和硬件）集成测试，属于系统测试**	9.6	X			①(必要时)	①(必要时)	①(必要时)	① 计算机系统集成测试规格说明 ② 计算机系统集成测试记录 ③ 计算机系统故障模拟测试规格说明 ④ 计算机系统故障模拟测试记录 ⑤ 系统测试报告	
7.1	**计算机系统集成测试一般要求**									
a	计算机系统集成测试应准备以下文件资料：①系统说明，包括软件需求规格说明；②系统安装的软件列表和版本号；③软件功能描述；④软件维护和使用手册；⑤系统和船舶其他系统之间接口的列表；⑥数据传输标准的列表。									
b	计算机系统集成测试应规定：①将系统拆分为各个集成集；②测试用例和测试数据；③执行测试的类型；④测试环境，包括工具、支持软件和配置描述；⑤判定测试完成的准则。									
c	计算机系统集成测试应验证系统以下方面：①功能；②故障和故障影响；③性能；④软件和硬件之间的集成；⑤人机界面；⑥与其他系统的接口。									
d	在进行计算机系统集成测试时，应区别开发人员按自己意图所执行的活动和从用户立场出发所进行的活动。									
e	在计算机系统集成测试中，对计算机系统的任何修改或变更进行了影响分析，以确定所有受影响的软件组件/模块，以及所需要的再验证、再设计活动。									
f	计算机系统集成测试应文档化，测试结果是否满足测试目的和测试准则。如果出现失败，应记录失败原因。									
g	对于 II 类、III 类系统，应保留并按要求向 CCS 提交计算机系统集成测试的证明文件，文件包括测试计划和测试报告。									
7.2	**计算机系统故障模拟测试要求**									
a	通过故障分析证明对于单一故障，系统能够进入故障安全状态，并且运行中的系统不会降低到不能满足 CCS 规定的可接受性能标准。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
b	应尽可能真实地进行故障模拟。故障模拟测试规格说明包括以下内容：①故障组件或元器件名称；②故障类型；③故障注入方式；④要求的故障响应（输出记录）。									
c	故障模拟的测试用例及其预期结果应文档化。应说明故障模拟测试结果以及是否满足测试目的和测试准则。如果出现失败，应记录和分析失败原因。									
8	**工厂验收测试（FAT），包括软件确认测试**	8.2.1.7 9.7							① 系统说明 ② FAT 程序 ③ FAT 报告 ④ 用户手册 ⑤ 系统测试报告等	
8.1	**编制 FAT 程序（试验大纲）**		X				Ⓐ	Ⓐ		
a	FAT 程序应从系统测试中选出具有代表性的测试项目，包括正常的功能测试和故障模拟测试（即故障响应测试）。选择测试项目的原则是：①针对软件需求规格说明，FAT 内容的完整性；②针对软件需求规格说明，FAT 内容的正确性；③可重复性；④精确定义的测试配置。									
8.2	**执行 FAT**		X				Ⓦ	Ⓦ		
a	在实际硬件上执行 FAT，并具备必要的用于模拟功能和故障响应的工具或手段。对于其他测试方案，如采用同型硬件或模拟硬件（仿真器），应征得 CCS 同意。									
b	对于 II 类和 III 类系统，应进行了网络测试，以验证其符合网络韧性要求。在征得 CCS 同意的情况下，网络测试可以作为船上测试的一部分进行。									
c	对于 II 类和 III 类系统，系统技术要求的实施情况作为 FAT 的一部分进行验证。									
d	对于 II 类和 III 类系统，拥有可信的第三方测试报告。	附录4: 2.3								
8.3	**编制 FAT 报告**		X				Ⓘ	Ⓘ		
a	FAT 报告等测试结果应进行文档化，并包括以下内容：① FAT 过程按时间顺序记录，以便追溯 FAT 活动的顺序；② FAT 程序的版本；③被 FAT 验证的软件需求；④使用的工具、设备及其校准数据；⑤ FAT 时安装在系统中的软件（包括软件版本）的列表。⑥实际结果和预期结果的差异。									
b	当实际结果和预期结果出现差异时，应进行分析和评估，确定是继续测试，还是提出变更请求，并返回软件开发生命周期的较早阶段。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
c	FAT 报告应证明所有软件规定的要求都得到了满足,并且软件不执行非预定的功能。FAT 报告还应还表明：(a)软件已通过测试；或(b)未通过测试的原因。									
8.4	**其他 FAT 文件**		X				Ⓘ (必要时)	Ⓘ (必要时)		
a	其他 FAT 文件，如用户手册、系统测试报告等，必要时提交给 CCS 备查。									
9	**硬件的环境合规性要求**	8.2.1.4	X			Ⓘ (必要时)	Ⓘ	Ⓘ	① 环境符合性测试报告或型式认可证书。	
a	符合 CCS《电气电子产品型式认可试验指南》要求的环境符合性测试报告或型式认可证书。									
10	**船上测试前的准备工作**								① 系统说明 ② 系统类别清单 ③ 风险评估报告 ④ 系统结构说明 ⑤ FAT 报告 ⑥ 用户手册	
10.1	**系统类别清单**	8.2.2.3		X		Ⓐ	Ⓐ	Ⓐ		
a	根据系统的故障影响确定系统属于哪个类别，并形成系统类别清单。									
10.2	**风险评估报告**	8.2.2.4		X		Ⓐ (必要时)	Ⓐ (必要时)	Ⓐ (必要时)		
a	如果 CCS 提出要求，系统集成商应对船舶的特定系统进行风险分析，形成风险评估报告，以确定系统的适用类别。									
b	若基于风险评估分析修正了系统类别，可能需要获得 CCS 和系统供应商的同意。									
c	当计算机系统的风险显而易见时，允许免除提交风险评估报告，但应提交证明文件以说明免除的理由。此时 d、e 条不适用。									
d	采用了适当的分析方法，如故障树分析、风险分析、 FMEA 或 FMECA 分析；（c 条生效时，本条不适用）									
e	通过故障分析证明：对于单一故障，系统能够进入故障安全状态，并且运行中的系统不会降低到不能满足 CCS 规定的可接受性能标准。（c 条生效时，本条不适用）									
f	风险评估分析中应明确 II 类和 III 类系统数据链路失效的状况。（适用时）									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
10.3	**系统结构说明**	8.2.2.5		X		Ⓘ	Ⓘ	Ⓘ		
a	应规定船舶的计算机集成系统（System of systems），并形成系统结构说明。									
b	系统结构说明应至少包含以下内容：①整个系统结构的概述（集成系统）；②每个系统的用途和主要功能；③不同系统之间的通信和接口。									
11	**船上测试**	8.2.2.6 8.2.2.7							① SAT 程序 ② SAT 报告 ③ SOST 程序 ④ SOST 报告	
11.1	**编制船上测试程序（试验大纲）**			X			Ⓐ	Ⓐ		
a	船上测试程序包括设计功能验证。									
b	船上测试程序包括内部故障或外部系统设备故障引发的安全响应验证。									
c	船上测试程序包括和船舶上其他系统间安全互连的验证。									
d	船上测试程序包括系统验收测试程序和集成系统测试程序。当测试范围相似时，可以将这两项测试合并为一项。									
11.2	**执行船上测试**			X			Ⓦ	Ⓦ		
a	在计算机系统安装之后，并与船上相关机械/电气/过程系统，包括与其他控制和监测系统之间可能存在的接口集成之后，进行系统验收测试（SAT），以验证计算机系统的功能运行情况。									
b	不同计算机系统在船上最终环境中安装和集成之后，进行整船的集成测试（即集成系统测试，SOST），以验证不同系统在完整安装之后的功能，包括所有接口和相互依赖关系是否符合要求和规定。SOST 应至少验证以下几个方面：①集成系统的整体功能；②系统之间的故障响应符合故障安全原则；③性能；④人机界面；⑤不同系统之间的接口和互连。									
c	无线数据通信设备应在系泊试验和航行试验期间进行测试，证明在预期的操作条件下，射频传输不会因电磁干扰引起自身和任何其他设备的故障。									
d	对于 II 类和 III 类系统，技术要求的实施情况作为 SAT 的一部分进行验证。									
e	根据 CCS 要求，可能会对 II 类和 III 类系统进行网络测试，以验证其符合网络韧性要求。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
11.3	**编制船上测试报告**			X			①	①		
a	根据测试情况生成船上测试报告，包括 SAT 报告和 SOST 报告。									
b	船上测试报告应包含对被测软件的总体评价。									
c	给出测试环境与实际操作环境的差异、以及这种差异对测试结果的影响评估。									
d	测试总结应包含“所有结果都符合预期”、“遇到的问题”（如适用）和“与要求的偏差”（如适用）。									
12	**计算机系统的变更验证**	8.4 9.8							① 变更管理程序 ② 变更请求或变更说明 ③ 变更影响分析结果 ④ 变更记录 ⑤ 相应测试报告	
12.1	**一般验证要求**		X	X	X	① (必要时)	①	①		
a	系统供应商和系统集成商应对已批准系统的变更方案进行影响分析，同时在必要时向 CCS 报备。影响分析包括：①确定变更的后果；②确定对现有文件的影响；③确定所需的验证和测试活动；④确定是否需要将变更告知其他利益相关方；⑤确定变更前是否需要获得其他利益相关方（如 CCS 和/或业主）的批准。									
b	根据变更影响分析结果，返回软件开发生命周期的合适阶段。									
c	应明确规定如何对船上计算机系统的软件和数据进行备份和恢复。在系统维护过程中，应能将软件回滚到以前安装的版本，目的是使系统恢复到已知的稳定状态。应记录和分析回滚，以发现和消除导致变更失败的根源。									
d	变更应尽可能在安装到船上之前进行验证。变更安装之后，应根据文档化的验证程序在船上进行验证，包括：①验证新功能和/或改进是否达到预期效果；②通过回归测试，验证变更没有对不该受到影响的功能或能力产生任何负面影响。									
e	对系统和软件的变更应形成记录，以保证变更的可见性和可追溯性。变更记录应至少包括以下内容：①变更目的；②变更说明；③变更影响分析的主要结论；④任何新系统或软件的标识和版本；⑤测试报告或测试总结。软件变更情况可以记录在软件注册表或同类文件中。									
f	在船舶建造阶段（ FAT 期间和之后），CCS 会结合变更管理程序在具体项目中的实际应用情况进行验证。									

序号	要　求	参考条目	系统供应商	系统集成商	业主	Ⅰ类系统	Ⅱ类系统	Ⅲ类系统	需提供的文件	是否满足
g	在船舶营运阶段，CCS 通常在船舶年度检验时对变更进行验证。检验时，业主应向 CCS 提供变更管理程序和相关变更记录。									
12.2	**重大变更附加验证要求**									
a	系统供应商和系统集成商对 II 类和 III 类系统的软件进行的后续重大变更应提交给 CCS 批准。		X	X			Ⓐ	Ⓐ		
b	对于 II 类和 III 类系统，CCS 应见证软件重大变更的验证过程。			X			Ⓦ	Ⓦ		

注 1：表中采用的符号及其含义如下:

Ⓐ 提交 CCS 批准　　Ⓘ 提交 CCS 备查　　Ⓦ 需 CCS 见证

注 2：如果表中具体要求项的“角色”和“系统类别”没有提出要求（空白），那么则采用其标题项的要求。

注 3：根据实际情况，可以对表中的具体要求项进行裁剪。

注 4：表中“需提供的文件”，可以合并或分解，也可以使用其他名称，只要拥有本指南要求的内容即可。

注 5：表中“是否满足”填写的标志含义：X 通过；O 没有通过；- 不适用。“没有通过”或“不适用”的要求项，可以留空，不填写标志。

测试和验证的认可结论：_____

认可人员：_____　认可日期：_____

附录 2　小型低复杂度计算机系统的评估

1　目的

1.1　通过对小型低复杂度计算机系统的单案评估，对其软件评估方法进行合理有效的简化。

2　要求

2.1　文档

2.1.1　软件说明可根据系统供应商和系统集成商的内部文件管理系统，将表 10.1 中需要提供的文件合并，但内容应包括：

(1) 系统功能描述，包括软件模块功能描述和相关可编程设备硬件描述、系统和船舶其他系统之间接口的列表、数据传输标准的列表，特别是功能、性能、模块和其他部件之间的相互约束和依赖关系；

(2) 软件设计说明，包括软件功能描述、软件维护和使用手册，特别是软件的配置，其中包括优先级策略；

(3) 系统安装的软件列表和版本号；

(4) 失效模式分析；

(5) 冗余系统的切换机制（若有）；

(6) 系统测试、集成测试和故障模拟测试方法。

2.2　测试

(1) 对新设计的产品，应核查其失效模式分析，并按经确认的系统供应商和系统集成商提供的试验方法进行测试。

(2) 提供软件模块、子系统和系统层级的可编程设备功能测试证据和集成测试证据。

(3) 对软件复用或修改，还应注意回归测试。

注：软件复用是将已有软件的各种有关知识用于建立新的软件，以缩减软件开发和维护的花费。软件复用是提高软件生产力和质量的一种重要技术。软件复用主要是代码级复用，被复用的不专指程序，也包括领域知识、开发经验、设计决定、体系结构、需求、设计、代码和文档等一切有关方面。

3　输入

3.1　计算机系统需求规格说明

4　输出

4.1　软件说明

4.2　硬件说明

4.3　测试报告

附录 3　计算机系统设计和实现阶段的技术建议

1　一般要求

1.1　计算机安全相关系统的设计（包括软、硬件的整体结构、传感器、执行器、可编程电子、嵌入式软件和应用软件等，见下图），应当符合以下 1.1.1～1.1.2 的全部要求：

1.1.1　硬件安全完整性要求包括：

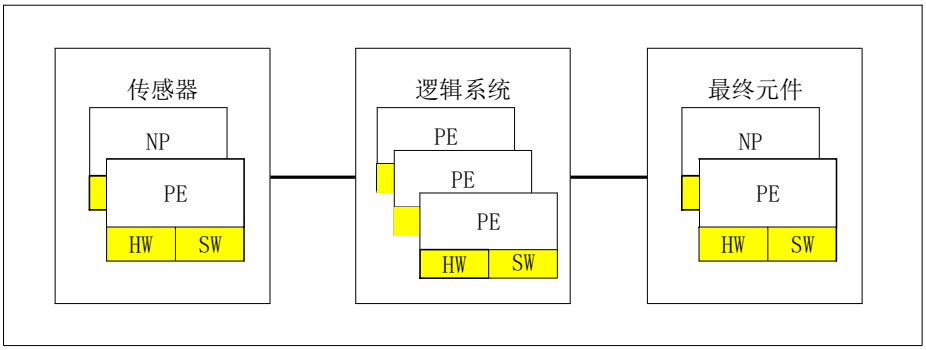
(1)　硬件安全完整性的结构约束；和

(2)　危险随机硬件失效概率的要求。

1.1.2　系统安全完整性要求包括：

(1)　避免失效的要求和系统故障控制的要求；或

(2)　设备“经使用证实”的证据。



可编程电子结构		
PE 硬件结构	PE 软件结构	
	PE 嵌入式软件	PE 应用软件
PE 硬件中通用的和应用时的具体特性： 例如包括： ——诊断测试； ——冗余处理器； ——双 I/O 卡	例如包括： ——通信驱动器； ——故障处理； ——可执行软件	例如包括： ——输入/输出功能； ——派生功能 （例如，未提供嵌入式软件服务时的传感器检验）

PE：可编程电子，NP：非可编程装置，HW：硬件，　SW：软件。

图附录 3-1.1.2　PE 硬件和软件结构的关系

1.2　在计算机系统既执行安全功能又执行非安全功能的部分，除非能够表明实现安全功能和非安全功能是充分独立的（也就是说，非安全功能的失效不会引起安全功能的危险失效），否则都应被视为与安全相关的。只要可行，安全功能应与非安全功能分开。

1.3　计算机系统由拥有最高安全完整性等级的安全功能的安全完整性等级来决定，除非能够表明不同安全完整性等级的安全功能的实现是充分独立的。

1.4　如要求安全功能之间相互独立（见 1.2 和 1.3），在设计时以下几条应文档化：

1.4.1　达到独立的方法；

1.4.2　方法的合理性证明。

2　硬件安全完整性的技术和措施：操作中的失效控制

附录 3 表 2-1～附录 3 表 2-6 给出了有关硬件安全完整性技术和措施的建议。

附录 3 表 2-1　I/O 单元和接口（外部通信）

诊断技术/措施	见 IEC61508-7	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
测试模式	A6.1	高	
代码保护	A6.2	高	
多通道并行输出	A6.3	高	仅当诊断测试间隔内数据流改变时才有效
监视输出	A6.4	高	仅当诊断测试间隔内数据流改变时才有效

附录 3 表 2-2　数据通路（内部通信）

诊断技术/措施	见 IEC61508-7	经考虑能达到的最大诊断覆盖率	注
一位硬件冗余	A7.1	低	
多位硬件冗余	A7.2	中	
完全硬件冗余	A7.3	高	
使用测试模式进行检查	A7.4	高	
传输冗余	A7.5	高	仅对瞬时故障有效
信息冗余	A7.6	高	

附录 3 表 2-3　电源

诊断技术/措施	见 IEC61508-7	经考虑能达到的最大诊断覆盖率	注
使用安全断电或切换到备用电源单元的过压保护	A8.1	低	应使用本表中的技术，也推荐使用其他技术。
使用安全断电或切换到备用电源单元的电压控制(次级)	A8.2	高	
带安全断电或切换到备用电源单元的断电	A8.3	高	应使用本表中的技术，也推荐使用其他技术。
无功电流的原则	A1.5	低	仅对断电有用

附录 3 表 2-4　程序序列（看门狗）

诊断技术/措施	见 IEC61508-7	经考虑能达到的最大诊断覆盖率	注
具有分离时基但无时间窗的看门狗	A9.1	低	
具有分离时基和时间窗的看门狗	A9.2	中	
程序序列的逻辑监视	A9.3	中	依赖于监视质量
程序序列的时序和逻辑监视的组合	A9.4	高	
具有在线检验的时序监视	A9.5	中	

附录 3 表 2-5　传感器

诊断技术/措施	见 IEC61508-7	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
无功电流的原则	A1.5	低	仅对无需连续控制、未达到或保持 EUC 安全状态的 E/E/PE 安全相关系统才有效
模拟信号监视	A2.7	低	
测试模式	A6.1	高	
输入比较/表决	A6.5	高	仅当诊断测试间隔内数据流改变时才有效
参考传感器	A12.1	高	依赖于失效检测的诊断覆盖率
可靠开启的开关	A12.2	高	

附录 3 表 2-6　最终元件（执行器）

诊断技术/措施	见 IEC61508-7	经考虑能达到的最大诊断覆盖率	注
利用在线监视检测失效	A1.1	低（低要求模式） 中（高要求或连续模式）	依赖于失效检测的诊断覆盖率
继电器触点监视	A1.2	高	
无功电流的原则	A1.5	低	仅对无需连续控制、未达到或保持 EUC 安全状态的 E/E/PE 安全相关系统才有效
测试模式	A6.1	高	
监视	A13.1	高	依赖于失效检测的诊断覆盖率

多个执行器的交叉监视	A13.2	高	

3 系统完整性的技术和措施的建议

3.1 附录 3 表 3.1-1、附录 3 表 3.1-2 给出了有关系统安全完整性技术和措施的建议。

3.1.1 控制由硬件和软件设计引起的失效；

3.1.2 控制由环境应力或影响引起的失效；

3.1.3 控制操作过程的失效。

附录 3 表 3.1-1 用于控制由硬件设计引起的系统失效的技术和措施

	技术/措施	见 IEC61508-7	I	II	III
1	程序序列监视	A.9	极力推荐（注1） 低（注2）	极力推荐 低	极力推荐 中
2	利用在线监视检测失效	A1.1	推荐 低	推荐 低	推荐 中
3	利用冗余硬件进行测试	A2.1	推荐 低	推荐 低	推荐 中
4	访问端口和边界扫描结构的标准测试	A2.1	推荐 低	推荐 低	推荐 中
5	代码保护	A6.2	推荐 低	推荐 低	推荐 中
6	多种硬件	B1.4	– 低	– 低	推荐 中
注：要求至少应用一种 2～6 中的技术。 注 1：技术/措施的重要程度，包括必须采用、极力推荐、推荐、-(既不推荐，也不反对）。 注 2：采用的技术/措施，应至少达到的有效性，包括低、中、高。					

附录 3 表 3.1-2 用于控制由环境应力或影响引起的系统失效的技术和措施

	技术/措施	见 IEC61508-7	I	II	III
1	防止电压击穿、电压波动、过压、低压的措施	A8	极力推荐	必须采用	必须采用
2	分隔开电力线和信号线（注1）	A11.1	极力推荐	必须采用	必须采用
3	提高抗干扰性	A11.3	极力推荐	必须采用	必须采用
4	抗物理环境（如温度、湿度、振动等）的措施	A14	极力推荐	必须采用	必须采用
5	程序序列监视	A9	极力推荐 低	极力推荐 低	极力推荐 中
6	抗温升措施	A10	极力推荐 低	极力推荐 低	极力推荐 中
7	多线路的空间分隔	A11.2	极力推荐 低	极力推荐 低	极力推荐 中

8	利用在线监视检测失效（注2）	A1.1	推荐 低	推荐 低	推荐 中
9	利用冗余硬件进行测试	A2.1	推荐 低	推荐 低	推荐 中
10	代码保护	A6.2	推荐 低	推荐 低	推荐 中
11	反价信号传输	A11.4	推荐 低	推荐 低	推荐 中
12	多种硬件（注3）	B1.4	– 低	– 低	– 中
13	软件结构	GB/T20438.3 的 7.4.3	见 GB/T20438.3 的表 A.2		

注：要求至少应用一种 8～13 中的技术。

注 1：若信息传输采用光介质，则无需分离电力线和信号线。对于为系统组件供电和为这些组件传送信息而设计的低功率电缆,也无需分离电力线和信号线。

注 2：对于在低要求工作模式下工作的安全相关系统（例如紧急关闭系统），通过在线监视检测失效所达到的诊断覆盖率通常为低或无。

注 3：若通过确认和广泛工作经验证明：为满足目标失效量，硬件充分避免了设计故障并足以防止共因失效，则不需要多种硬件。

附录 4　开发阶段的软件测试要求

1　软件测试问题等级

软件测试问题分为：致命问题、严重问题、一般问题、轻微问题、改进建议。开发完成的软件不能出现致命问题和严重问题。

(1) 致命问题：必然导致重大的软件任务无法完整完成的软件问题，或导致系统重要工作过程中出现死机的软件问题。

(2) 严重问题：可能导致软件任务无法完整完成的软件问题，或导致软件任务完成受到部分影响的软件问题。

(3) 一般问题：虽然不影响软件任务的完成，但对软件的功能、性能、可靠性、安全性等重要质量特性有影响的软件问题；或难以断定软件的外在影响，但程序代码本身存在严重性缺陷的软件问题。

(4) 轻微问题：虽然不影响软件的功能、性能、可靠性、安全性等重要质量特性，但对软件的易用性、效率、维护性、可移植性等一般特性有影响的软件问题；或难以断定软件的外在影响，但程序代码本身存在非严重性缺陷的软件问题。

(5) 改进建议：对软件使用无影响，但对软件的规范性、清晰性、易理解性等可进一步完善的问题，或其他建设性的意见。

2　相关方的软件测试要求

2.1　在软件开发生命周期内，计算机系统的软件测试依据实施主体可以分为：开发方测试、第三方测试、以及验收测试。

2.2　开发方测试

开发方测试的一般要求如下：

(1) 开发方测试的实施主体为软件承制方。软件承制方通常是系统供应商或子供应商。

(2) 开发方测试一般需进行软件模块测试、软件集成测试、计算机系统集成测试和软件确认测试。

(3) 开发方应对测试发现的问题进行分类和处理。

(4) 软件变更后，开发方需进行相应级别的回归测试。

(5) 测试过程产生的文档应纳入配置管理。

(6) 针对不同的测试级别，开发方测试产生的文档至少包括：测试计划、测试记录和测试报告（可含软件问题，也可采用独立的软件问题报告）。

2.3　第三方测试

第三方测试的一般要求如下：

(1) 第三方测试的实施主体为 CCS 的软件测试实验室，或经 CCS 认可的专业软件测试机构。

(2) 对于 II 类和 III 类计算机系统的软件应进行第三方测试。

(3) 测试过程产生的文档应纳入配置管理。

(4) 第三方测试的准入条件：

① 被测件包括软件（源代码、可执行程序、项目文件、配置文件），项目任务书，软件需求规格说明，设计规格说明、以及必要的通讯协议、模型公式、用户手册/使用说明等；

② 被测件及相关文档应出自受控库或产品库。

(5) 对发现的软件问题应按照问题属性和问题等级进行分类。

(6) 第三方测试发现问题的处理过程如下：

① 第三方以软件问题报告的形式正式向软件承制方提交测试中发现的软件问题。

② 软件承制方确认软件问题，填写处理意见，返给第三方测试机构。

③ 软件承制方对软件修改后，提交被测件和变更影响分析结果。第三方对修改后的软件进行回归测试。

(7) 针对不同级别的测试，第三方测试产生的文档至少包括：测试计划、测试记录和测试报告（可含软件问题，也可采用独立的软件问题报告）。

2.4 验收测试

验收测试属于软件确认活动，一般要求如下：

(1) 验收测试的实施主体为软件交办方。软件交办方通常是系统集成商或者业主。

(2) 验收测试的被测件应出自受控库或产品库。

(3) 验收测试一般需对软件的功能、性能和接口进行测试，必要时，对安全性进行测试。

(4) 验收测试应对发现的软件问题进行分类和处理。

(5) 对于验收测试中发现的软件问题应详细填写软件问题报告单，并及时通知软件承制方。

(6) 验收测试产生的文档至少包括：测试计划、测试记录和测试报告（可含软件问题，也可采用独立的软件问题报告）。

3 软件测试工具和测试环境

3.1 测试工具

(1) 应根据测试要求和测试项目的特点选择合适的测试工具，包括采购的商用测试工具和自行开发的测试工具。

(2) 应采取技术手段保证自行开发的测试工具的功能、性能达到要求。

(3) 用于有指标或量程要求的软件测试工具在投入使用前应对其适用范围进行校核。

(4) 对软件测试工具进行管理，应具有对软件测试工具进行版本控制、升级以及技术支持的方法。

3.2 测试环境

(1) 测试环境包括被测软件的运行环境和测试用况（仿真）环境。

(2) 若测试项目对运行环境有特定的要求，可为此自行研制（包括部分自行研制或二次开发）特定的测试环境来进行测试；也可使用软件开发方或应用方的特定环境来进行测试。

(3) 应对软件测试环境和真实运行环境的差异性进行分析，一般宜考虑数据、外部接口、系统负载等方面的差异性。

(4) 在进行软件确认时，被测软件应在真实系统工作环境或相容的系统运行环境里运行。若选择仿真或模拟测试环境，应加以论证，并获得 CCS 的同意。

4 软件测试类型

根据软件的测试级别和测试需求，选择下面合适的软件测试类型。本指南所列的软件测试类型并未详尽。

4.1 文档审查

依据文档检查单对被测软件文档进行审查，一般包括以下内容：

(1) 审查文档齐全性；

(2) 审查文档标识和签署的完整性；

(3) 审查文档内容的完备性、准确性、一致性、可追踪性；

(4) 审查文档格式的规范性。

4.2 代码审查

依据代码检查单对被测软件进行审查，一般包括以下内容：

(1) 审查工程文件的完整性、一致性；

(2) 审查代码和设计的一致性；

(3) 审查代码执行标准的情况；

(4) 审查代码逻辑表达的正确性；

(5) 审查代码结构的合理性；

(6) 审查代码的可读性；

(7) 审查约束文件的符合性。

4.3 代码走查

根据代码逻辑查找被测软件缺陷，一般包括以下内容：

(1) 对至少一个完整的功能模块或完整的专题进行走查；

(2) 人工检查代码逻辑，记录走查结果；

(3) 必要时，可以画出结构图、状态迁移图和时序关系图等。

4.4 静态分析

静态分析是一种对代码的机械性的和程序化的特性分析方法，一般要求如下：

(1) 静态分析应明确分析工具的名称和版本；

(2) 静态分析的主要内容包括：

① 控制流分析；

② 数据流分析；

③ 接口分析；

④ 表达式分析；

⑤ 代码静态质量度量；

⑥ 编码规则检查。

4.5 功能测试

功能测试是对软件需求规格说明或设计规格说明中的功能需求逐项进行的测试，以验证其功能是否满足要求。

功能测试的一般要求如下：

(1) 通过等价类分析确定软件的输入；

(2) 输入等价类应包括正常等价类和非正常等价类；

(3) 功能测试可结合其它测试类型一起进行，如：边界测试、强度测试、安全性测试等；

(4) 在做计算机系统集成测试或软件确认测试时，应对控制流程的正确性、合理性进行验证。

4.6 性能测试

性能测试是对软件需求规格说明或设计规格说明中的性能需求逐项进行的测试，以验证其性能是否满足要求。

性能测试的一般要求如下：

(1) 针对精度性能和时间性能进行测试：

① 针对具有数据精度要求的功能，测试出实际数据处理的精度值；

② 针对具有时间精度要求的功能，测试出实际时间响应的精度值。

(2) 测试为完成功能所需处理的数据量；

(3) 测试软件运行所占用的空间；

(4) 测试软件与硬件的集成性能；

(5) 测试计算机系统对并发事务和并发用户访问的处理能力；

(6) 测试结果应得到具体的量化数值，应至少得到3组实测值；

(7) 给出性能测试的最大值、最小值、平均值的统计结果；

(8) 性能测试可结合其他测试类型一起进行，如：余量测试、强度测试等。

4.7 接口测试

对软件需求等文档中规定的各个接口进行测试，一般包括以下内容：

(1) 针对所有的外部接口进行测试，并检查接口实现的正确性；

(2) 接口的每个特性至少被一个正常测试用例和一个被认可的异常测试用例所覆盖；

(3) 测试不同的接口数据、通信速率、错误类型等对软件功能和性能的影响。

4.8 强度测试

在软件运行正常至发生故障的过程中，用于检验软件在扩展情况下可工作的临界点，一般包括以下内容：

(1) 提供最大处理的信息量；

(2) 提供数据处理能力的饱和实验指标；

(3) 在错误状态下进行软件反应的测试；

(4) 在规定的持续时间内，进行连续非中断的测试。

4.9 余量测试

余量测试是对软件是否到达需求规格说明中要求的余量的测试。如无明确特殊要求，一般应有20%以上的余量。

余量测试应对时间余量、空间余量、传输余量进行测试，一般要求如下：

(1) 针对具有时间约束要求的功能，应测试出实际执行时间相对于时间约束要求的余量；

(2) 针对具有空间约束要求的功能，应测试出实际占用空间相对于空间约束要求的余量；

(3) 针对外部通讯接口，应测试出实际传输时间、传输数据量相对于硬件配置能力的余量。

4.10 边界测试

边界测试是对软件处在边界或端点情况下运行状态的测试，一般要求如下：

(1) 对输入域或输出域的边界或端点进行测试；

(2) 对状态转换的边界或端点进行测试；

(3) 通常是针对整数域空间进行测试，但对数目极大而无法穷尽的实数域也应进行边界测试；

(4) 边界测试可结合其它测试类型一起进行，如功能测试、性能测试。针对功能/性能界限的边界或端点进行测试。

4.11 人机交互界面测试

人机交互界面测试的一般要求如下：

(1) 测试操作和显示界面与软件需求规格说明中要求的一致性和符合性；

(2) 以非常规操作、误操作、快速操作来检验人机界面的健壮性；

(3) 测试对错误命令或非法数据的检测能力与提示情况；

(4) 测试对错误操作流程的检测与提示；

(5) 依据用户手册或操作手册，逐条验证文实一致性；

(6) 人机交互界面测试可结合其它测试类型一起进行，如：功能测试、性能测试、边界测试等。

4.12 恢复性测试

对有恢复或重置功能的软件的每一类导致恢复或重置的情况逐一进行测试，以验证其恢复或重置功能。恢复性测试是要证实在克服硬件故障后，系统能否正常继续进行工作，且不对系统造成任何损害。

恢复性测试的一般要求如下：

(1) 对软件探测错误的功能进行测试；

(2) 对出现故障后通过容错措施恢复正常工作的能力进行测试；

(3) 对失效后通过自复位或备机切换等措施恢复继续工作的能力进行测试；

(4) 对系统失效后重新运行时软件依据记录数据恢复续接式工作的能力进行测试；

(5) 恢复性测试可结合其他测试类型一起进行，如：安全性测试、功能测试、性能测试等。

4.13 安全性测试

安全性测试是检验软件中已存在的安全性、安全保密性措施是否有效的测试。测试应尽可能在符合实际使用的条件下进行。

安全性测试的一般要求如下：

(1) 进行软件安全性分析，并且在软件需求中明确每一个危险状态及导致危险的可能原因，在测试中全面检验软件在这些危险状态下的反应；

(2) 对软件安全性需求中确定的软件故障模式进行测试；

(3) 对软件可靠性安全性设计准则的实现情况进行测试；

(4) 应对软件设计中用于提高安全性的结构、算法、容错、冗余、中断处理等方案进行测试；

(5) 应对可能的异常事件进行测试，包括：

① 可能的硬件异常事件；

② 可能的软件异常事件；

③ 可能的操作异常事件；

④ 可能的输入异常事件。

(6) 测试应尽可能在符合实际使用的条件下进行；

(7) 除在正常条件下测试外，应在异常条件下测试软件，以表明不会因可能的单个或多个输入错误而导致不安全状态；

(8) 应包含硬件及软件输入故障模式测试；

(9) 应包含边界、界外及边界接合部的测试；

(10) 应包括“0”、穿越“0”以及从两个方向趋近于“0”的输入值；

(11) 应包含在最坏情况配置下的最小和最大输入数据率，以确定系统的固有能力及对这些环境的反应；

(12) 操作员界面测试应包括在安全性关键操作中的操作员错误，以验证系统对这些错误的响应；

(13) 测试双工切换、多机替换的正确性和连续性；

(14) 对重要数据的安全保护能力进行测试；

(15) 安全性测试可结合其它测试类型一起进行，如：接口测试、强度测试、恢复性测试等。

4.14 逻辑测试

利用软件内部的逻辑结构及有关信息，设计或选择测试用例，对逻辑路径进行测试，检查软件状态，确定实际状态是否与预期状态一致，一般包括以下内容：

(1) 语句覆盖；

(2) 分支覆盖；

(3) 条件覆盖，

(4) 表达式覆盖；

(5) 位翻转覆盖；

(6) 状态机覆盖。

4.15　时序测试

在典型工况、最大工况和最小工况下，对软件的时延、建立时间、保持时间等指标进行测试，一般包括以下内容：

(1) 测试建立、保持时间是否满足要求；

(2) 测试时序控制信号相位、时延、电平宽度等是否满足要求；

(3) 测试脉冲信号的频率、占空比等是否满足要求。

4.16　功耗分析

对被测软件运行时所消耗的功率进行分析，一般包括以下内容：

(1) 在额定工作频率、工作电压、环境温度、输入信号频率、输出负载电容和驱动电流、内部信号的翻转率等约束条件下，进行功耗分析；

(2) 在额定运行时间条件下，进行功耗分析。