ICS 35.020
CCS L 70

T/CASME

团　　体　　标　　准

T/CASME XXX—2024

自动化控制软件开发项目管理规范

Project management specification for automation control software development

（征求意见稿）

2024－XX－XX 发布　　2024－XX－XX 实施

中国中小商业企业协会　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由扬州菁添勤科技有限公司提出。

本文件由中国中小商业企业协会归口。

本文件起草单位：扬州菁添勤科技有限公司……

本文件主要起草人：……

自动化控制软件开发项目管理规范

1 范围

本文件规定了自动化控制软件开发项目（以下简称“项目”）管理的概述、项目保障、过程管理、软件安全、评价与改进。

本文件适用于自动化控制软件开发项目的管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 20032 项目风险管理 应用指南

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 23691 项目管理 术语

GB/Z 23692 项目管理 框架

GB/T 25058 信息安全技术 网络安全等级保护实施指南

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 37507 项目管理指南

GB/T 41831 项目管理专业人员能力评价要求

GA/T 708 信息安全技术 信息系统安全等级保护体系框架

GA/T 709 信息安全技术 信息系统安全等级保护基本模型

GA/T 710 信息安全技术 信息系统安全等级保护基本配置

GA/T 1389 信息安全技术 网络安全等级保护定级指南

GA/T 1390（所有部分） 信息安全技术 网络安全等级保护基本要求

3 术语和定义

GB/T 20032、GB/T 23691、GB/T 37507、GB/T 20032界定的术语和定义适用于本文件。

4 概述

4.1 管理要素

4.1.1 项目管理要素包括项目管理对象、项目管理过程、项目成果三个方面。项目管理队应根据项目管理对象的要求及约束条件，通过执行项目管理过程中的活动产生项目成果，实现项目建设目标。

4.1.2 项目管理过程根据项目阶段的划分及项目活动的特点，分为启动过程组、规划过程组、执行过程组、监督与控制过程组、收尾过程组，每个过程组包括一系列活动，作用于项目全生命周期的各个阶

段，项目管理过程遵循 P（计划）-D（执行）-C（检查）-A（行动）循环。

4.1.3　项目成果包括项目建设成果与项目管理过程成果，项目建设成果包括采购的硬软件设备、可运行的软硬件系统、设计文档、用户手册、咨询报告、运维手册等及可执行程序或源代码；项目管理过程成果包括立项报告、招标文件、投标文件、合同、项目实施计划、项目周报、评审记录、变更记录、会议纪要等。

4.2　项目过程

项目过程如图1所示。

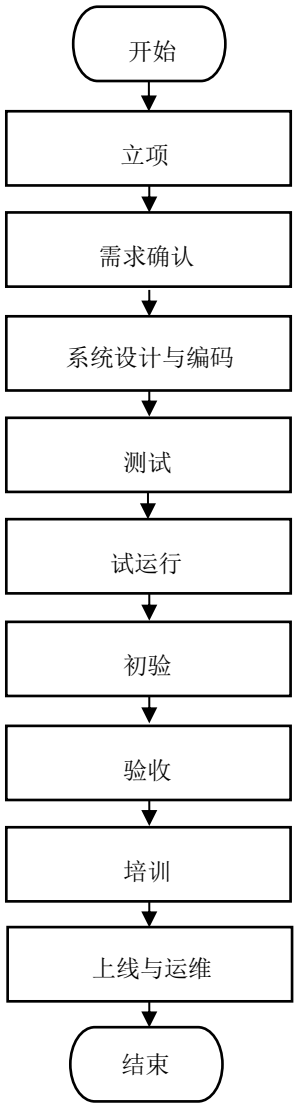

图1　项目过程示意图

4.3　项目管理方法

4.3.1　总则

项目管理应利用技术与工具体现“可视化管理”的要求，包括模板管理、需求管理、评审管理、绩效管理，管理方法关系如图2所示。

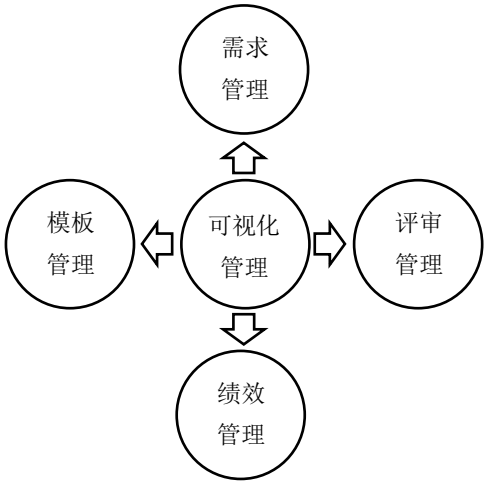

图2　项目管理方法

4.3.2　模板管理

活动开始时确定对于项目过程中的关键活动的主要工作模板，项目管理组基于模板对项目过程进行管理与控制。

4.3.3　需求管理

利用需求跟踪矩阵保证需求在项目全生命周期内的延续性与一致性，利用原型技术保证需求的可视化。

4.3.4　评审管理

利用评审技术对于关键技术进行论证，确保技术方案的可行性，评审方式包括文档审核与会议审核两种形式，必要时可请外部专家参加评审。

4.3.5　绩效管理

在项目启动阶段明确项目的应用目标，并作为项目绩效考核的核心指标，建立项目工作组在项目的全生命周期中围绕应用目标指导各个阶段的工作。

5　项目保障

5.1　通则

5.1.1　应按 GB/T 37507 的规定进行项目管理工作。

5.1.2　宜按 GB/Z 23692 制定项目管理框架。

5.1.3　项目管理人员宜具备 GB/T 41831 规定的第二级及以上的专业技能能力。

5.2　岗位职责

5.2.1　项目领导小组

由高层领导组成，负责项目高层决策、资源协调、绩效考核等工作。

5.2.2 技术总监

负责项目的日常管理工作，审核项目立项报告，负责对项目的立项批准、资源安排、变更决策及项目验收工作；负责项目的日常监理工作，负责项目技术方案的审批。

5.2.3 项目经理

负责项目的日常管理工作，负责组织完成项目的立项报告工作，负责项目的全过程管理，包括项目计划管理、需求报告编写、方案设计、编程管理、测试管理、试用管理、项目总结等。

5.2.4 项目成员

分组对项目进行需求跟踪、设计开发、数据处理、项目实施、软件测试、硬件配置、使用培训等工作。

5.3 风险控制

5.3.1 风险分类

项目主要风险如下：

a) 项目外部风险：
   1) 社会环境风险：国际、国内经济技术的波动、自然灾害等；
   2) 管理风险：项目的管理职能与管理对象状况及其可能的变化带来的风险，如管理组织、领导素质、管理计划等因素。
b) 项目内部风险：
   1) 技术风险：由与项目相关的技术因素的变化而给项目建设带来的风险，包括技术成熟性、技术复杂性、与其他项目的相关性、技术性能、技术费用和技术进度等；
   2) 费用风险：由项目任务要求不明确，或受技术和进度等因素的影响而可能给项目费用带来超支的可能性，包括任务要求明确性、技术风险影响、进度风险影响、成本预算准确性、合同类型影响、合同报价影响等；
   3) 进度风险：由不确定性因素的存在而导致项日完工期拖延的风险，包括技术因素、计划合理性、资源充分性、项目人员经验等。

5.3.2 风险管理

风险管理应按GB/T 20032的规定进行。

5.4 保密

5.4.1 保密制度

应建立项目保密制度，如保密管理制度、商业秘密载体保密管理制度、涉密信息系统和保密管理制度、保密要害部门部位保密管理制度、涉密人员保密教育和管理制度、涉密案件报告查处制度、保密会议制度、保密工作责任制考核制度等。保密制度应根据项目状态及时修订完善。

5.4.2 保密责任制

应建立密责任制，包括保密工作责任制、涉密人员责任制、定密责任制、保密要害岗位负责人及工作人员责任制、涉密信息系统管理和维护人员责任制、保密工作机构和保密干部落实情况等。

5.5 安全保障

5.5.1 网络安全

5.5.1.1 应制定网络安全防护策略，包括通信平台安全、网络平台安全、系统平台安全、应用软件安全。

5.5.1.2 安全设计重点关注应用层面的安全问题及与各安全支撑平台的集成。应用层面的安全包括权限控制、数据存储加密、数据传输加密、防恶意攻击、防数据泄密、防恶意下载等。

5.5.2 物理安全

5.5.2.1 应制定物理安全防护策略，包括人员、数据、设备、支持系统、介质和所需的供给品。

5.5.2.2 物理安全的控制措施包括安全设施的选择和建设、设施安全管理、人员管理控制。

5.5.2.3 应利用强制能力控制机制，使对外提供服务的进程以普通用户身份运行。

5.5.3 安全责任制度

5.5.3.1 应建立安全责任制度，包括：

a) 设置安全管理机构；
b) 成立安全管理小组，明确职责；
c) 配备专职安全管理人员；
d) 明确项目安全管理职责，落实安全主体责任；
e) 制定安全管理制度、岗位职责等。

5.5.3.2 安全管理小组应由系统分析、软件、硬件、保卫、审计、人事、通信等有关方面人员组成。

5.5.4 安全检查

5.5.4.1 在项目实施过程中，应定期开展安全自纠自查工作，制定专项隐患排查工作方案，重点对可能出现隐患的方面进行排查。

5.5.4.2 应建立安全检查档案制度，对检查处理情况记录在案。

6 过程管理

6.1 立项

6.1.1 成立项目评估委员会负责开发项目立项审批。评估委员会应由公司总经理或指定负责人召集，由管理层人员组成。

6.1.2 形成项目需求说明书，确定项目需求管理人或项目申请人。

6.1.3 项目申请人填写项目立项申请书，向项目评估委员会提出立项申请，立项申请书应说明项目的背景、目的、效益、成本、需求等，并由技术部门提供支持和技术说明。

6.1.4 评估项目可行性，若不批准，应给出理由并中止项目，中止的项目可整改后重新申请。评估结果应包括：

a) 建议项目启动日期；
b) 期望项目完成日期；
c) 项目等级系数；
d) 项目优先级；
e) 资源冲突程度。

6.2 需求确认

6.2.1　需求确认流程见图 3。

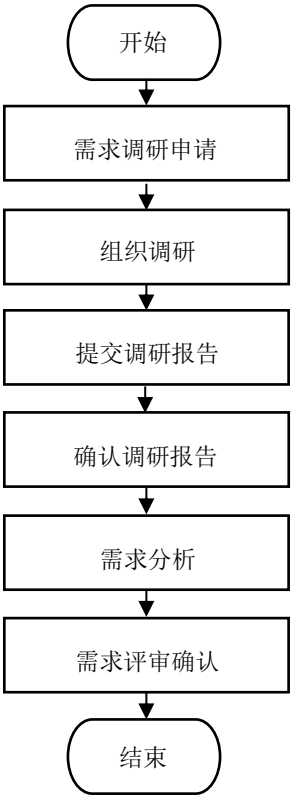

图3　需求确认流程图

6.2.2　需求调研要求如下：

a)　应制定需求调研计划，下发正式的文件明确调研的目的、时间、人员、内容；
b)　相关部门应配合需求调研活动；
c)　可采用业务场景模拟、业务用例、界面原型等方式展现需求调研与分析的结果；
d)　可采用专家评审会的方式，确保需求分析成果满足项目要求。

6.3　系统设计与编码

6.3.1　系统设计与编码流程见图 4。

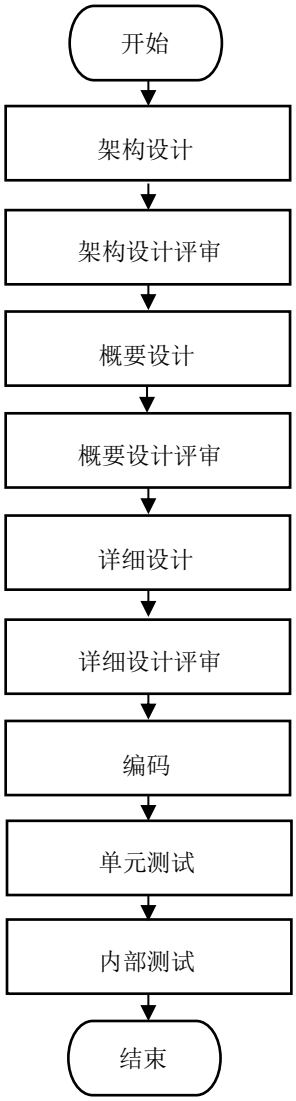

图4　系统设计与编码流程图

6.3.2　系统设计与编码要求如下

a)　应按确认的设计模板进行设计文档的编制；

b)　对于设计过程中出现的重大变更，应按需求变更流程进行管控；

c)　应编制全面的测试用例进行单元测试与内部测试；

d)　应每周定期汇报项目进展情况。

6.4　测试

6.4.1　测试流程见图 5。

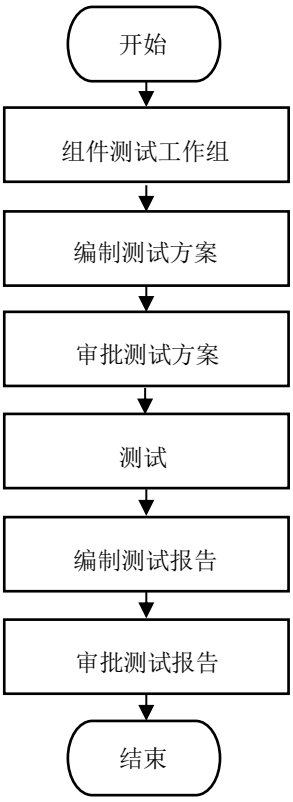

图5　测试流程图

6.4.2　在内部测试的基础上完成系统集成测试，应满足软件正常运行的要求。

6.4.3　测试包括测试准备与系统测试，测试内容包括功能测试、用户界面测试、性能测试、接口测试、安全测试等。

6.4.4　测试要求如下：

a)　组建测试工作组，工作组包括承建单位、建设方、业务部门等；

b)　应在系统测试之前完成内部测试工作，并将需要测试的系统部署在测试环境中；

c)　应根据项目合同要求，编制测试方案、测试用例；

d)　若项目合同中约定由第三方测试机构进行系统测试，则按合同规定进行；

e)　若项目需要与其它系统进行集成测试，应协调其它系统开发商进行联合集成测试，并出具集成测试报告。

6.5　试运行

6.5.1　试运行流程见图 6。

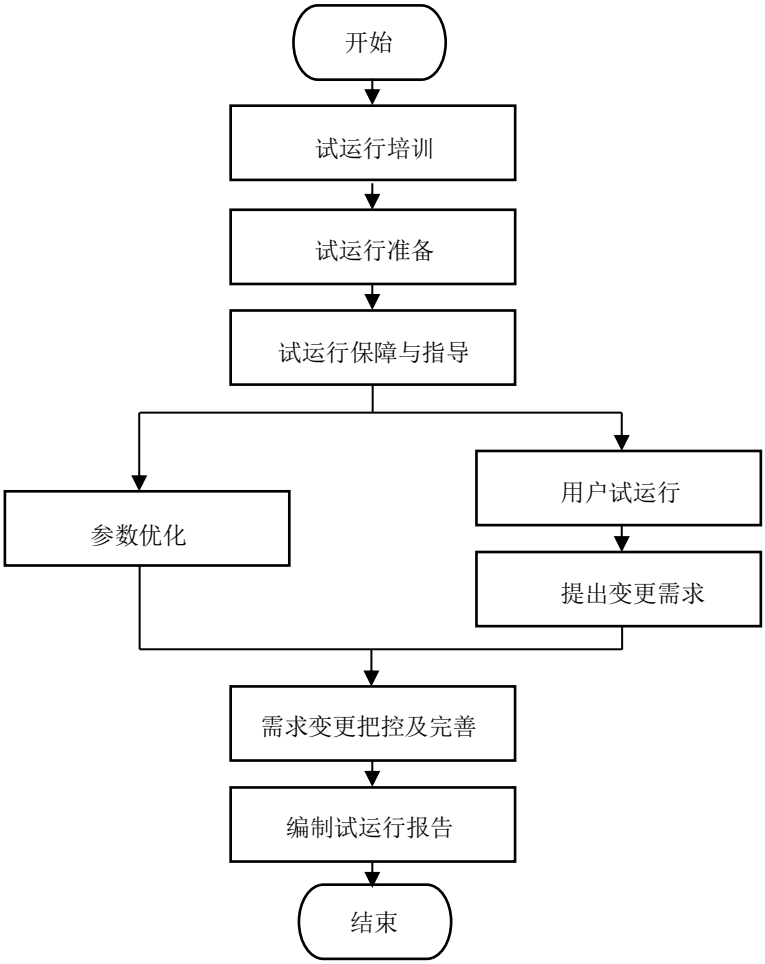

图6　试运行流程图

6.5.2　通过试运行优化业务流程与配置，修复试运行过程中出现的问题。

6.5.3　试运行流程要求如下：

a)　试运行前应做好试运行培训和用户帐号等数据准备工作；

b)　试运行过程中应收集问题，及时有侧重地解决问题，保障试运行顺利进行；

c)　试运行过程中应做好需求变更管理，满足项目实际需求且使需求变更在合理范围内。

6.6　初验

6.6.1　初验流程见图 7。

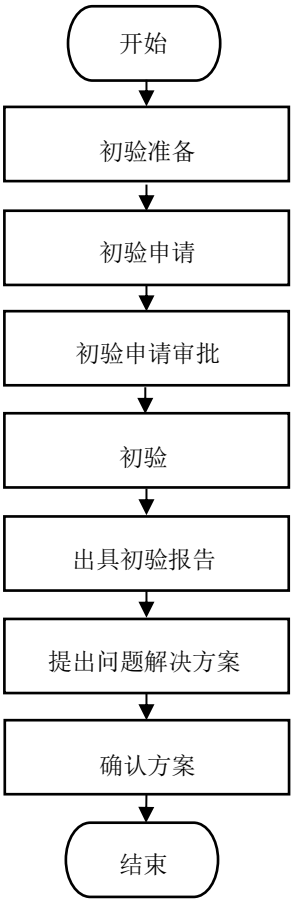

图7　初验流程图

6.6.2　初验要求如下：

a)　初验前应做好系统运行情况检查和系统试运行问题解决情况检查，只有所有的检查均通过之后，才可进行项目初验；

b)　初验前，宜出具系统试运行报告，作为系统初验的依据；

c)　初验前，并修改完善项目技术文档，包括需求分析说明书、需求规格说明书、系统概要设计说明书、系统详细设计说明书、系统数据库设计说明书、系统接口设计说明书、系统上线部署手册、系统用户手册、系统维护手册；

d)　初验应由相关方共同参与；

e)　初验报告应详细说明初验遗留问题及相关方约定的承诺。

6.7　验收

6.7.1　验收流程见图 8。

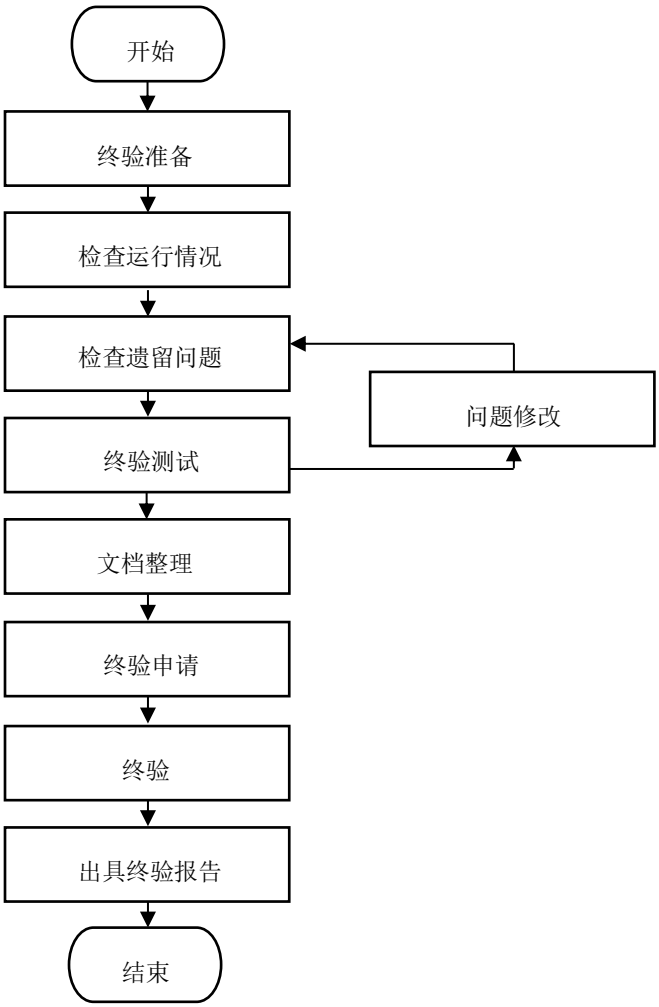

图8　验收流程图

6.7.2　验收要求如下：

a)　验收之前应明确初验遗留问题都已解决完成，或者已明确替代解决方案；

b)　验收时应修改完善项目技术文档，包括需求分析说明书、需求规格说明书、系统概要设计说明书、系统详细设计说明书、系统数据库设计说明书、系统接口设计说明书、系统上线部署手册、系统用户手册、系统维护手册；

c)　若项目合同中约定由第三方测试机构进行系统测试，则按合同规定进行；

d)　验收应由相关方共同参与。

6.8　培训

6.8.1　确定培训时间、培训地点，进行系统演示、使用培训、操作指导等培训。

6.8.2　培训过程中应收集问题和建议，进行跟踪处理。

6.9　上线与运维

6.9.1　制定上线计划，确定上线工作时间表和部署的环境，记录软件部署和运行结果。

6.9.2　组根据系统运行情况对系统进行优化，记录系统的运行情况、系统问题和处理后的版本。

6.9.3　上线后，应定期对服务器进行维护、系统运行监控、安全加固、漏洞修复等对系统运行指标、

告警、日志进行监控与分析，处理隐患。

7 软件安全

7.1 项目设计时应考虑以下安全要求：

a) 应用系统体系架构安全，如从应用系统架构设置系统权限管理、防越权设计、增设过滤管理等应用系统架构机制等；
b) 数据库安全：如保证系统的数据的完整性、一致性、逻辑性和可用性，数据库数据的定期备份，数据库访问口令安全管理，数据库访问口令加密等；
c) 应用开发安全管理：如防止开发现场原代码、生产数据及重要加密算法泄露、遗失、被盗等，强化保密协议等的签订和管理等；
d) 系统传输安全：为可以使用 CA 认证，SSL 加密传输，VPN 接入等多种方式等；
e) 系统使用安全：制定使用管理规定，如制定终端设备使用安全、信息保密管理及账户管理规定，指定专门系统管理员等。

7.2 对于实行信息系统安全等级保护的项目，应符合 GB 17859、GB/T 22239、GB/T 22240、GB/T 25058、GB/T 25070、GA/T 708、GA/T 709、GA/T 710、GA/T 1389、GA/T 1390（所有部分）的相关规定。

8 评价与改进

8.1 评价

对项目进行评价，通过后评价机制不断优化项目管理水平，给出优化运行与持续改进的建议。

8.2 改进

8.2.1 应根据评价结果，提出纠正措施和预防措施，持续改进。

8.2.2 应确保不符合要求的开发过程和结果得到识别和控制，并规定不符合项控制以及处置的有关职责和权限。在不符合项得到纠正后应对其再次进行验证，证实该项已符合要求。

8.2.3 应识别不符合项出现的原因并采取纠正措施，防止不符合项的再次发生纠正措施应与不符合项的影响程度相适应。

8.2.4 采取纠正措施应形成文件记录，记录内容应包括以下内容：

a) 评审中所存在的问题；
b) 问题产生的根本原因以及次生原因；
c) 确定和实施所需的纠正措施；
d) 所采取措施的相对应结果；
e) 所采取纠正措施的有效性；